Foundations in Privacy Toolkit

Table of Contents

Foundations in Privacy Toolkit

As many health care providers know and experience, exchanging patient information can be challenging from both a legal and operational perspective. From the legal perspective, providers are forced to sort through the myriad of privacy laws, rules, and regulations and determine which rules apply to a particular use or disclosure of patient information. Given that Minnesota Law often conflicts with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), this is no easy feat. From an operational perspective, organizations are required by HIPAA to develop privacy policies and procedures and train their workforce on these complex rules.

The Foundations in Privacy Toolkit (the "Toolkit") was developed to address these challenges. Pursuant to the ***Privacy, Security and Consent Management for Electronic Health Information Exchange grant*** (the "Grant")[1], the Minnesota Department of Health ("MDH") partnered with Gray Plant Mooty to analyze legal barriers and develop tools to support the exchange of health information in Minnesota.

The Toolkit contains the following types of material, organized by subject area:

- Template policies and procedures
- Flow charts
- Template agreements
- Checklists

These documents can be used by providers in many ways. The policy and procedure documents can be customized and implemented as part of an organization's HIPAA privacy compliance efforts. The flow charts and checklists can be used to analyze business relationships and unique disclosure situations, and the template agreements can be used to guide negotiations and simplify execution. All of the documents can be used to educate and train workforce.

It is important to note that the Toolkit is a ***foundation*** for HIPAA and Minnesota law compliance. It does not address every scenario, and providers will need to supplement these materials to include legal requirements and standards specific to their organization. Further, some areas of privacy law are subject to multiple interpretations; while we have described alternative views for some of these issues we have not attempted to address all of the areas where differing interpretations exist. Providers will also need to modify Toolkit documents as the law changes.

This Toolkit is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein. Please feel free to contact any of the following members of Gray Plant Mooty's Health Law Group.

Catie Bitzan Amundsen	*Jesse A. Berg*	*Jennifer Reedstrom Bishop*
Sarah Duniway	*Wade S. Hauser*	*Timothy A. Johnson*
Greg A. Larson	*Julia C. Reiland*	*Erin B. Stein*

[1] This grant project is part of a $45 million State Innovation Model (SIM) cooperative agreement, awarded to the Minnesota Departments of Health and Human Services in 2013 by The Center for Medicare and Medicaid Innovation (CMMI) to help implement the Minnesota Accountable Health Model.

[Enter Organization Logo]

DEFINITIONS

Policy Number: [Enter]
Effective Date: [Enter]

In General: Any terms used but not otherwise defined in this policy have the definitions set forth in HIPAA Privacy Rule, HIPAA Security Rule and HIPAA Breach Notification Rule, 42 C.F.R. Part 2, or the Minnesota Health Records Act, as applicable. The following definitions have a meaning specific to this policy or, if the definitions are the same as the definitions provided in the applicable law, are provided for the convenience of the reader.

1) **Affiliate**: An entity that controls, is controlled by, or is under common control with another entity.

2) **Authorization:** A signed written document meeting the requirements of 45 C.F.R. § 164.508.

3) **Breach**: Except as otherwise provided in the HIPAA breach notification rule, "breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule which compromises the security or privacy of the protected health information.

4) **Consent:** Written permission to release health information that is dated and signed by the individual.

5) **Health Care Operations**: Any of the following activities, to the extent that the activities are related to covered functions:

   (i) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

   (ii) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

   (iii) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and

excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(iv) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(v) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(vi) Business management and general administrative activities of the entity, including, but not limited to:

(A) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(B) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(C) Resolution of internal grievances;

(D) The sale, transfer, merger, or consolidation of all or part of *[Organization]* with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(E) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of *[Organization]*.

6) **HIPAA**: The federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and the accompanying Regulations.

7) **Marketing**: Marketing includes any communication about [*Organization*]'s products or services that encourages individuals to purchase or use the products or services. Marketing does not include a communication made:

(i) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, provided any financial remuneration received by [*Organization*] in exchange for making the communication is reasonably related to [*Organization*]'s cost of making the communication;

(ii) For the following treatment and health care operations purposes, except where [*Organization*] receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by [*Organization*], including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, [*Organization*], including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

8) **Medical Emergency**: Medically necessary care which is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.

9) **Mental Health Records**: Information, whether oral or recorded, that relates to the past, present, or future mental health or condition of an individual.

10) **Minnesota Health Records Act**: Minnesota Statutes sections 144.291–144.298.

11) **Payment**: Payment means:

(i) The activities undertaken by:

(A) Except as prohibited under 45 CFR § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(B) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(ii) The activities in section (i) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(A) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(B) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(C) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(D) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(E) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(F) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(1) Name and address;

(2) Date of birth;

(3) Social security number;

(4) Payment history;

(5) Account number; and

(6) Name and address of the health care provider and/or health plan.

12) **PHI**: Protected health information as defined in 45 C.F.R. 160.103.

13) **Psychotherapy Notes**: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

14) **Qualified Service Organization**: An individual or entity who:

(i) Provides services to a part 2 program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and

(ii) Has entered into a written agreement with a part 2 program under which that individual or entity:

(A) Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the part 2 program, it is fully bound by the Part 2 regulations; and

(B) If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by the Part 2 regulations.

15) **Regulations**: the HIPAA Privacy Rule ("Privacy Rule"), HIPAA Security Rule ("Security Rule"), and the HIPAA Breach Notification Rule ("Breach Notification Rule"), which are codified in 45 C.F.R. Parts 160 and 164.

16) **Related Health Care Entity**: An Affiliate of the provider releasing the health records.

17) **Secretary**: The Secretary of the United States Department of Health and Human Services

18) **Substance Use Disorder**: A cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. This definition does not include tobacco or caffeine use.

19) **Treating Provider Relationship**: Means that, regardless of whether there has been an actual in-person encounter:

(i) A patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated, or agrees to accept consultation, for any condition by an individual or entity, and;

(ii) The individual or entity undertakes or agrees to undertake diagnosis, evaluation, and/or treatment of the patient, or consultation with the patient, for any condition.

20) **Treatment**: The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

21) **Withdrawal Management**: The use of pharmacotherapies to treat or attenuate the problematic signs and symptoms arising when heavy and/or prolonged substance use is reduced or discontinued

22) **Workforce**: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

[Enter Organization Logo]

BREACH OF UNSECURED PHI

Policy Number: [Enter]
Effective Date: [Enter]

HIPAA requires Covered Entities to notify affected individuals, the U.S. Department of Health & Human Services, and, in some cases, the media of a "Breach" of Unsecured PHI. <u>This policy is designed for use by health care providers that qualify as Covered Entities.</u> HIPAA also requires Business Associates to notify the Covered Entity following the Business Associate's discovery of a Breach of Unsecured PHI. *See* 45 C.F.R. § 164.410.

As discussed in Part II below, Minnesota law also requires disclosure of a "breach of the security of the system" in some circumstances. Minn. Stat. § 325E.61.

I. HIPAA Breach Policy:

A. Purpose

[Organization] must comply with rules related to privacy incident response and breach notification. *[Organization]* shall immediately respond to any actual or potential Breach of PHI (a "Privacy Incident") to ensure confidentiality is maintained and to mitigate any adverse effects resulting from the Privacy Incident. Privacy Incidents shall be reported to the Privacy/Security Official immediately for further investigation as outlined below.

B. In General

The Privacy/Security Official shall notify patients (and the Secretary and potentially the media, as described below) of any Breach of Unsecured PHI as required under the Regulations and pursuant to the following procedure:

1. Notification of Privacy/Security Official

Workforce members shall as soon as possible, notify the Privacy/Security Official of any Privacy Incident. The Privacy/Security Official shall ensure that any necessary training occurs so that Workforce members understand their obligations to make such reports to the Privacy/Security Official. The Privacy/Security Official, along with the Response Team, as outlined in Section I.D of this policy (the "Response Team"), will investigate all reports of Privacy Incidents to determine whether the Privacy Incident in fact constitutes a violation of the Privacy Rule (subpart E of 45 C.F.R. part 164).

2. **2. Risk Assessment to Determine Whether the Privacy Incident is a Breach**

If the Privacy Incident constitutes a violation of the Privacy Rule, the Privacy/Security Official and the Response Team will conduct a documented risk assessment of the violation to determine if the Privacy Incident meets the regulatory definition of "Breach" or if it can be demonstrated that there is a low probability that the PHI has been

compromised based on an analysis of certain factors, as set forth under the Regulations at 45 C.F.R. § 164.402.

3. **3. Exceptions**

In conducting this analysis, the Privacy/Security Official and Response Team will also determine and document if the violation meets any of the regulatory exceptions to the definition of Breach at 45 C.F.R. § 164.402(1)(i)-(iii). These exceptions include:

> (i) An unintentional acquisition, access, or use of PHI by a Workforce member or person acting under the authority of *[Organization]*, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.
>
> (ii) Any inadvertent disclosure by a person who is authorized to access PHI at *[Organization]* to another person authorized to access PHI at *[Organization]*, or organized health care arrangement in which *[Organization]* participates, and the information received as a result of such disclosure is not further used or disclosed.
>
> (iii) A disclosure of PHI where *[Organization]* has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

4. **4. Risk Assessment Factors**

Except as provided directly above, any unauthorized Use or Disclosure of PHI in violation of the Privacy Rule is presumed to be a Breach. However, the Response Team will conduct a documented risk assessment of the violation to determine if the regulatory definition of "Breach" has been triggered by the Privacy Incident or if it can be demonstrated that there is a low probability that the PHI has been compromised based on an analysis of at least the four factors set forth below. However, additional factors may need to be considered to appropriately assess the risk that the PHI has been compromised, given the circumstances of the impermissible Use or Disclosure, and as determined to be appropriate by the Privacy/Security Official and the Response Team.

- The nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification. Examples of particularly sensitive data would include a patient's social security number, credit card number, or health history.

- The unauthorized person who used the PHI or to whom the disclosure was made. For example, a recipient who is obligated to abide by HIPAA (e.g., another Covered Entity) generally poses a lower risk of compromising the PHI than someone who has no independent obligations to comply with HIPAA.

- Whether the PHI was actually acquired or viewed. For example, PHI is not actually acquired or viewed when a laptop containing PHI is stolen or

lost and a forensic study of the laptop shows that the PHI was never accessed. PHI would be actually acquired or viewed if *[Organization]* mails PHI to the wrong person and the person opens the letter.

- The extent to which the risk to the PHI has been mitigated. For example, there may be a lower risk of compromise if *[Organization]* receives satisfactory assurances from the recipient that there was no further Use or Disclosure of the PHI and that the PHI has been destroyed.

[Organization]'s analysis should include each of the factors discussed above and such other factors as the Privacy/Security Official and the Response Team determine to be necessary. *[Organization]* will then evaluate the overall probability that the PHI has been compromised by considering all factors in combination.

5. **5. Burden of Proof**

In the event of a Use or Disclosure of PHI in violation of the Privacy Rule, *[Organization]* has the burden of demonstrating that the Use or Disclosure does not constitute a Breach or that all notifications required under HIPAA have been made. *See* 45 C.F.R. § 164.414(b).

6. **6. Notification to Patients**

If the violation is determined to be a Breach, the Privacy/Security Official will notify each individual whose Unsecured PHI has been, or is reasonably believed by *[Organization]* to have been, accessed, acquired, used, or disclosed, as a result of such Breach. The Privacy/Security Official will provide this notification without unreasonable delay, but in any event within 60 calendar days after the date the Breach was discovered. *[Organization]* shall delay the notification pursuant to a request of law enforcement as described in section 9 below. The Privacy/Security Official shall give notice in the manner described in 45 C.F.R. § 164.404(d) and the notification will contain the following information:

- A brief description of what happened, including the date of the Breach and date of discovery of the Breach, if known;

- A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

- Any steps the patient(s) should take to protect themselves from potential harm resulting from the Breach;

- A brief description of what *[Organization]* is doing to investigate the Breach, to mitigate harm to patients, and to protect against any further Breaches; and

- Contact procedures for patients to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

7. **7. Notification to the Secretary of Department of Health & Human Services**

Following the discovery of a Breach of Unsecured PHI, *[Organization]* must notify the Secretary of the United States Department of Health and Human Services pursuant to 45 C.F.R. § 164.408. For Breaches of Unsecured PHI involving 500 or more individuals, *[Organization]* shall, except pursuant to a delay requested by law enforcement as described in section 9 below, provide notice to the Secretary contemporaneously with the notice to patients discussed above and in the manner specified on the HHS website. For Breaches of Unsecured PHI involving fewer than 500 individuals, *[Organization]* shall maintain a log or other documentation of such Breaches and, not later than 60 days after the end of each calendar year, provide notice to the Secretary of Breaches discovered during the preceding calendar year, in the manner specified on the HHS website. *[Organization]* can make this notification on the HHS Website.

8. **8. Notification to the Media**

For any Breach involving more than 500 patients, *[Organization]* must notify the media pursuant to 45 C.F.R. § 164.406. Except pursuant to a delay requested by law enforcement as described in section 9 below, *[Organization]* will provide such notice without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach.

9. **9. Delay Requested by Law Enforcement**

If a law enforcement official states to *[Organization]* that a notification, notice, or posting required by this policy would impede a criminal investigation or cause damage to national security, *[Organization]* shall delay such notification, notice, or posting in accordance with this policy and 45 C.F.R. § 164.412.

- If the law enforcement official's statement is in writing and specifies the time for which a delay is required, *[Organization]* will delay such notification, notice, or posting for the time period specified by the official;

- If the law enforcement official's statement is made orally, *[Organization]* will document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a law enforcement official submits a written statement to *[Organization]* during that time.

C. **Retention**

The Privacy/Security Official shall maintain a log of all risk assessments and breach notifications made by the *[Organization]* pursuant to this policy. The log should

maintain documentation that all required notifications were made, or alternatively, of the risk assessment analysis that an impermissible Use or Disclosure did not constitute a Breach in cases where it was determined that a Breach did not occur. All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate all appropriate steps were completed. All supporting documentation associated with the potential Breach shall be maintained for a minimum of six (6) years.

D. **Response Team**

1. **1. Composition of Response Team**

When notified of a Privacy Incident, the Privacy/Security Official shall assemble a Response Team with composition determined by the facts and circumstances of the Privacy Incident. Response Team members shall include the Privacy/Security Official and personnel as determined to be appropriate, which may include:

- Representatives from the location or department where the incident occurred;
- Risk management representative;
- Information technology representative;
- Outside legal counsel and other experts as appropriate.

2. **2. The Response Team Shall Take the Following Actions:**

- Create a timeline of events and determine additional facts as necessary;
- Determine response(s) to incident and assign responsibilities and timeframe for completion; and
- Determine if any policies and procedures or processes must be changed to mitigate incident recurrence. Assign responsibility for making changes and follow-up to confirm completion.

E. **Miscellaneous**

1) **The Privacy/Security Official shall maintain files of Privacy Incident Response Team investigations and meetings;**

2) **The policies and procedures relating to training, complaints, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures and documentation (as required under 45 C.F.R. § 164.530(b), (d), (e), (g), (h), (i) and (j)) apply to the provisions outlined in these Breach Notification Procedures;**

3) **Capitalized terms not otherwise defined herein shall have the meanings assigned to them in the HIPAA regulations.**

II. **Breach of the Security of the System Policy:**

A person or business that conducts business in Minnesota, must comply with Minnesota law regarding a "breach of the security of the system." Minn. Stat. § 325E.61. Government entities must comply with similar rules. *See* Minn. Stat. § 13.055. <u>This policy is designed to explain the obligations of non-governmental health care providers.</u> Many other states have similar rules designed to protect residents of those states.

A. **Purpose**

[Organization] must comply with Minnesota law regarding a "breach of the security of the system." *[Organization]* shall immediately respond to any actual or potential breach of the security of the system according to the same policies and procedures documented above.

B. **In General**

The Privacy/Security Official shall notify affected residents of Minnesota (and potentially consumer reporting agencies) of any breach of the security of the system pursuant to the following procedure:

1. **1. Assessment to Determine Whether the Privacy Incident is a Breach of the Security of the System**

Following notification of Privacy/Security Official of any Privacy Incident, the Privacy/Security Official, along with the Response Team, will investigate and determine whether the Privacy Incident constitutes a breach of the security of the system as defined in Minnesota Statutes section 325E.61.

2. **2. Definition of Breach of the Security of the System**

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by *[Organization]*.

3. **3. Exception**

Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

4. 4. Definition of Personal Information

The term “personal information” means, when not encrypted, an individual’s first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number;
- Driver’s license number or Minnesota identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

5. 5. Notification to Patients

If the violation is determined to be a breach of the security of the system, the Privacy/Security Official will notify each Minnesota resident of whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The Privacy/Security Official will provide this notification in the most expedient time possible and without unreasonable delay. *[Organization]* will delay the notification pursuant to a request of law enforcement in accordance with Minnesota Statutes section 325E.61(c). The Privacy/Security Official shall give notice in the manner described in Minnesota Statutes section 325E.61(g).

6. 6. Notification to Consumer Reporting Agencies

If *[Organization]* discovers a breach of the security of the system requiring notification of more than 500 persons at one time, *[Organization]* shall also notify, within 48 hours, all major national consumer reporting agencies (as defined in 15 U.S.C. § 1681a(p)) of the timing, distribution, and content of the notices to individuals.

[Enter Organization Logo]

DISCLOSING INFORMATION TO BUSINESS ASSOCIATES

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Policy Purpose:

This policy establishes guidelines for the disclosure of patient health information to, and use by, a business associate.

B. Policy Implementation

1. General Rule

A business associate is a person or entity that performs certain functions, activities, or services for or on behalf of [*Organization*] that involves the use or disclosure of PHI.

If [*Organization*] enters into a Business Associate Agreement and obtains satisfactory assurance that the business associate will appropriately safeguard PHI, [*Organization*] may disclose PHI to the business associate and allow that business associate to create, receive, maintain, or transmit PHI on [*Organization*]*'s* behalf. [*Organization*] is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

[GPM Note: Although Minnesota law generally requires that individuals consent to the release of PHI, Minnesota law does not require a specific form of consent. [Organization] may expressly address disclosures to its business associates in its standard consent form. Alternatively, [Organization] may release information to its business associates under the theory that the business associate is acting as its agent and the activities and services performed by the business associate fall within the permissions [Organization] secures via the consent form.]

Substance Use Disorder Patient Records. 42 CFR Part 2 similarly permits [*Organization*] to disclose substance use disorder patient records to agencies that provide services to [*Organization*]. While the HIPAA Regulations call these agencies "business associates," Part 2 calls these agencies "Qualified Service Organizations." Prior to disclosing substance use disorder patient records, [*Organization*] must enter into a written agreement that meets the requirements of Part 2.

For more information on disclosing Substance Use Disorder Patient Records, refer to policy number [Enter], Disclosures of Substance Use Disorder Patient Records.

Throughout this Policy, use of the term "protected health information" or "PHI" includes electronic protected health information (or "ePHI"), and vice versa.

2. **Determining Who is a Business Associate**

[*Organization*] shall determine whether or not an entity/vendor is a business associate of [*Organization*] through the following three questions:

a. Does [*Organization*] have a contractual or other business or services relationship with the entity/vendor to perform services or activities on behalf of [*Organization*]?

This includes functions or activities such as claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; certain patient safety activities; billing; benefit management; practice management; and re-pricing.

It also includes entities/vendors that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for [*Organization*].

A member of [Organization]'s workforce is NOT a business associate.

b. Does [*Organization*] need to supply the entity/vendor with PHI or access to PHI in order for the entity/vendor to perform its service or activity on behalf of [*Organization*]?

c. Is the service or activity a service or activity other than treatment?

If the answer to all three of these questions is "Yes", the entity/vendor is a business associate of [*Organization*].

Who is NOT a business associate. When a contract is with another provider to provide treatment, the vendor/provider is NOT a business associate. Similarly, if [*Organization*] is a member of a health plan network and the only relationship between the health plan (payer) and [*Organization*] is one where [*Organization*] submits claims for payment to the plan, then [*Organization*] is not a business associate of the health plan. Each covered entity is acting on its own behalf when [*Organization*] submits a claim to a health plan, and when the health plan assesses and pays the claims.

For additional help on making this determination, members of [*Organization*]'s workforce should consult the business associate flow chart entitled, "How to Identify a 'Business Associate'".

3. **Business Associate Agreements**

[*Organization*] shall use a written agreement with its business associates to ensure and document that its business associates will appropriately safeguard PHI received from [*Organization*].

If [*Organization*] becomes aware of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation under the contract or other arrangement, [*Organization*] shall take reasonable steps to cure the breach or end the violation, as applicable. If the steps taken to cure the breach or end the violation are unsuccessful, [*Organization*] shall terminate the contract, if feasible.

If the business associate becomes aware of a pattern of activity or practice of the subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the contract or other arrangement, the business associate shall take reasonable steps to cure the breach or end the violation, as applicable. If the steps taken to cure the breach or end the violation are unsuccessful, the business associate shall terminate the contract, if feasible.

Substance Use Disorder Patient Records. Prior to disclosing substance use disorder patient records, [*Organization*] must enter into a written agreement, often called a Qualified Service Organization Agreement, that meets the requirements of Part 2. *See* Section 4 below for information on how to satisfy these requirements.

4. **Requirements for Business Associate Agreements**

A business associate agreement between [*Organization*] and a business associate must:

a. Establish the permitted and required uses and disclosures of PHI by the business associate. The agreement may not authorize the business associate to use or further disclose the PHI in a manner that would violate the HIPAA Regulations or these policies if the use or disclosure was done by [*Organization*]; However:

   i. The agreement may permit the business associate to use and disclose PHI for the proper management and administration of the business associate; and

   ii. The agreement may permit the business associate to provide data aggregation services relating to the health care operations of [*Organization*].

b. Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;

c. Provide that the business associate will use appropriate safeguards and comply, where applicable, with the HIPAA Regulations provisions pertaining to electronic protected health information, to prevent use or disclosure of ePHI other than as

provided for by its contract;

d. Provide that the business associate will report to [*Organization*] any use or disclosure of the PHI not provided for by its contract, whenever it becomes aware of such unauthorized use or disclosure, including breaches of unsecured PHI;

e. Provide that the business associate will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate shall agree to the same restrictions and conditions that apply to the business associate with respect to the PHI;

f. Provide individuals access to PHI in accordance with these policies and the HIPAA Regulations;

g. Provide individuals the right to amend PHI in accordance with these policies and the HIPAA Regulations;

h. Provide individuals the right to an accounting of disclosures of PHI in accordance with these policies and the HIPAA Regulations;

i. Provide that to the extent the business associate is to carry out [*Organization*]*'s* obligations under the HIPAA Regulations, the business associate will comply with the requirements that apply to [*Organization*];

j. Require the business associate to make its internal practices, books, and records relating to the use and disclosure of PHI received from [*Organization*] (or created or received by the business associate on behalf of [*Organization*]) available to the Secretary of Health and Human Services for purposes of determining [*Organization*]*'s* compliance with the HIPAA Regulations;

k. Requires the business associate to report to [*Organization*] any security incident of which it becomes aware, including breaches of unsecured PHI;

l. At termination of the agreement, if feasible, return or destroy all PHI received from [*Organization*] (or created or received by the business associate on behalf of [*Organization*]) that the business associate maintains in any form (including copies of such information). If the return or destruction of the PHI is not feasible, the business associate shall extend the protections of the contract to the information and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the information infeasible; and

m. Authorize termination of the contract by [*Organization*], if [*Organization*] determines that the business associate has violated a material term of the contract.

When entering into arrangements with business associates, [*Organization*] should use the Template Business Associate Agreement.

Business Associate Agreements involving Substance Use Disorder Patient Records. Prior to disclosing substance use disorder patient records, [*Organization*] must enter into a written agreement with the vendor/entity under which that vendor/entity:

1. Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the programs, it is fully bound by Part 2 and promises to safeguard such information; and

2. If necessary, it will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment, except as permitted by Part 2.

To satisfy this requirement, [*Organization*] staff should take [*Organization*]'s template Business Associate Agreement and insert the following language:

Business Associate acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from [Organization], it is fully bound by the Confidentiality of Substance Use Disorder Patient Records regulations at 42 CFR Part 2. If necessary, Business Associate will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment, except as permitted by these regulations.

For more information on disclosing Substance Use Disorder Patient Records generally, refer to policy number [Enter], Disclosures of Substance Use Disorder Patient Records.

5. **Special Situations Related to the Business Associate Agreement**

   a. *If a business associate is required by law to perform a function or activity on behalf of* [*Organization*]: If a business associate is required by law to perform a function or activity on behalf of [*Organization*] or to provide a service described in the HIPAA Regulations' definition of *business associate*, [*Organization*] may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without a business associate contract or a memorandum of understanding, provided that [*Organization*] attempts in good faith to obtain satisfactory assurances as described in the requirements for a business associate contract, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

b. *If authorization to terminate the contract is inconsistent with the statutory obligations*: *[Organization]* may omit from its business associate agreement the authority to terminate the agreement for a material breach of the agreement, if such authorization is inconsistent with the statutory obligations of [*Organization*] or its business associate.

c. *If* [*Organization*] *and the business associate have a data use agreement:* [*Organization*] may comply with the HIPAA Regulations if [*Organization*] discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and [*Organization*] has a data use agreement with the business associate.

6. **Use and Disclosure of PHI by a Business Associate for the Business Associate's Own Management and Administration**

The business associate agreement between [*Organization*] and a business associate may permit the business associate to **use** (not disclose) the PHI received by the business associate, if necessary:

a. For the proper management and administration of the business associate; or

b. To carry out the legal responsibilities of the business associate.

The business associate agreement between [*Organization*] and a business associate may permit the business associate to **disclose** the PHI received by the business associate for: (A) the proper management and administration of the business associate; or (B) carrying out the legal responsibilities of the business associate, if:

a. The disclosure is required by law; or

b. The business associate obtains reasonable assurances from the person to whom the PHI is disclosed that:

i. It will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

ii. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

7. **Business Associate Contracts with Subcontractors**

The requirements of this policy apply to contracts or other arrangements between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contractors or other arrangements between [*Organization*] and business associate.

When entering into arrangements with subcontractors, business associates should use the Template Subcontractor Business Associate Agreement.

8. **Documentation Regarding a Business Associate Contract**

[*Organization*] shall document and retain a business associate contract or memorandum of understanding, in written or electronic format for at least six (6) years from the date when the business associate contract or memorandum of understanding was last in effect.

II. Procedure:

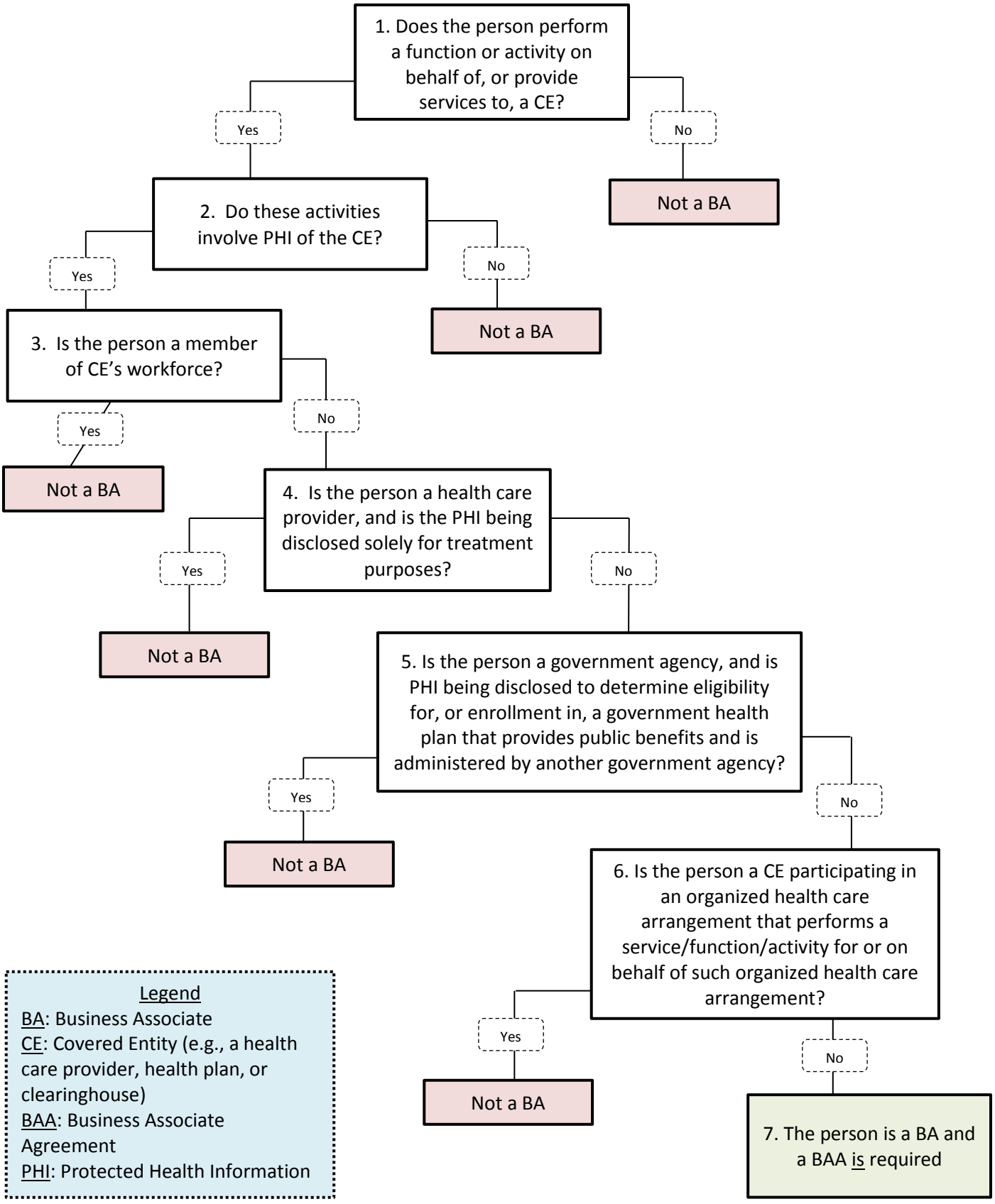
A. [*Organization*] and its employees will determine whether an entity/vendor is a business associate in accordance with this policy.

B. If an entity/vendor is a business associate of [*Organization*], Director or designee must contact the Privacy Officer to set up the needed written agreements.

C. [*Organization*] will only disclose PHI to a business associate in accordance with this policy and the written agreements.

How to Identify a "Business Associate"

For Health Care Providers



Legend

BA: Business Associate

CE: Covered Entity (e.g., a health care provider, health plan, or clearinghouse)

BAA: Business Associate Agreement

PHI: Protected Health Information

Instructions for Boxes 1-7

1) **Functions/Activities** include claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing.

   Services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

   *Note that the potential BA can be an individual or entity, and a CE may be a BA of another CE.

   *Remember that the person must be acting *for or on behalf of* a CE, not on its own behalf. For example, when a health care provider discloses PHI to a health plan for payment purposes, there is no BA relationship. This is because both are acting on its own behalf as a CE, not as the 'business associate' of the other.

2) **Protected Health Information (PHI)** means individually identifiable health information that is: (a) transmitted electronically; (b) maintained electronically; or (c) transmitted or maintained in any other form or medium. Individually identifiable health information (IIHI) is information that is a subset of health information, including demographic information collected from an individual, and:

   a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

   b) Relates to the past, present, or future physical or mental health or condition or an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

      i) That identifies the individual; or

      ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

   PHI *excludes* IIHI: (a) In education records covered by FERPA; (b) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (c) In employment records held by a CE in its role as an employer; and (d) Regarding a person who has been deceased for more than 50 years.

3) **Workforce** includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a CE, is under the direct control of such CE, whether or not they are paid by the CE.

4) Examples include:

   a) A hospital is not required to have a business associate agreement with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes;

   b) A physician is not required to have a business associate agreement with a laboratory when disclosing PHI for the treatment of the individual.

   c) A hospital laboratory is not required to have a business associate contract with a reference laboratory when disclosing PHI or treatment of the individual.

5) This includes the Medicare program.

6) **An organized health care arrangement** includes an arrangement or relationship in which participants are clinically integrated and an organized system of health care in which participating entities engage in certain joint activities. The full definition can be found at 45 CFR 160.103.

7) If the person is a BA, the CE and the BA must enter into a ***business associate agreement*** that ensures that the BA will appropriately safeguard PHI.

   See the Template Business Associate Agreement and/or the Business Associate Checklist to verify that the Business Associate agreement satisfies HIPAA requirements.
   For more information on BAs, *see* policy [Enter], "Disclosing Information to Business Associates."

Business Associate Agreement Checklist – Required and Optional Terms

Required Terms The following terms **must** appear in a Business Associate Agreement ("BAA").		
Regulatory Requirements	**Notes**	**Check-off**
164.502(e)(1)(i): **Basic Principle**: A Covered Entity ("CE") may disclose Protected Health Information ("PHI") to a business associate ("BA") and may allow a business associate to create, receive, maintain or transmit PHI on its behalf so long as a BAA is in place.		
164.504(e)(2):	**Notes**	**Check-off**
(i) **Identify – By Listing or Referring to Services Agreement:** Establish the permitted and required uses and disclosures of PHI by the BA.		
BA Can't do what CE Can't do: The contract may not authorize the BA to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the CE, except for the optional management/administration and data aggregation provisions listed in the "Optional Terms" section of this checklist.		
(ii) Provide that the BA will:	**Notes**	**Check-off**
(A) **Use/Disclose:** Not use or further disclose the information other than as permitted or required by the contract or as required by law.		
(B) **Safeguards:** Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule (Subpart C of 45 C.F.R. Part 164) with respect to Electronic PHI, to prevent use/disclosure of information other than as provided for by the BAA.		
(C) **Reports/Breach:** Report to the CE any use or disclosure of the information not provided for by its contract, or any Security Incident, of which it becomes aware, or any Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410.		
(D) **Subcontractors**: Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the BA agree in writing to the same restrictions and conditions that apply to the BA with respect to such information.		
(E) **Access**: Make available PHI in accordance with § 164.524;		
(F) **Amendments**: Make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526;		
(G) **Accounting**: Make available the information required to provide an accounting of disclosures in accordance with § 164.528;		
Accounting: Track information needed for an accounting.		
(H) **Privacy Rule.** To the extent BA is to carry out any of CE's obligations under the Privacy Rule, comply with the requirements of the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) that apply to CE in the performance of such obligations.		
(I) **Records**: Make its internal practices, books, and records relating to		

Required Terms The following terms **must** appear in a Business Associate Agreement ("BAA").		
Regulatory Requirements	**Notes**	**Check-off**
the use and disclosure of PHI received from, or created or received by the BA on behalf of, the CE available to the Secretary for purposes of determining the CE's compliance with the Privacy Rule;		
(J) **Return/Destroy**: At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by BA on behalf of, the CE that the BA still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.		
Termination Provision: Authorize termination of the contract by the CE, if the CE determines that the BA has violated a material term of the contract.		

Optional Terms The following terms often appear, but are not required to be in, a BAA. Their inclusion is often a matter of negotiating power and/or leverage between the CE and BA.		
Term	**Notes**	**Check-off**
Mgmt/Admin of BA: The contract may permit the BA to use and disclose PHI for the proper management and administration of the BA: **USE** if necessary: (A) For the proper management and administration of the BA; or (B) To carry out the legal responsibilities of the BA. **DISCLOSE** if (A) The disclosure is required by law; or (B)(1) The BA obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and (2) The person notifies the BA of any instances of which it is aware in which the confidentiality of the information has been breached.		
Data Aggregation: The contract may permit the BA to provide data aggregation services relating to the health care operations of the CE.		
"Suspected Breaches": Requirement that BA inform CE of a "suspected" Breach of Unsecured PHI and permit CE to engage in breach analysis.		
Broader Uses/Disclosures: Any permitted uses or disclosures of PHI that are broader than those listed in the Checklist above as "Required Terms." This may include, for example, permitting the use or disclosure of PHI for marketing, fundraising, de-identification, limited data sets or research purposes. The BA is not permitted to engage in these activities unless the CE has given BA permission to do so.		
More Specific Restrictions: Provisions specifically addressing BA's		

Optional Terms The following terms often appear, but are not required to be in, a BAA. Their inclusion is often a matter of negotiating power and/or leverage between the CE and BA.		
Term	**Notes**	**Check-off**
obligations under HIPAA with respect to marketing, fundraising, adhering to restrictions on disclosures, selling PHI, minimum necessary policies and procedures and other restrictions that apply to BA regardless of whether they are mentioned in the BAA.		
Indemnification: Indemnification provisions (one-way or mutual).		
Insurance: Insurance by BA to protect CE against BA's violations.		
Third Party Beneficiaries: Third party beneficiaries created or prohibited.		
Assignment: Assignment prohibited or permitted.		
Audits: Provisions obligating BA to allow CE to engage in periodic audits or inspections of the BA		
Penalties; Injunctions: Imposition of penalties in the event of a breach or unauthorized disclosure of PHI by BA, such as liquidated damages, or provisions establishing specific performance/equitable relief for CE in event of a violation.		
Representations: Warranties and representations that BA complies with HIPAA Security Rule and applicable provisions of Privacy Rule.		
HITECH Amendments: Commitment by BA to comply with HITECH-based regulatory changes to HIPAA provisions in the future.		
Workforce: Agreement by BA that its workforce will comply with applicable HIPAA provisions.		
Mitigation: Requirement that BA mitigate any harmful effects of impermissible use/disclosure.		
Restrictions on Subcontractors: As an alternative to the "Subcontractors" provision in the "Required Terms" section above, CEs may prohibit BAs from using subcontractors altogether or may attempt to require BA to use a particular form of Subcontractor BAA with subcontractors. CEs may prohibit BA from using subcontractors that are outside of the U.S. or not subject to jurisdiction in U.S. courts.		
Notifications: Provisions under which CE informs BA about: (1) CE's notice of privacy practices; (2) revocation of permission by an individual that affects BA's ability to use or disclose PHI; and (3) any restrictions on use or disclosure of PHI to which CE agrees and that affect BA's activities.		
Definitions: Section of BAA setting forth defined terms; provided, however, that careful review is warranted if it appears BAA is using definitions that are different than those found in HIPAA.		

[GPM Note: this Business Associate Agreement ("BAA") is written from the perspective of the Covered Entity ("CE"). Throughout the document, you will find drafter's notes "[GPM Notes]" for the CE to consider in making decisions about important issues governing the CE's relationship with the Business Associate ("BA"). Options for various provisions, and suggested language (*in bold italics)*, is also included where appropriate. Most of the options relate to a key decision that the CE will need to make—deciding how much control it wants to have over the activities of the BA. The more control exercised by the CE over the BA's conduct, the more likely it is that regulators could assert that CE should be liable for the BA's violations on the theory that BA is CE's "agent". The advantage in having control, however, is that the CE will be more likely to know if the BA is acting in accordance with HIPAA and better positioned to address the BA's noncompliance before a major problem ensues. In addition, the standard articulated by regulators for deciding whether the CE should be liable is not precise, so there is always some risk that regulators would seek to take the position that CE should be liable for the BA's violations, notwithstanding the manner in which the BAA is drafted].

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made and effective _____ ("Effective Date") by and between _____ (the "Covered Entity") and _____ (the "Business Associate") (each a "Party" and collectively the "Parties").

RECITALS

A. Pursuant to Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, ("HIPAA"), the Department of Health and Human Services ("HHS") has issued regulations at 45 C.F.R. Parts 160 and 164 (the HIPAA Security Rule, the HIPAA Privacy Rule, the HIPAA Enforcement Rule and the HIPAA Breach Notification Rule, referred to collectively herein as the "Regulations") to protect the security, confidentiality and integrity of health information.

B. The Parties have entered into an engagement whereby Business Associate will provide certain services to Covered Entity (the "Engagement"), and, pursuant to such Engagement, Business Associate may be considered a "business associate" of Covered Entity as defined in the Regulations.

NOW, THEREFORE, in consideration of the mutual covenants herein contained, the Parties agree to the provisions of this Agreement in order to comply with the Regulations.

I. Definitions

The following terms are defined as set forth below. Any terms used but not otherwise defined in this Agreement have the definitions set forth in the Regulations and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005, and any regulations promulgated thereunder. **[GPM note: HIPAA does not require a list of defined terms to be in the BAA. Their inclusion below is intended to reflect issues of high sensitivity with the goal of making sure that BAs are aware of some of their more significant obligations under HIPAA].**

a. "Breach" shall have the meaning set forth in 45 C.F.R. § 164.402.

b. "Designated Record Set" shall have the meaning set forth in 45 C.F.R. § 164.501 and shall include, but not be limited to, medical records and billing records about Individuals.

c. "Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103.

d. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

e. "Protected Health Information" or "PHI" means, subject to the definition provided at 45 C.F.R. § 160.103, individually identifiable health information that Business Associate receives from Covered Entity or creates, receives, transmits or maintains on behalf of Covered Entity for purposes of performing the services under the Engagement. Unless otherwise stated in this Agreement, any provision, restriction or obligation in this Agreement related to the use of PHI shall apply equally to EPHI.

f. "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

g. "Secretary" shall mean the Secretary of the Department of Health and Human Services or their designee.

h. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with the system operations in an information system. Notwithstanding the foregoing, the Parties acknowledge and agree that "Business Associate need not report all attempted but unsuccessful Security Incidents to Covered Entity, and that this Agreement constitutes notice to Covered Entity that such unsuccessful Security Incidents occur periodically. Unsuccessful Security Incidents include, but are not limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as such incidents do not result in actual unauthorized access, use, or disclosure of PHI.

i. "Subcontractor" means a person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.

j. "Unsecured PHI" shall have the same meaning as the term "Unsecured PHI" in 45 C.F.R. § 164.402.

Business Associate acknowledges and agrees that all PHI that is created or received by Covered Entity and disclosed or made available in any form by Covered Entity to Business Associate, or is created, received, maintained or transmitted by Business Associate on Covered Entity's behalf, will be subject to this Agreement. This Agreement will commence upon the

Effective Date and will continue as long as Business Associate has use, custody or access to PHI subject to this Agreement, and thereafter for the period required by the Regulations.

II. Obligations and Activities of Business Associate

a. Use and Disclosure. Business Associate will not use or further disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate will not use or disclose PHI in a manner that would violate the Regulations if done by Covered Entity.

b. Restrictions on Disclosures. Business Associate will comply with any requests for restrictions on certain disclosures of PHI, to which Covered Entity has agreed and of which Business Associate is notified by Covered Entity. In addition, Business Associate will permit an Individual to make a reasonable request that PHI relating to the Individual be supplied at alternative locations and/or by alternative means, or to make a request for restriction of the use and/or disclosure of PHI in accordance with 45 C.F.R. § 164.522, and Business Associate will provide notice of such requests to Covered Entity within ***[five (5)] [seven (7)]*** days. Business Associate agrees to comply with the requirements of 45 C.F.R. § 164.522(a)(vi) regarding requests for restriction on the disclosure of PHI to health plans for payment and health care operations purposes. Business Associate is prohibited from agreeing to any restriction on the use or disclosure of PHI or any alternative communication of PHI requested by an Individual without Covered Entity's prior written approval.

c. Sale of PHI; Marketing; Fundraising; Research. Business Associate will not, except for payments from Covered Entity for services performed pursuant to this Agreement or the Engagement, directly or indirectly receive remuneration, financial or otherwise, from or on behalf of the recipient in exchange for PHI. Business Associate will not use or disclose PHI for research or engage in any uses or disclosures that might be classified as marketing or fundraising without first obtaining prior written approval from Covered Entity.

d. Minimum Necessary. **[GPM Note: Under HITECH, the minimum necessary standard applies directly to BAs, which means BAs will be liable for their violations of this rule. We nonetheless recommend that CEs specify BA's obligation to comply with the minimum necessary rule in the BAA itself because that is most protective of the CE. We have included 2 options for addressing this: (1) CEs permitting the BA to follow its own policies on minimum necessary; or (2) requiring the BA to comply with the CE's policy on minimum necessary. The advantage of option 2 is that it affords the CE more oversight of the BA's activities. The disadvantage is that this added control makes it more likely the CE could be liable for BA's conduct. If option 2 is selected, the CE will need to ensure that BA has copies of its minimum necessary policies]. [Option 1]:** ***[Business Associate and Subcontractors, if any, will only request, use and disclose the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure.]*** **[Option 2]** ***[Business Associate will comply, and will ensure that its Subcontractors comply, with the Covered Entity's policies and procedures on the minimum necessary rule, a copy of which is attached hereto and incorporated herein as Exhibit ___].*** Business Associate agrees, and it will ensure that

its Subcontractors agree, to comply with Section 13405(b) of HITECH, any regulations issued thereunder or any guidance from the Secretary regarding what constitutes the definition of minimum necessary.

e. HIPAA Security Rule. Business Associate will develop, implement, maintain and use appropriate safeguards, and comply with the Security Rule at Subpart C of 45 C.F.R. Part 164, with respect to EPHI, to prevent use or disclosure of the PHI other than as provided for by this Agreement.

f. HIPAA Privacy Rule . Business Associate will comply with all requirements of the Privacy Rule at Subpart E of 45 C.F.R. Part 164 that apply to business associates.

g. Mitigation. Business Associate will mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

[GPM Note: the Omnibus rule obligates CEs to ensure that BAs enter into "subcontractor BAAs" with any "subcontractors". These subcontractor BAAs must obligate the subcontractor to comply with the same terms/conditions of the BAA between CE and BA, and must be at least as restrictive as that BAA (i.e., the subcontractor cannot be given greater rights to use and disclose PHI than those held by the BA itself).

We have included several options for addressing a BA's use of subcontractors. Option 1 (most protective of CE) prohibits the BA from using any subcontractors that will see PHI without first securing permission from the CE and, if CE agrees, using a form subcontractor BAA (attached as an exhibit). The advantage of this is that the CE will be able to control what the BA does with its PHI. The disadvantage is that BAs may push back on this obligation as overly burdensome. Option 2 permits using subcontractors, but obligates the BA to use a particular form of subcontractor BAA (attached as an exhibit). The advantage of this is that it is less onerous for the BA than option 1, while still affording CE some control over the BA's subcontractor relationships. The disadvantage is that the more control the CE has, the more likely the CE could be found liable for the BA's violations of HIPAA. Option 3 is the least restrictive because it obligates the BA to do only what is required under HIPAA. For all 3 options, we would recommend that the CE be thoughtful about BA's ability to send the CE's PHI to subcontractors outside of the U.S. without the CE first granting permission. This item is not specifically addressed in option 1 (because the CE has approval rights over subcontractors anyway). Options 2 and 3 indicate that offshoring is either prohibited unless CE approves or permitted if BA enters into subcontractor agreement with U.S. affiliate of offshore contractor. This is to make sure that regulators are not placed in a position where they feel they need to impose penalties against the CE (because of something an offshore party, not subject to U.S. jurisdiction, did) on the theory that CE didn't take steps to do anything about PHI leaving U.S. jurisdiction. The more protective option for the CE is to not permit offshoring without first granting permission to the BA.

Finally, where a CE will permit the BA to use subcontractors, the CE might also consider requiring that it be designated as a third party beneficiary in the BA's subcontractor BAA with the subcontractor. This would permit it to enforce the terms of that subcontractor BAA directly against the subcontractor. We have this provision as an option in Section VII(e) of the subcontractor BAA included as Exhibit A.]

[Option 1—most restrictive; delete options 2 and 3 if used]

h. Subcontractors. Business Associate will not permit any Subcontractor to create, receive, maintain or transmit PHI on behalf of Business Associate without first securing prior written approval from Covered Entity, which approval shall not be unreasonably withheld. Business Associate will provide Covered Entity with at least ***[five (5) days] [ten (10) days] [thirty (30) days]*** prior written notice of its desire to use a Subcontractor. Covered Entity will grant or deny permission within ***[five (5) days] [ten (10) days] [thirty (30) days]*** of a request from Business Associate. Business Associate agrees that if Covered Entity does not respond within that time frame, that this lack of response shall constitute a denial by Covered Entity of Business Associate's request. In the event Covered Entity agrees to Business Associate's request, Business Associate agrees that it is only permitted to use a Subcontractor to create, receive, maintain or transmit PHI on behalf of Business Associate if the Subcontractor and Business Associate execute the "Subcontractor Business Associate Agreement" attached hereto as Exhibit A. The Subcontractor Business Associate Agreement obligates the Subcontractor to comply with the same restrictions, conditions and requirements outlined in this Agreement that apply to Business Associate with respect to such PHI.

[Option 2—compromise; delete options 1 and 3 if used]

i. Subcontractors. Business Associate will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate, agrees in writing to the "Subcontractor Business Associate Agreement" attached hereto as Exhibit A. The Subcontractor Business Associate Agreement obligates the Subcontractor to comply with the same restrictions, conditions and requirements outlined in this Agreement that apply to Business Associate with respect to such PHI. Business Associate agrees that if a Subcontractor refuses to enter into the "Subcontractor Business Associate Agreement" attached hereto as Exhibit A, that Business Associate will not permit that Subcontractor to create, receive, maintain or transmit any PHI. Notwithstanding anything else in this Agreement that may be construed to the contrary, Business Associate agrees that it **[Option A]:** ***[will not permit any Subcontractor that is located outside of the United States to create, receive, maintain or transmit any PHI, without first securing prior written approval from Covered Entity.]*** **[Option B]:** ***[will permit a party that is located outside of the United States to create, receive, maintain or transmit PHI only if an affiliate of that party, located in the United States and subject to jurisdiction in the courts of the United States, is the Subcontractor with which Business Associate has entered into the Subcontractor Business Associate Agreement].***

[Option 3—least restrictive; delete options 1 and 2 if used]

j. Subcontractors. In accordance with the requirements of the Regulations, Business Associate will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions, requirements and conditions that apply to Business Associate with respect to that PHI, including the provisions outlined in this Agreement. Notwithstanding anything else in this Agreement that may be construed to the contrary, Business Associate agrees that it **[Option A]:** ***[will not permit any subcontractor that is located outside of the United States to create, receive, maintain or transmit any PHI, without first securing prior written approval from Covered Entity.]*** **[Option B]:** ***[will permit a party that is located outside of the United States to create, receive, maintain or transmit PHI only if an affiliate of that party, located in the United States and subject to jurisdiction in the courts of the United States, is the Subcontractor with which Business Associate has entered into a written agreement under which that Subcontractor agrees to the same restrictions, requirements and conditions that apply to Business Associate with respect to that PHI].***

k. Reports of Impermissible Use or Disclosure of PHI; Security Incident. Business Associate will report to Covered Entity any use or disclosure of PHI not provided for or permitted by this Agreement of which it becomes aware, or any Security Incident of EPHI of which it becomes aware, **[GPM note: there is no defined period under HIPAA by which BAs must provide this notice. However, because any "use" or "disclosure" of PHI not permitted under the BAA potentially could become a "Breach" of Unsecured PHI, a specific notice period (relatively short) should be used]** within ***[two (2) days] [three (3) days]*** of the date on which Business Associate first discovers the use, disclosure or Security Incident. In addition to its other obligations under this Agreement, Business Associate will take prompt action to correct any Security Incident or use or disclosure of PHI not permitted under this Agreement and any action pertaining to such Security Incident or unauthorized use or disclosure as required by applicable federal or state laws and regulations. **[GPM Note: if CE wants notification to go to someone at CE who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to its Privacy Officer but less pressing contract issues to go to the contracting department), CE can designate a specific contact to receive notification from BA]. [Option A]** ***[Business Associate will provide notification to _____ at Covered Entity.]*** **[Option B]** ***[Business Associate will provide notification to the Covered Entity official designated in Section VIII(c) of this Agreement.]***

[GPM Note: the next 2 sections are options for addressing HIPAA breaches. Option 1 permits the BA to do the analysis of whether a breach has occurred and then provide notice to the CE within a defined period. Option 2 obligates the BA to inform the CE of any "suspected breach" (within a defined period) but allows the CE to do the analysis if whether what has occurred actually gives rise to a breach. The advantage of Option 2 is that CE has control over this determination, which may be helpful because of the "presumption" of breach created under the Omnibus rule. The disadvantage of Option 2 is that it likely means a principal-agency relationship exists and potentially could result in CE being liable for conduct of the BA that violates HIPAA].

[Option 1—if selected, delete option 2]

l. Breaches of Unsecured PHI. Business Associate will report to Covered Entity any Breach of Unsecured PHI by Business Associate or any of its officers, directors, employees, Subcontractors or agents. **[GPM Note: if CE wants breach notification to go to someone at CE who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to its Privacy Officer but less pressing contract issues to go to the contracting department), CE can designate a specific contact to receive breach notification from BA. Otherwise notice can go to the general notice point for contracting issues]. [Option A]** ***[All notifications of Breach of Unsecured PHI will be made by Business Associate to _____ at Covered Entity.]*** **[Option B]** ***All notifications of Breach of Unsecured PHI will be made by Business Associate to the Covered Entity official designated in Section VIII(c) of this Agreement].*** **[GPM Note: CE has discretion to require a specific notice period and should make decision about appropriate timeframe within context of HIPAA breach notification standard of providing notice to individuals as soon as possible, but no later than 60 days after discovering breach. We would not generally recommend that the BA have longer than 5 days to provide this notice.]** All notifications required under this Section will be made by Business Associate without unreasonable delay and in no event later than ***[two (2) days] [three (3) days] [five (5) days]*** of discovery. Business Associate will use the standard at 45 C.F.R. § 164.410(a) to determine when the Breach is treated as discovered. All notifications will comply with Business Associate's obligations under, and include the information specified in, 45 C.F.R. § 164.410 and include any other available information that Covered Entity is required to include in its notification to individuals pursuant to 45 C.F.R. § 164.404(c). In the event of a Breach that is caused by the acts or omissions of Business Associate, its Subcontractors, officers, directors, employees or agents, Business Associate will cooperate with Covered Entity to notify, **[GPM Note: CE should consider whether to require BA to cover costs of notification due to a breach caused by BA]** ***[at Business Associate's expense]***, (i) individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate or Covered Entity to have been, accessed, acquired, used or disclosed, and (ii) the media, as required pursuant to 45 C.F.R. § 164.406, if the legal requirements for media notification are triggered by the circumstances of such Breach. **[GPM Note: following sentence relates to whether CE wants BA to be responsible for costs of notification of breach caused by BA. If not, this sentence can be deleted].** ***[Business Associate will indemnify Covered Entity for any reasonable expenses Covered Entity incurs in notifying individuals, the media and related expenses arising from a Breach, or costs of mitigation related thereto, caused by Business Associate or its officers, directors, employees, Subcontractors or agents.]*** Business Associate will cooperate in Covered Entity's Breach analysis process and procedures, if requested. Covered Entity will at all times have the final decision about the content of any notification required to be given under the Regulations.

[Option 2—if selected, delete option 1]

m. Breach of Unsecured PHI. Business Associate will report to Covered Entity any suspected Breach of Unsecured PHI by Business Associate or any of its officers, directors, employees, Subcontractors or agents. **[GPM Note: if CE wants breach notification to go to someone at CE who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to its Privacy Officer**

but less pressing contract issues to go to the contracting department), CE can designate a specific contact to receive breach notification from BA. Otherwise notice can go to the general notice point for contracting issues]. [Option A] ***[All notifications of Breach of Unsecured PHI will be made by Business Associate to _____ at Covered Entity.]*** **[Option B]** ***All notifications of Breach of Unsecured PHI will be made by Business Associate to the Covered Entity official designated in Section VIII(c) of this Agreement]*** All notifications required under this Section will be made by Business Associate without unreasonable delay and in no event later than ***[one (1) day] [two (2) days]*** of discovery. **[GPM Note: if CE will do breach analysis itself, CE should require very short notice period so that it can begin analysis quickly]**. Business Associate will use the standard at 45 C.F.R. § 164.410(a) to determine when the suspected Breach is treated as discovered. Covered Entity shall have discretion to determine whether a suspected Breach has given rise to a Breach. Business Associate will cooperate with Covered Entity and provide such information as Covered Entity reasonably requires in making this determination. In notifying Covered Entity of a suspected Breach, Business Associate will provide, to the extent reasonably possible, as much of the information it has that would be required in notifying a Covered Entity of a Breach, under 45 C.F.R. § 164.410. If Covered Entity determines that a Breach has occurred, Business Associate will provide any other available information that Covered Entity is required to include in its notification to individuals pursuant to 45 C.F.R. § 164.404(c). In the event Covered Entity determines a Breach has occurred that was caused by the acts or omissions of Business Associate, its Subcontractors, officers, directors, employees or agents, Business Associate will cooperate with Covered Entity to notify, **[GPM Note: CE should consider whether to require BA to cover costs of notification due to a breach caused by BA]** ***[at Business Associate's expense]***, (i) individuals whose Unsecured PHI has been, or is reasonably believed by Covered Entity to have been, accessed, acquired, used or disclosed, and (ii) the media, as required pursuant to 45 C.F.R. § 164.406, if the legal requirements for media notification are triggered by the circumstances of such Breach. **[GPM Note: following sentence relates to whether CE wants BA to be responsible for costs of notification. If not, this sentence can be deleted]** ***[Business Associate will indemnify Covered Entity for any reasonable expenses Covered Entity incurs in notifying individuals, the media and related expenses arising from a Breach, or costs of mitigation related thereto, caused by Business Associate or its officers, directors, employees, Subcontractors or agents.]*** Business Associate will cooperate in Covered Entity's Breach analysis process and procedures, if requested. Covered Entity will at all times have the final decision about the content of any notification required to be given under the Regulations.

[GPM Note: we have provided 2 options for the access to records provision. Option 1 affords the CE more control over how the BA acts. The advantage of this is that CE can make sure the BA acts appropriately. The disadvantage is that it is more likely to make CE potentially liable for the acts or omissions of BA. Option 2 gives more discretion to the BA. The advantage is that the CE is less likely to be liable for the BA's acts. The disadvantage is that the principal-agency analysis used by regulators to determine liability is not precise, so there is no guarantee that CE will not be found liable. Also, Option 2 gives more discretion

to the BA, which undermines CE's ability to make sure that BA performs appropriately].

[Option 1—more control for CE; delete option 2 if used]

n. Access . In the event an Individual requests access to PHI in a Designated Record Set from Business Associate, Business Associate will provide Covered Entity with notice of the same within ***[two (2)] [three (3)] [five (5)]*** days. Business Associate will provide access, within ***[two (2)] [three (3)] [five (5)]*** days of a request of Covered Entity and in the manner designated by Covered Entity, to PHI in a Designated Record Set to Covered Entity, or, as directed by Covered Entity, to an Individual or the Individual's designee in order to meet the requirements under 45 C.F.R. § 164.524 (Access). If the PHI that is the subject of a request is maintained by the Business Associate in a Designated Record Set electronically, Business Associate will provide an electronic copy of such information to the Covered Entity, or, as directed by the Covered Entity, to the Individual or the Individual's designee, in the format required by the Regulations and as directed by Covered Entity, in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.524.

[Option 2—more discretion for BA; delete option 1 if used]

o. Access. Business Associate will make available PHI in a Designated Record Set as necessary to satisfy Covered Entity obligations under 45 C.F.R. § 164.524 (access).

[GPM Note: we have provided 2 options for the amendment of records provision. The same comments above on the advantages and disadvantages of the access options apply to the amendment provisions].

[Option 1—more control for CE; delete option 2 if used]

p. Amendment. In the event Business Associate receives a request from an Individual for an amendment to PHI in a Designated Record Set, Business Associate will provide Covered Entity with notice of the same within ***[two (2)] [three (3)] [five (5)]*** days. Business Associate will make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 (Amendment) within ***[two (2)] [three (3)] [five (5)]*** days of a request of Covered Entity or an Individual and in the manner designated by Covered Entity, in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.526. Business Associate will incorporate any amendments to PHI it receives from Covered Entity and will notify Covered Entity of any amended PHI that it receives from third parties relating to Covered Entity's PHI.

[Option 2—more discretion for BA; delete option 1 if used]

q. Amendment. Business Associate will make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526 (Amendment).

[GPM Note: the Omnibus rule did not finalize the HITECH statutory change that will expand individuals' rights to an accounting of disclosures to include

treatment, payment and healthcare operations disclosures. Many objections have been raised with HHS about its 2011 proposed rule on accountings as being overly broad. However, HITECH does still contain the treatment, payment and operations provisions so there will likely be changes to the current HIPAA rules on accountings. Option 1 below is based on the HITECH statutory language, but still may need to be amended when regulations are issued. The advantage of using this provision is that it will provide some protection by addressing the HITECH statutory mandate and may, depending on the scope of the future rulemaking, result in the BAA not requiring further amendment. Other than the HITECH issue, the advantages and disadvantages of these options are the same as with respect to the access and amendment provisions above].

[Option 1—delete option 2 if used]

r. Accounting of Disclosures. Business Associate will document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to fulfill its obligations under the Regulations, including, but not limited to, responding to a request by an Individual for an accounting of disclosures in accordance with 45 C.F.R. § 164.528, and will provide such information to Covered Entity or an Individual, in the time and manner designated by Covered Entity. Except in the case of a direct request from an Individual for an accounting related to treatment, payment or healthcare operations disclosures through an electronic health record, if the request for an accounting is delivered directly to Business Associate or its agents or Subcontractors, Business Associate will, within five (5) days of a request, notify Covered Entity of the request. Covered Entity will either inform Business Associate to provide such information directly to the Individual, or it will request the information to be immediately forwarded to Covered Entity for compilation and distribution to such Individual, and Business Associate will provide such information in its possession within ten (10) days of Covered Entity's request. In the case of a direct request for an accounting from an Individual related to treatment, payment or healthcare operations disclosures through electronic health records, Business Associate will provide such accounting to the Individual in accordance with Section 13405(c) of HITECH and such regulations as are adopted thereunder. Covered Entity and Business Associate agree that the provisions of this section related to accounting of disclosures for treatment, payment and healthcare operations purposes from an electronic health record will only be effective as of such date such accountings of disclosures are required under HITECH. Business Associate and any agent or Subcontractors will maintain the information required for purposes of complying with this section for such period of time as is required under the Regulations and HITECH.

[Option 2—delete Option 1 if used]

s. Accounting of Disclosures. Business Associate will maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. § 164.528 (accountings).

t. Covered Entity's Obligations Under Privacy Rule. To the extent that Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E

of 45 C.F.R. Part 164, Business Associate will comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

u. Records. Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Covered Entity or to the Secretary for purposes of determining Covered Entity's compliance with the Regulations. Business Associate will notify Covered Entity regarding any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary, and upon request by Covered Entity, shall provide Covered Entity with a duplicate copy of such PHI.

[GPM Note: the following provision is optional. The CE may want to have audit/inspection rights over the BA so that the CE can judge whether BA is complying with HIPAA. The advantage of this is that oversight exercised by the CE is likely to help the CE prevent the BA from acting negligently. In addition, given the sensitivity of privacy issues, it may be the case that regulators will view a CE who does not require auditing in its BAAs as itself acting negligently. The disadvantage is that the auditing/inspection power is likely to give rise to a principal-agent relationship such that the CE can be liable for the BA's violations. If audit language will be part of the BAA, there are a range of operational issues that will need to be addressed, including how much notice is required; who conducts the audit; how the parties will address costs; and any limitations on scope of the audit. Bracketed language addressing all of these operational items is included in the provision below.]

[Option—audits; delete if not intended to be part of BAA].

v. Inspections; Audits . Within ***[three (3)] [five (5)] [ten (10)]*** days of a written request by Covered Entity, Business Associate will allow ***[Covered Entity] [a third party mutually agreed to by Covered Entity and Business Associate]*** to conduct a reasonable inspection of the policies and procedures, agreements, facilities, books, records and systems relating to the use or disclosure of PHI pursuant to this Agreement for the purpose of determining whether Business Associate has complied with this Agreement and the requirements of the Regulations; provided, however, that Covered Entity will protect the confidentiality of all proprietary information of Business Associate to which Covered Entity has access during the course of such inspection ***[and Business Associate and Covered Entity will mutually agree in advance upon the scope and location of such an inspection]***. The costs of the audit will be ***[covered by Covered Entity in the event the audit determines that Business Associate is in compliance with this Agreement and the Regulations and covered by Business Associate in the event the audit determines that Business Associate has violated this Agreement or the Regulations] [borne equally between the Parties]***. Covered Entity is permitted to engage in the inspections and audits set forth in this Section ***[as Covered Entity reasonably determines to be appropriate] [no more often than one time during each calendar year during which this Agreement is in effect].***

w. Workforce. Business Associate will ensure that its workforce members, employees and agents are aware of and agree to the same restrictions which apply to Business Associate with respect to the PHI.

x. Compliance with HITECH. Business Associate will comply with all requirements of Title XIII, Subtitle D of HITECH which are applicable to business associates, and will comply with all regulations issued by the Secretary to implement these referenced statutes, as of the date by which business associates are required to comply with such referenced statutes and regulations.

III. Permitted Uses and Disclosures by Business Associate

[GPM Note: the uses/disclosures in which the BA is permitted to engage will need to be tailored to the specific facts of the relationship. The CE should limit the permitted uses/disclosures to whatever is necessary for the relationship. The uses/disclosures that are generally found in BAAs are set forth immediately below, followed by several other uses/disclosures that may be relevant. If these other uses/disclosures are not relevant to your relationship, they should be deleted.]

a. Required by Law. Business Associate may use or disclose PHI as Required by Law.

[GPM Note: the BA should be given the rights to either (1) use/disclose PHI for a list of specific purposes; or (2) use/disclose PHI to carry out the Engagement. The advantage of Option 1 is that it gives the CE more control over how its PHI is used/disclosed. The disadvantage is that it requires drafting a specific list for each BAA. The advantage of Option 2 is that is less work intensive, while still compliant with HIPAA.]

[Option 1—specific purposes. If this is selected, CE will need to include a list of specific purposes for which the BA can use/disclose PHI. If this is selected, delete option 2].

b. Specific Purposes. Business Associate may only use or disclose PHI for the following specific purposes: **[GPM Note: list will need to be included].**

[Option 2—to carry out the Engagement. If this is selected, delete option 1.]

c. To Carry Out Engagement. Except as otherwise limited in this Agreement, for purposes of the services provided as part of the Engagement, Business Associate may use or disclose PHI solely to perform functions, activities, or services for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Regulations if done by Covered Entity.

[GPM Note: the following provision is optional under HIPAA. BAs are likely to seek its inclusion, however, because it is helpful for their internal operations. It is generally reasonable for the BA to have these rights. Delete if not intended to be part of the BAA].

d. Management and Administration. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, as provided in 45 C.F.R. § 164.504(e)(4). In addition, Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry

out the legal responsibilities of Business Associate, provided that such disclosures are Required by Law or Business Associate obtains, prior to the disclosure, reasonable assurances from the person to whom it is disclosed that such PHI will be held secure and confidential as provided pursuant to this Agreement and only disclosed as Required by Law or for the purposes for which it was disclosed to the third party, and that any breaches of confidentiality of the PHI which becomes known to such third party will be immediately reported to Business Associate.

[GPM Note: there are a range of other uses/disclosures that may be appropriate for a BAA, depending on the scope of the relationship. We have included several below. <u>If CE does not want these these additional uses to be part of the relationship, they should not be included in the BAA.</u> We have not included certain other uses/disclosures that arise from time to time in BAAs (such as fundraising, research, limited data sets or marketing) because those activities typically require additional review by counsel].

[Option—Data Aggregation (combining PHI from different CEs for analytical purposes). Delete if not intended to be part of the BAA].

e. <u>Data Aggregation.</u> Business Associate may use PHI to provide data aggregation services related to the health care operations of the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

[Option—De-Identified Information (note that PHI that is de-identified is no longer subject to HIPAA. This information can have proprietary value, and because de-identified information is not subject to HIPAA, can be freely bought and sold. CE should consider ownership/control issues over this information if it permits the BA to engage in de-identification). Delete if not intended to be part of the BAA].

f. <u>De-Identification.</u> Business Associate may use PHI to create information that is de-identified. Any such de-identification by Business Associate will be done in compliance with 45 C.F.R. § 164.514(b). **[GPM Note: CE will need to address ownership of de-identified information. Option 1 keeps it with CE and Option 2 gives ownership to BA. Note that this is not a HIPAA issue because once it is de-identified, the information is no longer subject to HIPAA]. [Option 1]: *[Business Associate agrees that de-identified information remains the sole property of Covered Entity and may only be used and disclosed by Business Associate on behalf of Covered Entity and pursuant to the Engagement].* [Option 2]*: [Covered Entity agrees that de-identified information may be used and disclosed on Business Associate's own behalf. Covered Entity agrees that any de-identified information is and will remain the sole property of Business Associate and, due to the regulatory treatment of de-identified information, is no longer PHI and not subject to this Agreement or the Regulations.]***

IV. <u>Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions</u>

[GPM Note: the following provisions are all optional. Their inclusion is generally recommended].

a. Notice of Privacy Practices. Covered Entity will provide Business Associate, upon request, with Covered Entity's Notice of Privacy Practices in effect at the time of the request.

b. Revocation of Permission. Covered Entity will provide Business Associate with any changes in or revocation of permission by an Individual to use or disclose PHI to the extent such changes may affect Business Associate's permitted or required uses and disclosures.

c. Restrictions on Use and Disclosure. Covered Entity will notify Business Associate of any material restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent such restrictions may affect Business Associate's use and disclosure of PHI.

V. Obligations of the Covered Entity

Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Regulations if done by Covered Entity.

VI. Termination

a. Termination for Cause by Covered Entity. Notwithstanding any contrary termination provision of any other agreement between the Parties, Covered Entity is authorized to terminate this Agreement and the Engagement as described in this Section if Covered Entity determines that Business Associate has violated a material term of this Agreement. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity will provide written notice of such breach to Business Associate and provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity, then Covered Entity may immediately terminate this Agreement; or Covered Entity may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and Covered Entity determines that cure is not possible.

b. Effect of Termination.

1. Except as provided in paragraph 2 of this section, upon termination of the Engagement, Business Associate will return or destroy all PHI received from Covered Entity or created, received, maintained or transmitted by Business Associate on behalf of Covered Entity. This provision will apply to PHI that is in the possession of Subcontractors of Business Associate and Business Associate will ensure compliance with this requirement by its Subcontractors. Neither Business Associate not Subcontractors will retain any copies of PHI.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate will provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement

of the Parties that return or destruction of PHI is infeasible, Business Associate will extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible for so long as Business Associate maintains such PHI. **[GPM Note: BAs will sometimes want unilateral power to determine whether return or destruction of PHI is not feasible. CEs should push back against that restriction].**

VII. Indemnification

[GPM Note: indemnification is not required by HIPAA. However, given the heightened penalties for HIPAA violations under HITECH, CEs should strongly consider its inclusion. BAs may want mutual indemnification commitments. CEs might argue against that on the theory that there is far less that a CE can do to harm a BA as compared to what the BA can do to harm the CE.]

Business Associate will defend, hold harmless and indemnify Covered Entity against any and all claims, liabilities, damages, judgments, costs and expenses (including reasonable attorney's fees and costs) asserted against, imposed upon or incurred by Covered Entity that arises out of, or in connection with, Business Associate's default under or failure to perform any contractual or other obligation, commitment or undertaking under this Agreement, or the negligence of Business Associate or its Subcontractors, employees, agents, or representatives in the discharge of its or their responsibilities, or any other act or omission of Business Associate or its Subcontractors, employees, agents or representatives. This provision will survive termination of the Agreement with respect to any claim, action, or proceeding by a third party that relates to acts or omissions occurring during the term of this Agreement.

VIII. Miscellaneous

a. Survival. The respective rights and obligations of Business Associate and Covered Entity under Sections II, VI, VII, and VIII of this Agreement will survive the termination of this Agreement.

[GPM Note: CE may seek to require that BA has insurance coverage that will protect CE from BA's violations of the BAA/HIPAA, to the greatest extent possible. BAs may push back on this because its existing insurance may not cover HIPAA issues and it may not want to acquire additional insurance. Note that the $1 million/$3 million amounts in the provision below reflect what is often seen in health care services agreement, but could be made higher or lower as agreed upon by the parties. If insurance will not be part of the BAA, the below provision should be deleted].

b. Insurance. Business Associate will maintain insurance in the minimum amounts of $1,000,000 per occurrence and $3,000,000 annual aggregate covering the acts and omissions of Business Associate under this Agreement. Business Associate will ensure that Covered Entity is named an additional insured under this insurance policy. Business Associate will provide Covered Entity with proof of such insurance upon request. Business Associate will notify Covered Entity no later than ten (10) days of any actual or threatened claim, action, or proceeding related to activities undertaken

pursuant to this Agreement and will cooperate in all respects with Covered Entity in the defense of any such claim, action, or proceeding. Business Associate will provide Covered Entity with notice within ten (10) days of any cancellation, termination or material alteration of any such insurance policies. Prior to the expiration or cancellation of any such policies, Business Associate will secure replacement of such insurance coverage upon the same terms and will furnish Covered Entity with a certificate of insurance. Failure of Business Associate to secure replacement coverage in the event of such cancellation, termination or material alteration of any such insurance policies will be a default hereunder, and Covered Entity will have the option to terminate this Agreement pursuant to Section VI.

c. Notification. Except as otherwise agreed to in this Agreement, any notice required or permitted under this Agreement will be given in writing and delivered personally or sent by certified mail, return receipt requested, or by reputable overnight delivery service, such as Federal Express, to the following addresses:

Covered Entity	Business Associate
_____	_____
_____	_____
_____	_____
_____	_____

Such addresses may be changed by either Party by written advice as to the new address given as above provided.

d. Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the Regulations, and HITECH. In the event of any inconsistency between the provisions of this Agreement, the Engagement and the Regulations, the Regulations will control.

e. No Third Party Beneficiaries. This Agreement is intended for the sole benefit of the Business Associate and Covered Entity and does not create any third party beneficiary rights.

f. Waiver. No waiver or discharge of any liability or obligation hereunder by Covered Entity on any one or more occasions will be deemed a waiver of any continuing or other liabilities or obligations; nor will they prohibit enforcement by Covered Entity of any liabilities or obligations on any other occasions.

g. Unenforceability. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event Covered Entity believes in good faith that any provision of the Agreement fails to comply with the then-current requirements of HIPAA, the Regulations, and other applicable law, including but not limited to HITECH and all regulations promulgated thereunder, Covered Entity will notify Business Associate in writing. For a period of

up to thirty (30) days, the Parties will address in good faith such concern and will amend the terms of this Agreement if necessary to bring it into compliance. If after such thirty (30) day period Covered Entity believes that this Agreement fails to comply with HIPAA, the Regulations, and other applicable law, including but not limited to HITECH and all regulations promulgated thereunder, then Covered Entity has the right to terminate this Agreement upon written notice to Business Associate.

h. Independent Contractors. Business Associate is not the agent of Covered Entity and Covered Entity does not control, supervise or instruct Business Associates or any Subcontractors. The Parties are independent contractors and nothing in this Agreement will be deemed to make them partners or joint venturers or make Business Associate an agent of Covered Entity.

i. No Assignment. Business Associate may not assign its rights, nor may it delegate any of its obligations, under this Agreement, without the express written consent of Covered Entity.

j. Entire Agreement. This Agreement is the entire agreement of the Parties related to its subject matter and supersedes all prior agreements between the Parties that were designated or qualified as business associate agreements and replaces all previous drafts, understandings and communications.

[GPM Note: the following provision ("Subcontractors") is optional and should only be used if CE is going to require the BA to use a particular form for its subcontractor BAAs, pursuant to the options outlined at Sections II(h), (i) and (j) above.]

k. Subcontractors. Business Associate agrees that any Subcontractors will be required to enter into the attached Subcontractor Business Associate Agreement prior to that Subcontractor creating, receiving, maintaining, transmitting, using or disclosing the PHI.

l. Remedies. Business Associate acknowledges and agrees that any breach of this Agreement by Business Associate may cause irreparable harm to Covered Entity, the amount of which may be difficult to ascertain. Business Associate agrees that Covered Entity may seek any legal remedy, including injunctive or specific performance for such harm, without bond, security or necessity of demonstrating actual damages. Such right of Covered Entity is in addition to the remedies otherwise available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate.

[GPM Note: CE might seek that BA represent that it complies with certain parts of HIPAA as a way of showing that CE is diligent in focusing on compliance. BA may push back on this because it amounts to an admission that BA understands and complies with everything, which likely gives regulators a rationale for focusing only on BA (and not CE) if that is what the circumstances warrant. In addition, this representation helps undermine the idea that CE should be liable for what BA does because BA is acknowledging that it understands HIPAA and is

in compliance with its requirements. Delete if not intended to be part of the BAA].

m. Representations and Warranties. Business Associate warrants and represents that it is in compliance with the Security Rule and the provisions of the Privacy Rule that apply to Business Associate.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective as of the Effective Date.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
_____	_____
By:_____	By:_____
Title:_____	Title:_____

[GPM Note: this Subcontractor Business Associate Agreement ("BAA") is written from the perspective of the HIPAA Covered Entity ("CE"). The idea is that CE's may require a Business Associate ("BA") that is going to use Subcontractors to enter into a particular form agreement, dictated by the CE. <u>This is not mandatory for CEs; rather, it is a way of ensuring that the BA uses certain provisions that are intended to protect the CE (e.g., insurance, indemnification, timing on breach notification, making CE a third party beneficiary of the Subcontractor BAA, etc.). Another option permitted under HIPAA is to simply permit the BA to contract with subcontractors on its own.</u> Throughout the document, you will find drafter's notes "[GPM Notes]" for the CE to consider in making decisions about important issues governing the relationship. Options and suggested language (*in bold italics)* is also included where appropriate. The <u>most important point</u> about the Subcontractor BAA is that the <u>BA cannot give the Subcontractor rights to use or disclose PHI that are more extensive than what the CE has given the BA in the BAA between the CE and BA</u> (referred to as the "Prime BAA" in this document). Accordingly, if the CE is dictating the terms of the Subcontractor BAA, the CE must ensure that any rights to use or disclose PHI granted by the BA to the Subcontractor under this BAA do not exceed what the CE has granted to the BA under the Prime BAA].

<u>EXHIBIT A</u>

SUBCONTRACTOR BUSINESS ASSOCIATE AGREEMENT

This Subcontractor Business Associate Agreement ("Agreement") is made and effective _____ ("Effective Date"), by and between _____ ("Business Associate") and _____ ("***Prime Subcontractor***") **[GPM Note: we have used the term 'Prime Subcontractor" so that references to the party signing this agreement are distinguishable from references to "subcontractors" with which that party might contract in the future and which would themselves be subject to HIPAA as a BA. It is anticipated that the actual name of the party would be used in lieu of "Prime Subcontractor" in this document.]** (each a "Party" and collectively the "Parties").

RECITALS

A. Pursuant to Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, ("HIPAA"), the Department of Health and Human Services ("HHS") has issued regulations at 45 C.F.R. Parts 160 and 164 (the HIPAA Security Rule, the HIPAA Privacy Rule, the HIPAA Enforcement Rule and the HIPAA Breach Notification Rule, referred to collectively herein as the "Regulations") to protect the security, confidentiality and integrity of health information.

B. Business Associate has been engaged to provide services to certain of its clients who are Covered Entities, as defined by HIPAA.

C. The Regulations obligate Business Associate, as a "business associate" defined by HIPAA to these Covered Entities, to ensure that its agents, including its Subcontractors, that create, receive, maintain or transmit Protected Health Information on behalf of the business associate, agree to the same restrictions and conditions that apply to Business Associate with respect to such Protected Health Information.

D. The Parties have entered into an arrangement whereby Prime Subcontractor will provide certain services, functions or activities to Business Associate related to services Business Associate is performing on behalf of Covered Entities involving Protected Health Information (the "Engagement"), and, as a result, Prime Subcontractor may create, receive, maintain or transmit Protected Health Information on behalf of Business Associate in fulfilling its obligations under the Engagement. As a result, Prime Subcontractor qualifies as a "Subcontractor" and as a business associate under the Regulations.

E. The Parties wish to enter into this Agreement that defines Prime Subcontractor's obligations with respect to Protected Health Information.

NOW, THEREFORE, in consideration of the mutual covenants herein contained, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

I. Definitions

The following terms are defined as set forth below. Any terms used but not otherwise defined in this Agreement have the definitions set forth in the Regulations and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005, and any regulations promulgated thereunder. **[GPM Note: the list of defined terms should be the same list as is included in the Prime BAA].**

a. "Breach" shall have the meaning set forth in 45 C.F.R. § 164.402.

b. "Designated Record Set" shall have the meaning set forth in 45 C.F.R. § 164.501 and shall include, but not be limited to, medical records and billing records about Individuals.

c. "Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103.

d. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

e. "Protected Health Information" or "PHI" means, subject to the definition provided at 45 C.F.R. § 160.103, individually identifiable health information that Business Associate receives from Covered Entity or creates, receives, transmits or maintains on behalf of Covered Entity for purposes of performing the services under the Engagement. Unless otherwise stated in this Agreement, any provision, restriction or obligation in this Agreement related to the use of PHI shall apply equally to EPHI.

f. "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

g. "Secretary" shall mean the Secretary of the Department of Health and Human Services or their designee.

h. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with the system operations in an information system. Notwithstanding the foregoing, the Parties acknowledge and agree that Prime Subcontractor need not report all attempted but unsuccessful Security Incidents to Business Associate, and that this Agreement constitutes notice to Business Associate that such unsuccessful Security Incidents occur periodically. Unsuccessful Security Incidents include, but are not limited to, pings and other broadcast attacks on Prime Subcontractor's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as such incidents do not result in actual unauthorized access, use, or disclosure of PHI.

i. "Subcontractor" means a person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.

j. "Unsecured PHI" shall have the same meaning as the term "Unsecured PHI" in 45 C.F.R. § 164.402.

The services provided by Prime Subcontractor to Business Associate under the Engagement require that Prime Subcontractor may be given access to PHI. Prime Subcontractor acknowledges and agrees that all PHI that is created or received by Business Associate and disclosed or made available in any form by Business Associate to Prime Subcontractor, or is created, received, maintained or transmitted by Prime Subcontractor on Business Associate's behalf, will be subject to this Agreement. This Agreement will commence upon the Effective Date and will continue as long as Prime Subcontractor has use, custody or access to PHI subject to this Agreement, and thereafter for the period required by the Regulations.

II. Obligations and Activities of Prime Subcontractor

a. Use and Disclosure. Prime Subcontractor will not use or further disclose PHI other than to perform the services set forth in the Engagement, as permitted or required by this Agreement or as Required by Law. Prime Subcontractor will not use or disclose PHI in a manner that would violate the Regulations if done by a Covered Entity.

b. Restrictions on Disclosures. Prime Subcontractor will comply with any requests for restrictions on certain disclosures of PHI to which Covered Entity has agreed and of which Prime Subcontractor is notified by Business Associate. In addition, Prime Subcontractor will permit an Individual to make a reasonable request that PHI relating to the Individual be supplied at alternative locations and/or by alternative means, or to make a request for restriction of the use and/or disclosure of PHI in accordance with 45 C.F.R. § 164.522, and Prime Subcontractor will provide notice of such requests to Business Associate within ***[five (5)] [seven (7)]*** days. **[GPM Note: CE should ensure that it uses a notice period that is equal to or shorter than**

what is required of BA under the Prime BAA]. Prime Subcontractor agrees to comply with the requirements of 45 C.F.R. § 164.522(a)(vi) regarding requests for restriction on the disclosure of PHI to health plans for payment and health care operations purposes. Prime Subcontractor is prohibited from agreeing to any restriction on the use or disclosure of PHI or any alternative communication of PHI requested by an Individual without Business Associate's prior written approval.

c. Sale of PHI; Marketing; Fundraising; Research. Prime Subcontractor will not, except for payments from Business Associate for services performed pursuant to this Agreement or the Engagement, directly or indirectly receive remuneration, financial or otherwise, from or on behalf of the recipient in exchange for PHI. Prime Subcontractor will not use or disclose PHI for research or engage in any uses or disclosures that might be classified as marketing or fundraising without first obtaining prior written approval from Business Associate.

d. Minimum Necessary. **[GPM Note: If the Prime BAA obligates the BA to adhere to specific policies and procedures, then the Subcontractor BAA should likewise bind the Prime Subcontractor. We have included 2 options for addressing minimum necessary, based on what is agreed upon in the Prime BAA: (1) BAs permitting the Prime Subcontractor to follow its own policies on minimum necessary; or (2) requiring the Prime Subcontractor to comply with the minimum necessary policies the BA has passed down. The provision used in the Subcontractor BAA should be passed on to Prime Subcontractor based on what is used in the Prime BAA]. [Option 1]:** ***[Prime Subcontractor and its Subcontractors, if any, will only request, use and disclose the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure.]*** **[Option 2]** ***[Prime Subcontractor will comply, and will ensure that its Subcontractors comply, with the specific policies and procedures on the minimum necessary rule, a copy of which is attached hereto and incorporated herein as Exhibit __].*** Prime Subcontractor agrees, and it will ensure that any of its agents or subcontractors who themselves qualify as Subcontractors under the Regulations and create, receive, maintain or transmit PHI on behalf of Prime Subcontractor agree, to comply with Section 13405(b) of HITECH, any regulations issued thereunder or any guidance from the Secretary regarding what constitutes the definition of minimum necessary.

e. HIPAA Security Rule. Prime Subcontractor will develop, implement, maintain and use appropriate safeguards, and comply with the Security Rule at Subpart C of 45 C.F.R. Part 164, with respect to EPHI, to prevent use or disclosure of the PHI other than as provided for by this Agreement.

f. HIPAA Privacy Rule. Prime Subcontractor will comply with all requirements of the Privacy Rule at Subpart E of 45 C.F.R. Part 164 that apply to business associates.

g. Mitigation. Prime Subcontractor will mitigate, to the extent practicable, any harmful effect that is known to Prime Subcontractor of a use or disclosure of PHI by Prime Subcontractor in violation of the requirements of this Agreement.

[GPM Note: the Omnibus rule obligates BAs to ensure that Prime Subcontractors (which are themselves considered business associates) enter into "subcontractor BAAs" with any of their own "subcontractors". These subcontractor BAAs must obligate the subcontractor to comply with the same terms/conditions of this Subcontractor BAA between the BA and the Prime Subcontractor and must be at least as restrictive (i.e., future subcontractors cannot be given greater rights to use and disclose PHI than those held by the Prime Subcontractor under this Agreement). With respect to offshoring of PHI, the most protective option is that subcontractors not be permitted to do this without securing permission from the BA (and that CE, in the Prime BAA, not permit the BA to offshore PHI without CE's permission). Of course, if offshoring is not permitted at all under the Prime BAA, then it cannot be permitted under this agreement.]

h. Subcontractors. In accordance with the requirements of the Regulations, Prime Subcontractor will ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of Prime Subcontractor agrees in writing to the same restrictions, requirements and conditions that apply to Prime Subcontractor with respect to that PHI, including the provisions outlined in this Agreement. Notwithstanding anything else in this Agreement that may be construed to the contrary, Prime Subcontractor agrees that it **[GPM Note: the option selected should be based on what is in the Prime BAA between CE and BA] [Option A]:** ***[will not permit any Subcontractor that is located outside of the United States to create, receive, maintain or transmit any PHI, without first securing prior written approval from the Business Associate.]*** **[Option B]:** ***[will permit a party that is located outside of the United States to create, receive, maintain or transmit PHI only if an affiliate of that party, located in the United States and subject to jurisdiction in the courts of the United States, is the Subcontractor with which Prime Subcontractor has entered into a written agreement under which that Subcontractor agrees to the same restrictions, requirements and conditions that apply to Prime Subcontractor with respect to that PHI].***

i. Reports of Impermissible Use or Disclosure of PHI; Security Incident. Prime Subcontractor will report to Business Associate any use or disclosure of PHI not provided for or permitted by this Agreement of which it becomes aware, or any Security Incident of EPHI of which it becomes aware, **[GPM note: The notice period used in this Agreement should be the same or shorter than the notice period used in the Prime BAA.]** within ***[two (2) days] [three (3) days]*** of the date on which Prime Subcontractor first discovers the use, disclosure or Security Incident. **[GPM Note: CE may want to require reports to go to someone at BA who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to BA's Security Officer so as to ensure notice goes to a particular official and not to general contracting department, CE might require BA to designate a specific contact to receive notification from Subcontractors). This should of course be decided based on CE's relationship with the BA]. [Option A]** ***[All such reports will be made by Prime Subcontractor to _____ at Business Associate].*** **[Option B]** ***[All such reports will be made by Prime***

Subcontractor to the Business Associate official designated in Section VII(c) of this Agreement.] In addition to its other obligations under this Agreement, Prime Subcontractor will take prompt action to correct any Security Incident or use or disclosure of PHI not permitted under this Agreement and any action pertaining to such Security Incident or unauthorized use or disclosure as required by applicable federal or state laws and regulations.

[GPM Note: the next 2 sections are options for addressing HIPAA breaches. The CE should use the same option it uses in its Prime BAA. Option 1 permits the Prime Subcontractor to do the analysis of whether a HIPAA breach has occurred and then provide notice to the BA within a defined period. The BA would then be required (under the Prime BAA) to report the same to CE. Option 2 obligates the Prime Subcontractor to inform BA of any "suspected breach" (within a defined period) but allows BA to do the analysis if whether what has occurred actually gives rise to a Breach. The BA would then be required under the Prime BAA to report the same to CE.]

[Option 1—if selected, delete option 2]

j. Breaches of Unsecured PHI. Prime Subcontractor will report to Business Associate any Breach of Unsecured PHI by Prime Subcontractor or any of its officers, directors, employees, Subcontractors or agents. **[GPM Note: CE may want to require breach reports to go to someone at BA who is not the official designated to receive general notice under this BAA (i.e., if CE wants notice to go to BA's Security Officer so as to ensure notice goes to a particular official and not to general contracting department, CE might require BA to designate a specific contact to receive breach notification from Subcontractors). The point is for CE to ensure that it receives notice ASAP from the BA, so designating a specific contact point at BA might be helpful in that regard. This should of course be decided based on CE's relationship with the BA]. [Option A]** ***[All notifications of Breach of Unsecured PHI will be made by Prime Subcontractor to _____ at Business Associate.]*** **[Option B]** ***[All notifications of Breach of Unsecured PHI will be made by Prime Subcontractor to the Business Associate official designated in Section VII(c) of this Agreement]***. **[GPM Note: if CE is dictating this agreement, CE has discretion to require a specific notice period and should make decision about appropriate timeframe within context of HIPAA breach notification standard of providing notice to individuals as soon as possible, but no later than 60 days after discovering breach. We would not generally recommend that the Prime Subcontractor have longer than 5 days to provide this notice. The notice period should not be longer than the period the BA has to notify the CE under the Prime BAA.]** All notifications required under this Section will be made by Prime Subcontractor without unreasonable delay and in no event later than ***[two (2) days] [three (3) days] [five (5) days]*** of discovery. Prime Subcontractor will use the standard at 45 C.F.R. § 164.410(a) to determine when the Breach is treated as discovered. All notifications will comply with the obligations of a business associate under, and include the information specified in, 45 C.F.R. § 164.410 and include any other available information that a Covered Entity is required to include in its

notification to individuals pursuant to 45 C.F.R. § 164.404(c). In the event of a Breach by Prime Subcontractor that is caused by the acts or omissions of Prime Subcontractor, its Subcontractors, officers, directors, employees or agents, Prime Subcontractor will cooperate with Business Associate as Business Associate may require to facilitate notification of, **[GPM Note: CE should consider whether to require Subcontractor to cover costs of notification due to a breach caused by Subcontractor]** ***[and at Prime Subcontractor's expense]***, (i) individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate or Covered Entity to have been, accessed, acquired, used or disclosed, and (ii) the media, as required pursuant to 45 C.F.R. § 164.406, if the legal requirements for media notification are triggered by the circumstances of such Breach. **[GPM Note: following sentence relates to whether CE wants Prime Subcontractor to be responsible for costs of notification of breach caused by Prime Subcontractor. If not, this sentence can be deleted]** ***[Prime Subcontractor will indemnify Business Associate for any reasonable expenses Business Associate incurs in notifying individuals, the media and related expenses arising from a Breach, or assisting Covered Entity in such notification or mitigation related thereto, of a Breach caused by Prime Subcontractor or its officers, directors, employees, Subcontractors or agents.]*** Prime Subcontractor will cooperate in Business Associate's Breach analysis process and procedures, if requested.

[Option 2—if selected, delete option 1]

k. Breach of Unsecured PHI. Prime Subcontractor will report to Business Associate any suspected Breach of Unsecured PHI by Prime Subcontractor or any of its officers, directors, employees, Subcontractors or agents. **[GPM Note: if CE wants breach notification to go to someone at BA who is not the official designated to receive general notice under this BAA (i.e., if CE wants breach notice to go to BA Security Officer, CE can require that BAs designate a specific contact to receive breach notification from Subcontractor). This should of course be decided based on CE's relationship with the BA]. [Option A]** ***[All notifications of a suspected Breach of Unsecured PHI will be made by Prime Subcontractor to _____ at Business Associate.]*** **[Option B] [***All notifications of a suspected Breach of Unsecured PHI will be made by Prime Subcontractor to the Business Associate official designated in Section VII(c) of this Agreement].** All notifications required under this Section will be made by Prime Subcontractor without unreasonable delay and in no event later than ***[one (1) day] [two (2) days]*** of discovery. **[GPM Note: this period should be relatively short and no longer than what is used in the Prime BAA]**. Prime Subcontractor will use the standard at 45 C.F.R. § 164.410(a) to determine when the suspected breach is treated as discovered. Business Associate will have discretion to determine whether a suspected Breach has given rise to a Breach. Prime Subcontractor will cooperate with Business Associate and provide such information as Business Associate reasonably requires in making this determination. In notifying Business Associate of a suspected Breach, Prime Subcontractor will provide, to the extent reasonably possible, as much of the information that would be required to be provided by a business associate in notifying a Covered Entity of a Breach, under 45 C.F.R. § 164.410. If Business Associate

determines that a Breach has occurred, Prime Subcontractor will provide any other available information that a Covered Entity is required to include in its notification to individuals pursuant to 45 C.F.R. § 164.404(c). In the event Business Associate determines a Breach has occurred that was caused by the acts or omissions of Prime Subcontractor, its Subcontractors, officers, directors, employees or agents, Prime Subcontractor will cooperate with Business Associate, as Business Associate may require, to facilitate notification of, **[GPM Note: CE should consider whether to require Subcontractor to cover BA's costs of notification due to a breach caused by BA. Because CE is ultimately responsible for handling notification, this would seem to give CE added protection]** ***[and at Prime Subcontractor's expense]***, (i) individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate or Covered Entity to have been, accessed, acquired, used or disclosed, and (ii) the media, as required pursuant to 45 C.F.R. § 164.406, if the legal requirements for media notification are triggered by the circumstances of such Breach. **[GPM Note: following sentence relates to whether CE wants Subcontractor to be responsible for costs of notification. If not, this sentence can be deleted]** ***[Prime Subcontractor will indemnify Business Associate for any reasonable expenses Business Associate incurs in notifying individuals, the media and related expenses arising from a Breach, or assisting Covered Entity in such notification or mitigation related thereto, of a Breach caused by Prime Subcontractor or its officers, directors, employees, Subcontractors or agents.]*** Prime Subcontractor will cooperate in Business Associate's Breach analysis process and procedures, if requested.

[GPM Note: in the access, amendment and accounting provisions below, CE should be sure to use timeframes that are equivalent to, or shorter than, those CE imposes on the BA in the Prime BAA].

l. Access. In the event an Individual requests access to PHI in a Designated Record Set from Prime Subcontractor, Prime Subcontractor will provide Business Associate with notice of the same within ***[two (2)] [three (3)] [five (5)]*** days. Prime Subcontractor will provide access, within ***[two (2)] [three (3) [five (5)]*** days of a request of Business Associate and in the manner designated by Business Associate, to PHI in a Designated Record Set to Business Associate, or, as directed by Business Associate, to an Individual or an Individual's designee in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.524 (Access). If the PHI that is the subject of a request is maintained by the Prime Subcontractor in a Designated Record Set electronically, Prime Subcontractor will provide an electronic copy of such information to Business Associate, or, as directed by Business Associate, to the Individual or the Individual's designee, in the format required by the Regulations and as directed by Business Associate, in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.524.

m. Amendment. In the event Prime Subcontractor receives a request from an Individual for an amendment to PHI in a Designated Record Set, Prime Subcontractor will provide Business Associate with notice of the same within ***[two (2)] [three (3)] [five (5)]*** days. Prime Subcontractor will make any amendments to PHI in a Designated

Record Set that Business Associate directs or agrees to pursuant to 45 C.F.R. § 164.526 (Amendment) within ***[two (2)] [three (3)] [five (5)]*** days of a request of Covered Entity or an Individual and in the manner designated by Business Associate, in order to meet the Covered Entity's obligations under 45 C.F.R. § 164.526. Prime Subcontractor will incorporate any amendments to PHI it receives from Business Associate and will notify Business Associate of any amended PHI that it receives from third parties relating to the PHI.

n. Accounting of Disclosures. Prime Subcontractor will document such disclosures of PHI and information related to such disclosures as would be required for a Covered Entity to fulfill its obligations under the Regulations and HITECH, including, but not limited to, responding to a request by an Individual for an accounting of disclosures in accordance with 45 C.F.R. § 164.528, and will provide such information to Business Associate or an Individual, in the time and manner designated by Business Associate. Except in the case of a direct request from an Individual for an accounting related to treatment, payment or healthcare operations disclosures through an electronic health record, if the request for an accounting is delivered directly to Prime Subcontractor or its agents or Subcontractors, Prime Subcontractor will, within ***[two (2)] [three (3)] [five (5)]*** days of a request, notify Business Associate of the request. Business Associate will either inform Prime Subcontractor to provide such information directly to the Individual, or it will request the information to be immediately forwarded to Business Associate for compilation and distribution to such individual or the Covered Entity, and Prime Subcontractor will provide such information in its possession within ***[ten (10)]*** days of Business Associate's request. In the case of a direct request for an accounting from an Individual related to treatment, payment or healthcare operations disclosures through electronic health records, Prime Subcontractor will provide such accounting to the Individual in accordance with Section 13405(c) of HITECH and such regulations as are adopted thereunder. Business Associate and Prime Subcontractor agree that the provisions of this section related to accounting of disclosures for treatment, payment and healthcare operations purposes from an electronic health record will only be effective as of such date such accountings of disclosures are required under HITECH. Prime Subcontractor and any agent or Subcontractors will maintain the information required for purposes of complying with this section for such period of time as is required under the Regulations and HITECH.

o. Business Associate Obligations Under Privacy Rule. To the extent that Prime Subcontractor is to carry out one or more of Business Associate's or Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, Prime Subcontractor will comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

p. Records. Prime Subcontractor will make its internal practices, books, and records relating to the use and disclosure of PHI available to Business Associate or to the Secretary for purposes of determining Business Associate's compliance with the Regulations. Prime Subcontractor will notify Business Associate regarding any PHI that Prime Subcontractor provides to the Secretary, to the extent permitted by law or

the Regulations, concurrently with providing such PHI to the Secretary, and upon request by Business Associate, will provide Business Associate with a duplicate copy of such PHI.

q. Inspections; Audits. Within five (5) days of a written request by Business Associate, Prime Subcontractor will allow Business Associate to conduct a reasonable inspection of the policies and procedures, agreements, facilities, books, records and systems relating to the use or disclosure of PHI pursuant to this Agreement for the purpose of determining whether Prime Subcontractor has complied with this Agreement and the requirements of the Regulations; provided, however, that Business Associate will protect the confidentiality of all proprietary information of Prime Subcontractor to which Business Associate has access during the course of such inspection. The costs of the audit will be covered by Business Associate in the event the audit determines that Business Associate is in compliance with this Agreement and the Regulations and covered by Prime Subcontractor in the event the audit determines that Prime Subcontractor has violated this Agreement or the Regulations. Business Associate is permitted to engage in the inspections and audits set forth in this Section no more often than one time during each calendar year during which this Agreement is in effect.

r. Workforce. Prime Subcontractor will ensure that its workforce members, employees and agents are aware of and agree to the same restrictions which apply to Prime Subcontractor with respect to the PHI.

s. Business Associate Status. Prime Subcontractor acknowledges and agrees that the Engagement and this Agreement result in Prime Subcontractor qualifying as a business associate (as defined in 45 C.F.R. § 160.103). As such, Prime Subcontractor will be regulated as a business associate pursuant to the Regulations and any Subcontractor relationships in which Prime Subcontractor engages.

t. Compliance with HITECH. Prime Subcontractor will comply with all requirements of Title XIII, Subtitle D of HITECH which are applicable to business associates, and will comply with all regulations issued by the Secretary to implement these referenced statutes, as of the date by which business associates are required to comply with such referenced statutes and regulations.

III. Permitted Uses and Disclosures by Prime Subcontractor

[GPM Note: if CE is going to dictate the terms of the Subcontractor BAA, the provisions in this section should be drafted so that they are consistent with the terms of the Prime BAA between CE and BA. The Prime Subcontractor cannot be given the ability to use/disclose PHI that is greater or more extensive than what the CE has given to the BA in the Prime BAA].

a. Required by Law. Prime Subcontractor may use or disclose PHI as Required by Law.

[GPM Note: if the Prime BAA only gives the BA the right to use/disclose PHI for a list of specific purposes, the Subcontractor BAA should likewise bind the

Prime Subcontractor to use/disclose PHI for a list of specific purposes, which are not more extensive than those given to the BA under the Prime BAA. If BA was given the rights to use/disclose PHI to carry out the Engagement, then Prime Subcontractor can be given the rights to use/disclose PHI to carry out Prime Subcontractor's Engagement with BA.]

[Option 1—specific purposes. If this is selected, delete option 2].

b. Specific Purposes. Prime Subcontractor may only use or disclose PHI for the following specific purposes: **[GPM Note: list will need to be included].**

[Option 2—to carry out the Engagement. If this is selected, delete option 1.]

c. To Carry Out Engagement. Except as otherwise limited in this Agreement, for purposes of the services provided as part of the Engagement, Prime Subcontractor may use or disclose PHI solely to perform functions, activities, or services for, or on behalf of, Business Associate, provided that such use or disclosure would not violate the Regulations if done by Business Associate or a Covered Entity.

[GPM Note: the provisions on management/administration can only be granted to the Prime Subcontractor if CE has given those rights to BA under the Prime BAA. If not, the provision below should be deleted].

d. Management and Administration. Except as otherwise limited in this Agreement, Prime Subcontractor may use PHI for the proper management and administration of Prime Subcontractor or to carry out the legal responsibilities of Prime Subcontractor, as provided in 45 C.F.R. § 164.504(e)(4). In addition, Prime Subcontractor may disclose PHI for the proper management and administration of Prime Subcontractor or to carry out the legal responsibilities of Prime Subcontractor, provided that such disclosures are Required by Law or Prime Subcontractor obtains, prior to the disclosure, reasonable assurances from the person to whom it is disclosed that such PHI will be held secure and confidential as provided pursuant to this Agreement and only disclosed as Required by Law or for the purposes for which it was disclosed to the third party, and that any breaches of confidentiality of the PHI which becomes known to such third party will be immediately reported to Prime Subcontractor.

[GPM Note: additional uses/disclosures that are sometimes part of a BAA may be relevant to a subcontractor BAA. The provisions below should only be included if they are part of the Prime BAA and Prime Subcontractor will be assisting the BA in these activities. To the extent the BA has these added rights under the Prime BAA, any services provided by Prime Subcontractor for BA will need to be consistent with, and no more extensive than, the rights given to the BA). If CE does not want Subcontractors assisting BA with this work, or if CE has not given rights to BA in the Prime BAA to perform these services, they should not be included in the Subcontractor BAA. We have not included certain other uses/disclosures that arise from time to time in Subcontractor BAAs (such as fundraising, research, limited data sets or marketing) because those activities typically require additional review by counsel.]

[Option—Data Aggregation (combining PHI from different CEs for analytical purposes). Delete if not intended to be part of the Subcontractor BAA].

e. Data Aggregation. Prime Subcontractor may use PHI to provide data aggregation services related to the health care operations of the Covered Entity as directed by Business Associate and as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

[Option—De-Identified Information (note that PHI that is de-identified is no longer subject to HIPAA. This information can have proprietary value, and because de-identified information is not subject to HIPAA, can be freely bought and sold. CE should consider ownership/control issues over this information in the Prime BAA if it permits the BA to engage in de-identification). Delete if not intended to be part of the Subcontractor BAA].

f. De-Identification. Prime Subcontractor may use PHI to create information that is de-identified. Any such de-identification by Prime Subcontractor will be done in compliance with 45 C.F.R. § 164.514(b). Prime Subcontractor agrees that it has no ownership interest in de-identified information and that de-identified information may only be used and disclosed by Prime Subcontractor on behalf of Business Associate and pursuant to the Engagement.

IV. Obligations of Business Associate

a. Notice of Privacy Practices. Business Associate will provide Prime Subcontractor, upon request, with Covered Entity's Notice of Privacy Practices in effect at the time of the request.

b. Revocation of Permission. Business Associate will provide Prime Subcontractor with any known changes in or revocation of permission by an Individual to use or disclose PHI to the extent such changes may affect Prime Subcontractor's permitted or required uses and disclosures.

c. Restrictions on Disclosure. Business Associate will notify Prime Subcontractor of any material restriction to the use or disclosure of PHI to which Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent such restrictions may affect Prime Subcontractor's use and disclosure of PHI.

d. Impermissible Uses and Disclosures. Business Associate will not request Prime Subcontractor to use or disclose PHI in any manner that would not be permissible under the Regulations if done by a Business Associate.

V. Termination

a. Termination for Cause by Business Associate. Notwithstanding any contrary termination provision of any other agreement between the Parties, Business Associate is authorized to terminate this Agreement and the Engagement as described in this Section if Business Associate determines that Prime Subcontractor has violated a material term of this Agreement. Upon Business Associate's knowledge

of a material breach of this Agreement by Prime Subcontractor, Business Associate will provide written notice of such breach to Prime Subcontractor and provide an opportunity for Prime Subcontractor to cure the breach or end the violation. If Prime Subcontractor does not cure the breach or end the violation within a reasonable time, then Business Associate may immediately terminate this Agreement; or Business Associate may terminate this Agreement if Prime Subcontractor has breached a material term of this Agreement and Business Associate reasonably determines that cure is not possible.

b. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of the Engagement, Prime Subcontractor will return or destroy all PHI received from Business Associate or created, received, maintained or transmitted by Prime Subcontractor on behalf of Business Associate. This provision will apply to PHI that is in the possession of Subcontractors of Prime Subcontractor and Prime Subcontractor will ensure compliance with this requirement by its Subcontractors. Neither Prime Subcontractor nor Subcontractors will retain any copies of PHI.

2. In the event that Prime Subcontractor determines that returning or destroying the PHI is infeasible, Prime Subcontractor will provide to Business Associate notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI is infeasible; Prime Subcontractor will extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible for so long as Prime Subcontractor maintains such PHI.

VI. Indemnification

a. Indemnification of Business Associate. Prime Subcontractor will defend, hold harmless and indemnify Business Associate and Covered Entity against any and all third party claims brought against Business Associate or Covered Entity (including related liabilities, damages, judgments, costs and expenses, reasonable attorney's fees and costs) asserted against, imposed upon or incurred by Business Associate or Covered Entity that arises out of, or in connection with, Prime Subcontractor's default under or failure to perform any contractual or other obligation, commitment or undertaking under this Agreement, or the negligence of Prime Subcontractor or its Subcontractors, employees, agents or representatives in the discharge of its or their responsibilities or any other act or omission of Prime Subcontractor or its Subcontractors, employees, agents or representatives. This provision will survive termination of the Agreement with respect to any claim, action, or proceeding by a third party that relates to acts or omissions occurring during the term of this Agreement.

VII. Miscellaneous

a. Survival. The respective rights and obligations of Business Associate and Prime Subcontractor under Sections II, V, VI and VII of this Agreement will survive the termination of this Agreement.

[GPM Note: CE may seek to require that BA obligate its subcontractors to have insurance coverage that will protect BA from subcontractor's violations of the BAA/HIPAA, to the greatest extent possible. BAs may push back on this because subcontractors' existing insurance may not cover HIPAA issues and subcontractors may not want to acquire additional insurance. Note that the $1 million/$3 million amounts in the provision below reflect what is often seen in health care services agreement, but could be made higher or lower as agreed upon by the parties. Delete if not intended to be part of the BAA].

b. Insurance. Prime Subcontractor will maintain insurance in the minimum amounts of $1,000,000 per occurrence and $3,000,000 annual aggregate covering the acts and omissions of Prime Subcontractor under this Agreement. Prime Subcontractor will ensure that Business Associate is named an additional insured under this insurance policy. Prime Subcontractor will provide Business Associate with proof of such insurance upon request. Prime Subcontractor will notify Business Associate no later than ten (10) days of any actual or threatened claim, action, or proceeding related to activities undertaken pursuant to this Agreement and will cooperate in all respects with Business Associate in the defense of any such claim, action, or proceeding. Prime Subcontractor will provide Business Associate with notice within ten (10) days of any cancellation, termination or material alteration of any such insurance policies. Prior to the expiration or cancellation of any such policies, Prime Subcontractor will secure replacement of such insurance coverage upon the same terms and shall furnish Business Associate with a certificate of insurance. Failure of Prime Subcontractor to secure replacement coverage in the event of such cancellation, termination or material alteration of any such insurance policies will be a default hereunder, and Business Associate shall have the option to terminate this Agreement pursuant to Section VI.

c. Notification. Except as otherwise agreed to in this Agreement, any notice required or permitted under this Agreement will be given in writing and delivered personally or sent by certified mail, return receipt requested, or by reputable overnight delivery service, such as Federal Express, to the following addresses:

Business Associate	Prime Subcontractor
_____	_____
_____	_____
_____	_____
_____	_____

Such addresses may be changed by either Party by written advice as to the new address given as above provided.

d. Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Business Associate (and Covered Entities to which Business Associate is a business associate) to comply with HIPAA, the Regulations, and other applicable law, including HITECH and all regulations promulgated thereunder.

[GPM Note: CE may want the Subcontractor BAA to expressly state that CE is a third party beneficiary of the Agreement. This would permit the CE to enforce the Subcontractor BAA directly against the Prime Subcontractor. A provision in this regard is included as Option 1. Option 2 provides that there are no third party beneficiaries].

[Option 1—delete option 2 if used]

e. Covered Entity is a Third Party Beneficiary. Business Associate and Prime Subcontractor expressly agree and acknowledge that this Agreement is intended for the benefit of Covered Entity and that Covered Entity has third party beneficiary rights under this Agreement to enforce the Business Associate's rights and obligations against Prime Subcontractor.

[Option 2—delete option 1 if used]

f. No Third Party Beneficiaries. This Agreement is intended for the sole benefit of the Business Associate and Prime Subcontractor and does not create any third party beneficiary rights.

g. Waiver. No waiver or discharge of any liability or obligation hereunder by Business Associate or Covered Entity on any one or more occasions will be deemed a waiver of any continuing or other liabilities or obligations; nor shall they prohibit enforcement by Business Associate or Covered Entity of any liabilities or obligations on any other occasions.

h. Unenforceability. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event Business Associate believes in good faith that any provision of the Agreement fails to comply with the then-current requirements of HIPAA, the Regulations, and other applicable law, including but not limited to HITECH and all regulations promulgated thereunder, Business Associate will notify Prime Subcontractor in writing. For a period of up to thirty (30) days, the Parties will address in good faith such concern and will amend the terms of this Agreement if necessary to bring it into compliance. If after such thirty (30) day period Business Associate believes that this Agreement fails to comply with HIPAA, the Regulations, and other applicable law, including but not limited to HITECH and all regulations promulgated thereunder, then Business Associate has the right to terminate this Agreement upon written notice to Prime Subcontractor.

i. Independent Subcontractors. Prime Subcontractor is not the agent of Business Associate and Business Associate does not control, supervise or instruct Prime

Subcontractor or any Subcontractors. The Parties are independent Subcontractors and nothing in this Agreement will be deemed to make them partners or joint venturers or make Prime Subcontractor an agent of Business Associate.

j. No Assignment. Prime Subcontractor may not subcontract any services or assign any rights, nor may it delegate any of its duties, under this Agreement, without the express written consent of Business Associate.

k. Entire Agreement. This Agreement represents the parties' sole and entire agreement concerning the subject matter herein and supersedes and replaces all previous drafts, understandings and communications.

l. Remedies. Prime Subcontractor acknowledges and agrees that any breach of this Agreement by Prime Subcontractor may cause irreparable harm to Business Associate, the amount of which may be difficult to ascertain. Prime Subcontractor agrees that Business Associate may seek any legal remedy, including injunctive or specific performance for such harm, without bond, security or necessity of demonstrating actual damages. Such right of Business Associate is in addition to the remedies otherwise available to Business Associate at law or in equity. Prime Subcontractor expressly waives the defense that a remedy in damages will be adequate.

m. Representations and Warranties. Prime Subcontractor warrants and represents that it is in compliance with the Security Rule and the provisions of the Privacy Rule that apply to business associates.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective as of the Effective Date.

BUSINESS ASSOCIATE:	**PRIME SUBCONTRACTOR:**
_____	_____
By: _____	By: _____
Title: _____	Title: _____

[GPM Note: This Template Data Use Agreement is to be used when a covered entity seeks to disclose a limited set of PHI to another entity for research, public health, and/or health care operations purposes. The PHI being disclosed must qualify as a "Limited Data Set" under HIPAA (*see* 45 C.F.R. § 164.514(e)(2)) and exclude direct identifiers of the individual or of relatives, employers, or household members of the individual. If the covered entity also seeks to disclose PHI that *includes* direct identifiers to a party to create the limited data set, a business associate agreement with that party is also required. Applicable provisions from the Template Business Associate Agreement can be combined with this Data Use Agreement to create one document. Note that this Template Data Use Agreement does not include business associate agreement provisions].

DATA USE AGREEMENT

This Data Use Agreement (the "Agreement") is entered into and made effective the _____ day of _____(the "Effective Date"), by and between _____ ("Covered Entity"); and _____ ("Data Recipient") (each a "Party" and collectively the "Parties").

WHEREAS, In conjunction with _____ **[GPM Note: Further describe the purpose(s) for which the limited data set will be disclosed. Permitted purposes include research, public health, or health care operations.]** (the "Purpose"), Covered Entity may from time to time disclose to Data Recipient, and Data Recipient may use, disclose, receive, transmit, or maintain, PHI in the form of a Limited Data Set ("Limited Data Set Information") **[GPM Note: Limited Data Set Information, although devoid of direct identifiers, is still considered PHI and arguably would still qualify as "Health Records" under the Minnesota Health Records Act (the "MHRA"). Consequently, disclosure of Limited Data Set Information must comply with the MHRA.]**;

WHEREAS, The Parties desire to enter into this Agreement so as to allocate responsibility for the Use and Disclosure of Limited Data Set Information and to comply with applicable requirements of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and the regulations promulgated thereunder by the United States Department of Health and Human Services ("HHS") codified at 45 C.F.R. Parts 160 and 164, (commonly known as the Privacy and Security Rules) as amended by the Privacy and Security provisions set forth in Section 13400 of the Health Information Technology for Economic and Clinical Health Act, Public law 111-5 ("HITECH Act"), (collectively referred to herein as the "HIPAA Regulations"), as they pertain to Limited Data Sets.

NOW THEREFORE, in consideration of the mutual promises and conditions contained herein, and for other good and valuable consideration, the Parties agree as follows:

ARTICLE 1
DEFINITIONS

Capitalized terms used, but not otherwise defined, in this Agreement will have the meaning ascribed to them in the HIPAA Regulations. Limited Data Set Information will have the meaning ascribed to "Limited Data Sets" in the HIPAA Regulations, but for the purposes of this Agreement will refer solely to Limited Data Set Information transmitted from or on behalf of

Covered Entity to Data Recipient or an agent or subcontractor of Data Recipient, or created by Data Recipient or its agent or subcontractor on behalf of Covered Entity. Unless otherwise specified, the use of the term PHI will be interpreted to include Limited Data Set Information.

ARTICLE 2
EFFECT AND INTERPRETATION

The provisions of this Agreement shall apply with respect to the Use or Disclosure of any Limited Data Set Information by the Parties in conjunction with the Purpose. This Agreement sets forth the terms and conditions pursuant to which Covered Entity will Disclose the Limited Data Set Information to Recipient. Covered Entity will limit the PHI it Discloses or makes available to Data Recipient to Limited Data Set Information. In the event of any conflict or inconsistency between this Agreement and any other agreement(s) between the Parties pertaining to the Purpose or the Limited Data Set Information, the terms of this Agreement will govern. The provisions of this Agreement are intended in their totality to implement 45 C.F.R. 164.514(e) as it concerns Data Use Agreements.

ARTICLE 3
GENERAL OBLIGATIONS OF DATA RECIPIENT

Section 3.1 Use and Disclosure of Limited Data Set Information. Data Recipient agrees to not Use or further Disclose Limited Data Set Information other than as permitted by Article 4 of this Agreement, or as otherwise Required By Law.

Section 3.2 Safeguards. Data Recipient agrees to use appropriate safeguards to prevent Use or Disclosure of the Limited Data Set Information other than as permitted by Article 4 of this Agreement. Without limiting the generality of the foregoing, Data Recipient further agrees to:

a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Limited Data Set Information it creates, receives, maintains, or transmits on behalf of Covered Entity;
b. Ensure that any agent, including any subcontractor, to whom it provides such Limited Data Set Information agrees to implement reasonable and appropriate safeguards to protect such information;
c. Report promptly (and in no case later than five (5) business days) to the Covered Entity any Security Incident or Breach of Unsecured PHI of which Data Recipient becomes aware.

Section 3.3 Reports of Impermissible Use or Disclosure of Limited Data Set Information. Data Recipient will report promptly (and in no case later than five (5) business days) to Covered Entity any Use or Disclosure of the Limited Data Set Information not permitted by Article 4 of this Agreement of which Data Recipient becomes aware.

Section 3.4 Identification and Contact of Individuals. Data Recipient will not attempt to identify the Individuals to whom the Limited Data Set Information pertains, or attempt to contact such Individuals, except with the prior written consent of Covered Entity.

Section 3.5 Agents. Data Recipient agrees to require that any agent to whom it, directly or indirectly, provides Limited Data Set Information will agree in writing to comply with the same restrictions and conditions that apply through this Article 3 to Data Recipient.

ARTICLE 4
PERMITTED USES AND DISCLOSURES BY DATA RECIPIENT

[GPM Note: HIPAA permits covered entities to use and disclose a Limited Data Set for the purposes of research, public health, and health care operations. However, due to the requirements under the MHRA related to obtaining consent for disclosures of health records to an external researcher solely for purposes of medical or scientific research, some covered entities may not want research to be an intended purpose of the activities that would otherwise be permitted under the Data Use Agreement. Two options are outlined below. Option 1 permits Data Recipient to use and disclose Limited Data Set Information for public health, health care operations, and research purposes. Option 2 permits Data Recipient to use and disclose Limited Data Set Information for public health and health care operations purposes only.]

[Option 1—Use and Disclsoure for research, public health, and health care operations permitted. Delete if Option 2 is selected.]

Data Recipient may, consistent with this Agreement, Use or Disclose Limited Data Set Information to a third party for purposes of Public Health, Health Care Operations or Research in accordance with the provisions of the HIPAA Regulations concerning Limited Data Sets, provided that such Use or Disclosure is (i) limited to the minimum information necessary to accomplish the Purpose; and (ii) would not violate the HIPAA Regulations if done by Covered Entity. Covered Entity represents and warrants that it has obtained consent to disclose Limited Data Set Information for the purpose of external Research or has otherwise determined that the Disclosure is permitted in accordance with Minnesota law.

[Option 2—Use and Disclosure permitted for public health and health care operations only. Delete if Option 1 is selected.]

Data Recipient may, consistent with this Agreement, Use or Disclose Limited Data Set Information to a third party for purposes of Public Health or Health Care Operations in accordance with the provisions of the HIPAA Regulations concerning Limited Data Sets, provided that such Use or Disclosure is (i) limited to the minimum information necessary to accomplish the Purpose; and (ii) would not violate the HIPAA Regulations if done by Covered Entity. Data Recipient acknowledges that while HIPAA generally would permit Use and Disclosure of Limited Data Set Information of Covered Entity for Research purposes, such Use and Disclosure is not an intended purpose under this Agreement. Accordingly, Data Recipient agrees that it will not Use or Disclose Limited Data Set Information of Covered Entity for Research purposes of Data Recipient itself or of any third party.

ARTICLE 5
TERM AND TERMINATION

Section 5.1 Term. This Agreement will commence as of the Effective Date and will remain in effect as long as Data Recipient retains the information described herein, unless this

Agreement is terminated sooner in accordance with Sections 5.2 or 5.3 of this Article.

Section 5.2 Termination for Material Breach. Any Party may terminate this Agreement based upon a material breach of this Agreement by the other Party, provided that the non-breaching Party gives the breaching Party ten (10) days written notice and the opportunity to cure such breach, and the breach is not cured during the notice period. In the event such material breach is not cured, the non-breaching Party may terminate this Agreement immediately upon the expiration of the notice period. In the event it is not possible to cure such material breach, the non-breaching Party may terminate this Agreement immediately and without any notice. **[GPM Note: Timing for termination and notification in this and other paragraphs in this document is just a suggestion and may vary based on the parties' needs and standard business practices].**

Section 5.3 Termination Permitted Due to Change in Law. Any Party may terminate this Agreement as permitted in accordance with Section 7.2 of this Agreement upon a change in an applicable law that causes performance in compliance with this Agreement to violate the law.

Section 5.4 Effect of Termination. The Parties acknowledge and agree that the provision of Limited Data Set Information to Data Recipient is conditioned upon this Agreement being in full force and effect. Therefore, upon termination of this Agreement, the Parties agree that Covered Entity will refrain from submitting Limited Data Set Information to Data Recipient, and Data Recipient will refrain from accepting Limited Data Set Information from Covered Entity. In the event the Parties engage in negotiations undertaken in accordance with Section 7.2 of this Agreement, the Parties will suspend during such period of negotiation any Use or Disclosure of Limited Data Set Information that the Party reasonably believes would violate any applicable state or federal law or regulation, including without limitation the HIPAA Regulations. Upon termination of this Agreement, Data Recipient agrees to promptly return or destroy, except to the extent infeasible, all Limited Data Set Information, including any Limited Data Set Information which Data Recipient has Disclosed to its subcontractors or agents. In the event that return or destruction of some or all of the Limited Data Set Information is infeasible, Data Recipient will continue to extend the protections of this Agreement to such Limited Data Set Information that is not returned or destroyed. The obligations of this Section 5.4 will survive any expiration or termination of this Agreement.

ARTICLE 6
INDEMNIFICATION

[GPM Note: Indemnification is not required by HIPAA or state privacy laws. However, given increased scrutiny and heightened penalties for HIPAA violations, Covered Entities may want to consider its inclusion. The provision below is an example of a one-way indemnification commitment running from Data Recipient to Covered Entity. Another alternative would be to use a mutual indemnification provision. Whether the Data Recipient can exclude this provision from the Data Use Agreement, and whether the Covered Entity will be successful in obtaining a one sided provision, likely will be a consequence of the negotiating leverage of the parties.]

Data Recipient will indemnify and hold harmless Covered Entity from and against any claim, cause of action, liability, direct losses, damages, costs and expenses (including without limitation reasonable attorney's fees) suffered by Covered Entity arising out of or in connection with any unauthorized Use or Disclosure of Limited Data Set Information or any other breach of this Agreement by Data Recipient or any of its subcontractors or agents. The Parties' obligations under this Article 6 regarding indemnification will survive any expiration or termination of this Agreement.

ARTICLE 7
MISCELLANEOUS

Section 7.1 Regulatory References. A reference in this Agreement to a section in the HIPAA Regulations means the section as in effect or as amended from time to time and for which compliance is required.

Section 7.2 Amendment. This Agreement may not be amended except by the mutual written agreement of the Parties. Notwithstanding the foregoing, the Parties agree to work together in good faith to take such action as is necessary to make technical amendments to this Agreement from time to time if necessary for Covered Entity and/or Data Recipient to comply with the requirements of HIPAA, the HIPAA Regulations, or any applicable provisions of any other federal or state law, as such laws or regulations may be amended from time to time. However, should any state or federal law or regulation now existing or enacted after the Effective Date of this Agreement, including without limitation HIPAA or the HIPAA Regulations, be amended or interpreted by judicial decision or a regulatory body in such a manner that a Party reasonably determines renders any provision of this Agreement in violation of such law or regulation or adversely affects the Parties' abilities to perform their obligations under this Agreement, the Parties agree to negotiate in good faith to amend this Agreement so as to comply with such law or regulation and to preserve the viability of this Agreement. If, after negotiating in good faith, the Parties are unable to reach agreement as to any necessary amendments, either Party may terminate this Agreement without penalty.

Section 7.3 Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Covered Entity and Data Recipient to comply with the HIPAA Regulations.

Section 7.4 Third Party Beneficiaries. There are no intended third party beneficiaries to this Agreement. Without limiting the generality of the foregoing, the Parties agree that Individuals whose Limited Data Set Information is Used or Disclosed to Data Recipient or its agents or subcontractors under this Agreement are not third-party beneficiaries of this Agreement.

Section 7.5 Waiver. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving Party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

Section 7.6 Correspondence. Any notice required or permitted under this Agreement will be given in writing and delivered personally or sent by certified mail, return receipt requested, or by reputable overnight delivery service, such as Federal Express, to the following addresses:

Covered Entity	**Data Recipient**
_____	_____
_____	_____
_____	_____
_____	_____

Section 7.7 Independent Contractors. The Parties are independent contractors and nothing in this Agreement shall be deemed to make them partners or joint venturers or make Data Recipient an agent of Covered Entity.

Section 7.8 Assignment. No Party may assign its respective rights or obligations under this Agreement without the prior written consent of the other Party.

Section 7.10 Governing Law. To the extent that federal law does not govern this Agreement, this Agreement shall be governed in accordance with the laws of the State of Minnesota, excluding its conflict of law provisions.

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective as of the Effective Date.

Covered Entity:	**Data Recipient:**
_____	_____
By: _____	By: _____
Title: _____	Title: _____

[Enter Organization Logo]

DISCLOSING INFORMATION IN A MEDICAL EMERGENCY

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy

A. Purpose

This policy establishes guidelines to be followed by [*Organization]*'s workforce when using or disclosing patient information in an emergency situation.

B. Policy Implementation—General Rule

While HIPAA permits [*Organization*] to disclose protected health information for treatment purposes without patient authorization, Minnesota law generally requires [*Organization*] to obtain patient consent prior to releasing health information. However, [*Organization*] is permitted to disclose patient health information in an emergency situation without consent if:

a. The patient is experiencing a Medical Emergency; and

b. [*Organization*] is unable to obtain the patient's consent due to:

   i. The patient's condition; or

   ii. The nature of the Medical Emergency.

If these elements are satisfied, [*Organization*] and its staff may disclose patient information without consent. However, if these elements are not satisfied [*Organization*] must obtain patient consent prior to disclosing information.

Substance Use Disorder Patient Records. In addition to the above requirements, [*Organization*] may only disclose substance use disorder patient records without patient consent if the disclosure is to medical personnel and is necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained. Disclosures to medical personnel of the Food and Drug Administration (the "FDA") is also permitted without prior informed consent when such medical personnel states that the health of any individual may be threatened by an error in the manufacture, labeling, or sale of a product that is regulated by the FDA, and that the disclosed information will be used for the exclusive purpose of notifying patients or their physicians of potential dangers. All such disclosures must be limited to the information necessary to treat the condition/Medical Emergency.

Immediately following the disclosure, [*Organization*] must document the following in the patient's record:

1. The name of the medical personnel to whom the disclosure was made and their affiliation with any health care facility;

2. The name of the individual making the disclosure;

3. The date and time of the disclosure; and

4. The nature of the emergency or error if the report was to the FDA.

<u>Re-Disclosure</u>. [*Organization*] is permitted to re-disclose substance use disorder patient records without patient consent when treating a patient for a Medical Emergency. However, [*Organization*] staff must always limit disclosures to the information necessary to carry out the purpose of the disclosure.

If the above elements are not satisfied, other exceptions may apply that would permit a disclosure without patient consent. For example, [*Organization*] is required by law to report certain events, including but not limited to gunshot wounds, burns, and infectious diseases. These events may take place during an "emergency". However, [*Organization*] is not required to obtain patient consent, or otherwise satisfy the emergency exception requirements, prior to disclosure.

C. Mental Health Records and Psychotherapy Notes

As with general health records, [*Organization*] can disclose general mental health records without patient consent if the patient is experiencing a Medical Emergency and the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the Medical Emergency.

However, prior to disclosing psychotherapy notes [*Organization*] must either obtain patient authorization or satisfy an exception to the authorization requirement. [*Organization*] can disclose psychotherapy notes without patient authorization if [*Organization*], in good faith, believes the use or disclosure: (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and (2) is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. If these elements are satisfied in an emergency situation, [*Organization*] may disclose psychotherapy notes without patient authorization.

D. Emergency Situation has Concluded

Once the emergency situation has concluded, [*Organization*] must obtain patient consent prior to disclosing information. Practically speaking, the patient may still be in a serious condition and/or in need of services from [*Organization*]—but if the patient's condition or the nature of the Medical Emergency does not prevent [*Organization*] from obtaining consent, patient consent is required (unless a different exception to the consent requirement under Minnesota law is satisfied).

II. Procedure

A. Prior to disclosing information in an emergency situation, [*Organization*] and its staff will:

    1. Determine whether the situation otherwise permits disclosure without patient consent (e.g., [*Organization*] is required by law to report gunshot wounds).

    2. Assess the situation to determine whether a Medical Emergency exists;

        i. <u>If substance use disorder patient records are at issue</u>: The treating provider is responsible for determining whether a bona fide medical emergency exists.

    3. Determine whether the patient is able to provide consent to the disclosure;

        i. If the patient is able to provide consent, obtain such consent prior to any disclosures.

        ii. If the patient is unable to provide consent due to either the patient's condition or the nature of the Medical Emergency, proceed to Step 4.

    4. Determine whether psychotherapy notes are involved;

        i. If they are, staff must determine whether patient authorization is required;

    5. Determine the purpose of the disclosure;

        i. If the disclosure is for treatment purposes and the above requirements are satisfied, the disclosure is permitted without patient consent.

        ii. If the disclosure is for other purposes (e.g., marketing), patient authorization is required.

B. Once disclosed, [*Organization*] must immediately document the disclosure and the nature of the medical emergency in the patient's record.

C. If [*Organization*] staff are unsure whether the above requirements are satisfied, they must consult with [*Organization*]'s [*compliance officer/privacy officer/other designee*] prior to disclosing such information.

[Enter Organization Logo]

USE AND DISCLOSURE OF PHI FOR FUNDRAISING

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes guidelines for *[Organization]*'s workforce to follow regarding the use or disclosure of PHI for fundraising purposes.

B. Policy Implementation

[Organization] may use and disclose PHI for fundraising purposes only in accordance with the HIPAA Regulations, applicable state law, and this Policy.

1. **Fundraising without an authorization**

[Organization] may use and disclose certain PHI for fundraising without a HIPAA authorization, if *[Organization]* complies with the requirements stated in Section 2 below, and the following circumstances are met:

a. The fundraising is for the benefit of *[Organization]*;

b. Any disclosures to a business associate or an institutionally related foundation are addressed in a business associate agreement or otherwise permitted under HIPAA;

c. *[Organization]* has included a statement in the Notice of Privacy Practices that *[Organization]* may contact the individual to raise funds for *[Organization]* and the individual has a right to opt out of receiving such communications;

d. The uses and disclosures of PHI are limited to the following subset of PHI (the "Permitted Fundraising Information"):

i. Demographic information related to the individual, including name, address, other contact information, age, gender, and date of birth;

ii. Dates of health care provided to an individual;

iii. Department of service information (for example, information about the general department of treatment such as cardiology, oncology, pediatrics, etc.);

iv. Treating physician;

v. Outcome information, such as information regarding the death of the patient or any sub-optimal result of treatment or services. The idea is for covered

entities to use this information in connection with fundraising purposes to screen and eliminate from fundraising solicitations those individuals experiencing a sub-optimum outcome; and

vi. Health insurance status.

The Minnesota Health Records Act requires providers to obtain written consent prior to disclosing health records unless an exception otherwise applies. Use and disclosure of PHI by a covered entity to fundraise for the covered entity's own benefit is considered a "health care operation" of that entity. The patient's consent to the use and disclosures of his or her health records for "health care operations" of *[Organization]* authorizes *[Organization]* to use/disclose the Permitted Fundraising Information described in B.1 to fundraise on its own behalf or contract with a business associate or institutionally related foundation for that purpose.

2. **Other requirements**

If pursuant to Section 1, *[Organization]* uses or discloses Permitted Fundraising Information for fundraising purposes without the patient's authorization, *[Organization]* shall satisfy the following requirements:

a. With each fundraising communication made to an individual, *[Organization]* must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost;

b. *[Organization]* may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications;

c. *[Organization]* may not make fundraising communications to an individual where the individual has elected not to receive such communications;

d. *[Organization]* may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications;

3. **Authorization required**

HIPAA requires *[Organization]* to obtain a valid authorization—that meets the requirements of policy number *[Enter]*, Authorization for Use and Disclosure of PHI—prior to use or disclosure of PHI for the purpose of fundraising if any of the requirements in Sections B.1 or B.2 are not met. For example, *[Organization]* would need to get authorization for any fundraising that is:

a. The fundraising is for the benefit of an entity other than *[Organization]*, even if the information at issue would otherwise be Permitted Fundraising Information;

b. The disclosure at issue involves activities that are more extensive than fundraising and instead meet the definition of "marketing";

c. The PHI used or disclosed includes information other than the Permitted Fundraising Information listed in Section 1(d) above. For example, *[Organization]* wants to use information about a specific illness, diagnosis or disease of recipients to raise funds.

II. Procedure:

A. Prior to using PHI for fundraising purposes, *[Organization]*'s Privacy Official or designee must:

1. Determine whether the information is Permitted Fundraising Information that meets the requirements of Sections B.1 and B.2 and that the other requirements outlined in those sections are addressed;

2. Determine whether the consent used by *[Organization]* permits the fundraising activities;

3. Determine whether a HIPAA authorization is required for the use or disclosure of the PHI;

4. Verify that a valid authorization has been obtained, if it is determined that an authorization is needed;

5. Verify that the other requirements described in this policy have been met.

[Enter Organization Logo]

USING AND DISCLOSING INFORMATION FOR HEALTH CARE OPERATIONS

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy

A. Purpose

This policy establishes guidelines to be followed by [*Organization*]'s workforce when using or disclosing information for Health Care Operations.

B. Policy Implementation—General Rule

[*Organization*]'s Own Health Care Operations

The general rule is that [*Organization*] or its workforce may use or disclose PHI without an individual's HIPAA authorization for [*Organization*]'s own Health Care Operations purposes. "Health Care Operations" is broadly defined and includes certain administrative, financial, legal, and quality improvement activities that are necessary to operate [*Organization*]'s business and provide treatment services. See Policy number [Enter], Definitions, for the full definition of "Health Care Operations."

Minnesota Law. Minnesota law generally requires [*Organization*] to obtain signed and dated patient consent prior to releasing health records, unless certain exceptions apply. [*Organization*] includes general language in its standard consent form indicating that [*Organization*] can disclose patient information for health care operations purposes. This satisfies the consent requirement under Minnesota law. [*Organization*] states in its Notice of Privacy Practices that it may use and disclose information for Health Care Operations; if there is language by which patient acknowledges and consents to the activities described as set forth in the Notice of Privacy Practices in [*Organization*]'s consent form, this would be an alternative option for the patient to provide the necessary consent under Minnesota law.

For more information about patient consent requirements under Minnesota law, refer to Policy [Enter], Consent to Disclose Health Information under Minnesota Law.

For information about unique requirements under the Minnesota Data Practices Act, refer to the guidance document entitled, "Additional Requirements under the Minnesota Data Practices Act."

Substance Use Disorder Patient Records. Unique rules apply when [*Organization*] seeks to disclose substance use disorder patient records for Health Care Operations. [*Organization*] may disclose information without patient consent to a qualified service organization, provided certain requirements are met. *See* 42 CFR §

2.12(c)(4). Staff should review policy number [Enter], Disclosing Information to Business Associates, for more detail. In addition, [*Organization*] can disclose substance use disorder patient records without patient consent to an entity with direct administrative control over [*Organization*], or for audit and evaluation activities in accordance with 42 C.F.R. § 2.53. Staff should consult with [*Organization*]'s [*compliance officer/privacy officer/other designee*] to determine whether a disclosure of substance use disorder patient records is permitted without patient consent. Additional information can be found in policy number [Enter], Disclosures of Substance Use Disorder Patient Information.

Another Entity's Health Care Operations

In addition, [*Organization*] can disclose PHI to another covered entity for the Health Care Operations of that covered entity in the following circumstances:

1. Each entity either has or had a relationship with the individual who is the subject of the PHI being requested and the PHI pertains to such relationship, and the disclosure is:

    a. For conducting quality assessment and improvement activities, or other activities discussed in subsection (i) of the definition of "Health Care Operations" (*see* [*Organization*]'s Definitions Policy);

    b. For reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, and other activities discussed in subsection (ii) of the definition of "Health Care Operations" (*see* [*Organization*]'s Definitions Policy); or

    c. For the purpose of health care fraud and abuse detection or compliance.

2. A covered entity that participates in an organized health care arrangement (an "OHCA") may disclose PHI to other participants in the OHCA for any Health Care Operations activities of the OHCA; or

3. Pursuant to patient authorization that meets HIPAA standards.

C. Disclosure of Minimum Necessary

When [*Organization*] and its workforce uses and discloses PHI for Health Care Operations purposes, or discloses, it must comply with the minimum necessary rule. This means that it can use or disclose only the information that is necessary.

II. Procedure

When using or disclosing health information for Health Care Operations purposes, [*Organization*] and its workforce shall:

A. Contact [*Organization*]'s [*compliance officer/privacy officer/other designee*] to confirm that such tasks and activities qualify as "Health Care Operations";

B. Ensure the patient has acknowledged and consented to [*Organization*]'s Notice of Privacy Practices; if the patient has not, obtain signed and dated consent; and

C. Determine whether the purpose is for [*Organization*]'s own Health Care Operations or for the Health Care Operations of another covered entity.

a. If for [*Organization*]'s purposes, no further action is needed; the use or disclosure is permitted.

b. If for the Health Care Operations of another covered entity; comply with one of the three permitted circumstances listed above.

[Enter Organization Logo]

AUTHORIZATION FOR USE AND DISCLOSURE OF PHI

Policy Number: [Enter]
Effective Date: [Enter]

[Note: This Policy addresses authorizations for use and disclosure of PHI for providers and does not include additional requirements that apply to health plans.]

I. Policy:

A. Purpose

This policy establishes the requirements for the creation and use of authorizations required under the HIPAA Regulations.

The Minnesota Health Records Act ("MHRA") does not differentiate between authorizations and consents but instead refers to "consent" language specifically in identifying how information will be disclosed.

However, the term "authorization" has a specific meaning under HIPAA. As discussed in this Policy, a valid HIPAA authorization form must include specific elements. While obtaining HIPAA authorization satisfies the consent requirements under the MHRA, obtaining consent that satisfies the MHRA does not necessarily constitute a valid HIPAA authorization (unless all of the HIPAA requirements are satisfied).

For more information on consent requirements under Minnesota law, refer to policy number [Enter], Consent to Use and Disclose Health Information Under Minnesota Law.

B. Policy Implementation

The general rule is that except as otherwise permitted under the HIPAA Regulations, [*Organization*] may not use or disclose PHI without valid authorization from the individual to whom the PHI pertains. [*Organization*] must use or disclose PHI only in accordance with the authorization.

There are exceptions to this rule. For example, [*Organization*] does not need to obtain HIPAA authorization for:

- Treatment purposes;
- Payment;
- Health Care Operations; and
- Releases that are required by law.

Additional exceptions may apply and [*Organization*] workforce should consult with the [*compliance officer/privacy officer/other designee*] as appropriate.

Substance Use Disorder Patient Records. When dealing with substance use disorder patient records, [*Organization*] generally may not use or disclose this information unless the individual has signed a consent form that satisfies Part 2 requirements. This is true even if the disclosure is otherwise permitted under the HIPAA Regulations. Any disclosure must be limited to the information necessary to carry out the purpose of the disclosure.

For more information on consent requirements for substance use disorder records, refer to policy number [Enter], Disclosures of Substance Use Disorder Records.

C. Authorizations for Use or Disclosure of PHI for Marketing

[*Organization*] must obtain HIPAA authorization for any use or disclosure of PHI for Marketing, unless the communication is:

I. A face-to-face communication made by [*Organization*] or its workforce to an individual; or
II. A promotional gift of nominal value.

If the Marketing involves any direct or indirect payments to [*Organization*] from or on behalf of a third party whose product or service is being described in the communication ("Financial Remuneration"), [*Organization*] must include language in the authorization form that clearly states remuneration in involved. Direct or indirect payments do not include any payments for treatment of an individual.

Refer to policy number [Enter], Use and Disclosure of PHI for Marketing, for the definition of "Marketing" and additional information.

D. Authorizations for Sale of PHI

[*Organization*] must obtain HIPAA authorization prior to any Sale of PHI. The authorization must state that the disclosure will result in remuneration to [*Organization*].

"Sale of PHI" means a disclosure of PHI by [*Organization*] or its business associate where [*Organization*] or business associate directly or indirectly receives remuneration in exchange for the PHI. Sale of PHI does not include a disclosure:

1. For public health purposes pursuant to § 164.512(b) or § 164.514(e);
2. For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by [*Organization*] or its business associate is a reasonable fee to cover the cost to prepare and transmit the PHI;
3. For treatment and payment purposes;
4. For the sale, transfer, merger, or consolidation of all or part of [*Organization*];
5. To or by a business associate for activities that the business associate undertakes on behalf of [*Organization*], or on behalf of a business associate in the case of a subcontractor, where the only remuneration provided is by [*Organization*] to the

business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

6. To an individual, when requested under § 164.524 or § 164.528;
7. Required by law; and
8. For any other purpose permitted by the HIPAA Privacy Rule where the only remuneration received by [*Organization*] or its business associate is a reasonable fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by other law.

E. Authorizations for Use or Disclosure of Psychotherapy Notes

[*Organization*] must obtain HIPAA authorization for any use or disclosure of Psychotherapy Notes. However, authorization is not required for the following:

1. Use by the originator of the Psychotherapy Notes for treatment;
2. Use or disclosure by [*Organization*] for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
3. Use or disclosure by [*Organization*] to defend itself in a legal action or other proceeding brought by the individual;
4. Use or disclosure that is required by the Secretary to investigate or determine [*Organization*]'s compliance with the HIPAA Privacy Rule;
5. Use or disclosure that is required by law;
6. Use or disclosure for health oversight activities by the originator of the Psychotherapy Notes;
7. Use or disclosure about decedents to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; or
8. Use or disclosure to avert a serious threat to health or safety pursuant to 45 C.F.R. § 164.512(j)(1)(i).

F. Content of Valid Authorization

All authorizations must be written in plain language and contain at least the following elements:

1. A specific and clear description of the information to be used or disclosed;

2. The name or other specific identification of the person(s) or group of persons authorized to make the requested use or disclosure;

3. The name or other specific identification of the person(s) or group of persons to whom [*Organization*] may make the requested use or disclosure;

4. A description of each purpose of the requested use or disclosure. The statement, "at the request of the individual," is a sufficient description of the purpose when an

individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statements, "end of the research study," "none" or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository;

   Note: The expiration date in Minnesota shall be one year from the time of issuance, or for a different period specified in the consent, consistent with Minnesota Statutes § 144.293, subd. 4;

6. Signature of the individual and date;

7. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided;

8. A statement of the individual's right to revoke the authorization in writing, and either:

   a. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

   b. A reference to [*Organization*]'s Notice of Privacy Practice if the Notice of Privacy Practice includes a statement regarding exceptions to the right to revoke and a description of how the individual may revoke the authorization.

9. A statement of [*Organization*]*'s* ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

   a. [*Organization*] may not condition treatment on whether the individual signs the authorization when it is prohibited to do so; or

   b. The consequences to the individual of a refusal to sign the authorization when [*Organization*] may condition treatment on failure to obtain such authorization.

10. A statement that the potential for information disclosed pursuant to the authorization to be subject to disclosure by the recipient and no longer be confidential by the HIPAA Regulations.

If [*Organization*] seeks an authorization from an individual for a use or disclosure of PHI, [*Organization*] must provide the individual with a copy of the signed authorization. A valid authorization may contain additional elements or information provided they are not inconsistent with the required elements.

Substance Use Disorder Patient Records. When dealing with substance use disorder patient records, [*Organization*] may not use or disclose any information about an

individual unless such individual has consented in writing on a form that meets the requirements of Part 2., or unless another limited exception applies. A Part 2 consent form is different from an authorization under the HIPAA Regulations—thus, [*Organization*] and its workforce must be sure to use the appropriate form.

<u>Authorization to Release Information to Others/Minnesota Law</u>. Minnesota Law requires that upon the written request by a spouse, parent, child or sibling of an individual being evaluated for or diagnosed with a mental illness, [*Organization*] must ask the individual whether he/she wishes to authorize a specific person (noted above) to receive information regarding the individual's current or proposed course of treatment.

If the individual so authorizes, the provider will communicate to the designated individual the person's current and proposed course of treatment. Such a consent is valid for one year or for a lesser period specified in the consent or for a different period provided by law.

However, if applicable patient records include substance use disorder records the more stringent requirements of Part 2 take precedence over this Minnesota law requirement. Thus, workforce must make sure that the disclosure is permitted under Part 2. In other words, even if Minnesota law authorizes or compels a disclosure, [*Organization*] must not disclose the substance use disorder patient records if the disclosure is prohibited by Part 2.

Additional information can be found in policy number [Enter], Disclosures of Substance Use Disorder Patient Records.

G. Invalid Authorizations

Authorizations are not valid if the document submitted has any of the following defects:

1. The expiration date has passed or the expiration event is known by [*Organization*] to have occurred.

2. The authorization has not been filled out completely, with respect to a core element or required statement, if applicable.

3. The authorization is known by [*Organization*] to have been revoked.

4. The authorization is compound authorization or been conditioned on individual receiving treatment, payment, enrollment in a health plan, or eligibility for benefits.

5. Any material information in the authorization is known by [*Organization*] to be false.

H. Compound Authorizations

An authorization for use or disclosure of PHI may not be combined with any other document to create compound authorization, except for research studies and the disclosure of psychotherapy notes.

1. An authorization for a research study may be combined with any other type of written permission for the same or another research study. This includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where [*Organization*] has conditioned the provision of research related treatment on the provision of one of the authorizations, as permitted under the HIPAA Regulations, any compound authorization created must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

2. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes

3. An authorization, other than an authorization for a use of disclosure of psychotherapy notes, may be combined with any such authorization under this section, except when [*Organization*] has conditioned the provision of treatment, payment or enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations. The prohibition on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits does not apply to a compound authorization created in accordance with a research study.

I. Prohibition on Conditioning of Authorizations

[*Organization*] may not condition the provision to an individual of treatment, payment, and enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

1. [*Organization*] may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research; and

2. [*Organization*] may condition the provision of health care that is solely for the purpose of creating PHI for the disclosure of the PHI to a third party.

J. Revocation of Authorizations

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

1. [*Organization*] has taken action in reliance thereon; or

2. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

<u>Substance Use Disorder Patient Records.</u> If an authorization pertains to substance use disorder patient records and the revocation is made verbally, [*Organization*] must honor this revocation. However, you should obtain written revocation when possible.

Additional information can be found in policy number [Enter], Disclosures of Substance Use Disorder Patient Records.

K. Documentation

[*Organization*] must document and retain any signed authorization according to the HIPAA Regulations and its policy on documentation.

II. **Procedure:**

A. When [Organization] and its staff requests information or receives a request from another person related to PHI, it will adhere to the above policy prior to using or disclosing such PHI.

B. If a personal representative has authority to act for the consumer there must be a description of that authorization and the personal representative must sign the document.

C. The consumer and/or the personal representative must receive a copy of the completed authorization prior to being sent to the person requesting information.

D. A client may revoke an authorization at any time, provided that the revocation is in writing except to the extent that [*Organization*] has relied on the authorization to request information to date.

E. All signed authorizations must be placed in the client's chart/file. These records are kept in each program for seven years before being destroyed.

F. The [compliance officer/privacy officer/other designee] will document the request or release on the [*Organization*] Accounting for Disclosure of PHI form.

HIPAA Authorization Checklist

Required Elements The following elements/statements must appear in a HIPAA authorization form.		
164.508(c)(1): Core Elements: An authorization must include the following:	**Notes**	**Check-off**
(1) **Description**. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion		
(2) **Name of disclosing person/entity**. The name (or other specific identification) of the person (or class of persons) authorized to use or disclose information.		
(3) **Name of receiving person/entity**. The name (or other specific identification) of the person (or class of persons) authorized to receive or use information		
(4) **Purpose**. A description of the purpose for the use or disclosure. The statement "at the request of the individual" is sufficient if the individual initiates the authorization and does not provide additional information regarding the purpose.		
(5) **Expiration date/event**. The statement, "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research.		
(6) **Date/Signature**. The date and signature of the individual providing the authorization. If signed by an authorized representative, it must also include a description of the representative's authority to act on behalf of the individual.		
164.508(c)(1): Required Statements. The authorization must include a statement describing:	**Notes**	**Check-off**
(1) **The right to revoke**. Must state that the individual has a right to revoke the authorization in writing and either: (A) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (B) if exceptions to the right to revoke are addressed in the Notice of Privacy Practices, a reference to such Notice.		
(2) **Ability/Inability to condition services on authorization**. Must state either: (A) the CE may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs an authorization; or (B) the consequences to the individual of a refusal to sign the authorization.		
(3) **Redisclosure**. The potential for information disclosed to be subject to a redisclosure by the recipient and no longer protected by the Privacy Rule.		
Other requirements	**Notes**	**Check-off**
(1) **Plain Language**. The authorization must be written in plain language.		
(2) **Copy**. CE must provide the individual with a copy of the signed authorization.		
(3) **Compound authorizations**. The authorization is not combined with any other document unless: (1) the authorization is for use and disclosure of PHI		

Required Elements The following elements/statements must appear in a HIPAA authorization form.		
for a research study, and it is combined with another type of written permission for the same or another research study (provided such compound authorization clearly differentiates between any conditioned and unconditioned research components on the provision of such authorization); (2) the authorization is for a use or disclosure of psychotherapy notes and is combined with another authorization for a use or disclosure of psychotherapy notes; (3) the authorization is combined with another authorization (other than an authorization for a use or disclosure of psychotherapy notes), provided a CE has not conditioned the provision of treatment, payment, enrollment in health plan, or eligibility for benefits on the signing of one of the authorizations (unless such authorization is for number (1) above).		
(4) **Marketing**. If the authorization is for marketing, and the marketing involves financial remuneration to the CE from the third party, the authorization must state that such remuneration is involved.		
(5) **Sale of PHI**. If the authorization is for sale of PHI, the authorization must state that the disclosure will result in remuneration to the CE.		

[Enter Organization Logo]

DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

Policy Number: [Enter]
Effective Date: [Enter]

The HIPAA Privacy Rule allows, but does not require, Covered Entities to disclose PHI without the patient's consent in response to certain judicial and administrative processes. *See* 45 C.F.R. § 164.512(e). However, the Minnesota Health Records Act allows disclosure of health records without the patient's consent only pursuant to "specific authorization in law." Minn. Stat. § 144.293, subd. 2(2).

I. Disclosures for Judicial and Administrative Proceedings Policy:

A. Purpose

This policy establishes guidelines for [*Organization*] to follow regarding the disclosure of PHI in response to a subpoena, court order, or other lawful process originating from a judicial or administrative proceeding.

B. In General

In accordance with the requirements and restrictions outlined in this policy, [*Organization*] may use or disclose PHI, without the written authorization of the individual or giving the individual the opportunity to agree or object, in response to an order of a court or administrative tribunal or some other mandate in applicable state or federal law, provided that *[Organization]* discloses only the PHI expressly authorized by such order or mandate.

Alternatively, [*Organization*] may disclose PHI in the context of judicial and administrative proceedings if this occurs pursuant to the written authorization of the patient. For information regarding the content of the authorization and other information about authorization forms, refer to policy number [*Enter*], Authorization for Use and Disclosure of PHI.

C. Minimum Necessary

[*Organization*] must limit it use and disclosure of PHI pursuant to this policy to the minimum necessary to accomplish the intended purpose of the use or disclosure. For information regarding the requirements of the minimum necessary rule, refer to policy number [*Enter*], Minimum Necessary Requests for, or Uses or Disclosures of, PHI.

D. Minnesota Law

[*Organization*] may disclose PHI in the context of judicial and administrative proceedings pursuant to a request accompanied by a court order. Examples of court orders include: (a) Minnesota state court order; (b) Minnesota federal court order; (c) order signed by a Minnesota judge or administrative law judge; (d) subpoena accompanied by a Minnesota court order, etc.

[*Organization*] may also disclose PHI in this context pursuant to another "specific authorization in law." For example, Minnesota Statutes section 256B.27 provides that the Minnesota Commissioner of Human Services shall be allowed access to all personal medical records of medical assistance recipients for the purposes of investigating vendors of medical care or whether the medical care was medically necessary.

E. Other Disclosures Permitted by HIPAA

1. Satisfactory Assurance

Although the Minnesota Health Records Act may only permit disclosure of health records based on "specific authorization in law"—which is generally interpreted as requiring an order of a court or an administrative tribunal or some other mandate of federal or state law—HIPAA does not prohibit [*Organization*]'s use or disclosure of PHI, without the written authorization of the individual or giving the individual the opportunity to agree or object, in the course of any judicial or administrative proceeding as follows:

a. In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if [*Organization*] receives "satisfactory assurance" from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request. Such "satisfactory assurance" shall require a written statement and accompanying documentation demonstrating that:

    i. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

    ii. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and

    iii. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and: (A) No objections were filed; or (B) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

b. In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if [*Organization*] receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a "qualified protective order" that meets the requirements of this policy. Such "satisfactory assurance" shall require a written statement and accompanying documentation demonstrating that:

i. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

ii. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

2. **A Qualified Protective Order**

For the purposes of this policy a "qualified protective order" with respect to PHI means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

a. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

b. Requires the return or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

3. **Disclosure without Satisfactory Assurance**

HIPAA permits [*Organization*] to disclose PHI in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, without receiving satisfactory assurance, if:

a. [*Organization*] makes reasonable efforts to provide notice to the individual, including sufficient information about the litigation or proceeding in which the PHI is requested, to permit the individual to raise an objection to the court or administrative tribunal; or

b. [*Organization*] makes reasonable efforts to provide notice to the individual, including sufficient information about the litigation or proceeding in which the PHI is requested, to permit the individual to seek a qualified protective order.

<u>Substance Use Disorder Patient Records.</u> [*Organization*] may disclose substance use disorder patient records in response to a subpoena if the patient signs a consent permitting a release of the information requested in the subpoena. However, if the patient does not provide consent, [*Organization*] cannot release substance use disorder patient records unless a court also issued an order that complies with 42 C.F.R. Part 2. *See* 42 C.F.R. § 2.61.

<u>Witness Testimony.</u> Physicians, surgeons, dentists, chiropractors, registered nurses, psychologists, consulting psychologists, licensed social workers, and chemical dependency counselors, among others, must comply with Minnesota Statutes section 595.02 when testifying as a witness or when involved in discussions pursuant to an action for malpractice, error, mistake, or failure to cure against [*Organization*].

4. **Documenting Disclosures of PHI under this Policy**

[*Organization]* will document any disclosures under this policy and will retain the documentation associated with the disclosure for at least six (6) years from the date of the disclosure.

II. Disclosures for Judicial and Administrative Proceedings Procedure:

A. [*Organization*]'s Privacy Official or designee will comply with the above stated policy and ensure the compliance of other Workforce members.

B. In the event [*Organization*]'s Workforce have questions about whether specific authorization in law exists for a disclosure, or whether a document styled as a "court order" is sufficient to meet the obligations of this policy, HIPAA, the Minnesota Records Act or other applicable provisions of federal or state law, they will consult with [*Organization*]'s Privacy Official.

C. [*Organization*]'s Privacy Official or designee will document any such releases in a manner that will allow [*Organization*] to provide an accounting of disclosures to patients.

D. [*Organization*]'s Privacy Official or designee will document related information in the patient's chart.

[Enter Organization Logo]

USE AND DISCLOSURE OF PHI FOR MARKETING

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes guidelines for *[Organization]*'s workforce to follow regarding the use or disclosure of PHI for marketing purposes.

B. Policy Implementation

[Organization] may use and disclose PHI for marketing purposes only in accordance with the HIPAA Regulations, applicable state law, and this Policy.

1. **Authorization for use or disclosure of PHI for marketing**

Except as provided in section 2 of this policy, *[Organization]* must obtain a valid HIPAA authorization, as defined by the Regulations, from the patient or a personal representative prior to any use or disclosure of PHI for "marketing" as defined in section 3 of this policy. The authorization required by this section must be a signed document that meets the requirements of 45 C.F.R. § 164.508 and Policy number [Enter], Authorization for Use and Disclosure of PHI.

In addition, if the marketing involves "financial remuneration" from or on behalf of a third party, the authorization must state that such remuneration is involved. Information on what constitutes "financial remuneration" is included in section B.3, below.

The Minnesota Health Records Act requires "consent" for the disclosure of a patient's health records for marketing. An authorization for marketing that meets the requirements of the HIPAA Regulations will satisfy the consent requirements under the Minnesota Health Records Act. However, a consent that satisfies the Minnesota Health Records Act may not necessarily include all of the elements required for a valid HIPAA authorization required to permit uses and disclosures of PHI for marketing.

2. **Exceptions to the authorization requirement**

[Organization] need not obtain the patient's authorization if the communication is:

a. A face-to-face communication made by *[Organization]* to an individual; or

b. A promotional gift of nominal value provided by *[Organization]*.

3. **"Marketing" defined**

a. Except as provided in paragraph (2) of this definition, *marketing* means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

b. *Marketing* does not include a communication made:

   i. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by *[Organization]* in exchange for making the communication is reasonably related to *[Organization]*'s cost of making the communication.

   ii. For the following treatment and health care operations purposes, except where *[Organization]* receives financial remuneration in exchange for making the communication:

      (1) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

      (2) To describe a health-related product or service (or payment for such product or service) that is provided by *[Organization]*; or

      (3) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of "treatment" in the Regulations.

Authorization is not required for these uses unless *[Organization]* receives "financial remuneration" in exchange for making the marketing communication and the remuneration is provided by or on behalf of the entity whose product is being described. The term "financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described. The term does not include any payment for treatment of an individual. To trigger the authorization and disclosure requirements described in this policy, the financial remuneration *[Organization] r*eceives from a third party must be for the purpose of making a communication and such communication must encourage individuals to purchase or use the third party's product or service.

Thus, for example, an authorization is required if *[Organization]* intends to make a communication to its patients regarding the acquisition of mammography screening equipment if the equipment manufacturer paid *[Organization]* to send the communication. An authorization is not required, however, if a local charitable organization, such as a breast cancer foundation, funded *[Organization]*'s mailing to patients about the new equipment. Similarly, if a third party provides financial remuneration to *[Organization]* to implement a program, such as a disease management program, *[Organization]* could provide individuals with communications about the

program without obtaining an authorization as long as the communications are about *[Organization]*'s program itself, and not about encouraging individuals to use or purchase the third party's product or service.

The consent requirements of the Minnesota Health Records Act are pertinent to the types of disclosures described in section 3(2) even though those disclosures are excluded from HIPAA's definition of marketing. However, the language used by health care providers in consent forms will often be sufficiently broad to encompass the types of disclosures described in that section within the scope of what is otherwise permitted under the consent. *[Organization]* should confirm that its approach to obtaining consent sufficiently addresses disclosures of health records for any activities described in section 3(2).

4. **Business Associates**

If *[Organization]* contracts with a business associate to assist it in the use or disclosure of PHI for marketing, *[Organization]* must have a business associate agreement consistent with Policy number [Enter], Disclosing Information to Business Associates, with the business associate that addresses these activities. The business associate agreement should ensure that the business associate's use or disclosure of PHI for marketing purposes is consistent with this policy. In addition, business associates may not use or disclose PHI from *[Organization]* to engage in marketing on behalf of the business associate itself, unless the patient has signed an authorization for this activity that meets the requirements of Policy number [Enter], Authorization for Use and Disclosure of PHI.

II. Procedure:

A. Prior to using PHI for marketing purposes, *[Organization]*'s Privacy Official or designee must:

1. Determine whether the proposed communication at issue is "marketing" as defined in Section 3 of this policy.

2. If the proposed communication is not marketing, determine whether *[Organization]*'s consent form is sufficient to permit any disclosure of health records for the communication.

3. Verify that a consent has been obtained, if it is determined that a consent is needed;

4. If the communication is marketing, determine if an authorization is required for the use or disclosure of the PHI;

5. Verify that a valid authorization has been obtained, if it is determined that an authorization is needed;

6. Verify that the other requirements described in this policy have been met.

[Enter Organization Logo]

USE AND DISCLOSURE OF MENTAL HEALTH RECORDS

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes guidelines to be followed by *[Organization]*'s workforce when using or disclosing Mental Health Records, including Psychotherapy Notes.

B. Policy Implementation—General Rule

[Organization] must obtain patient consent prior to disclosing Mental Health Records, unless an exception to the consent requirement under Minnesota law applies. Workforce should refer to policy [enter], Consent to Use and Disclose Health Information under Minnesota Law, for more information about disclosures under Minnesota law and these exceptions.

Although disclosure of Mental Health Records is generally permitted with patient consent, special rules do apply to certain types of records (e.g., Psychotherapy Notes) and certain disclosure scenarios (e.g., disclosure to law enforcement). Many of these special rules are set forth in this policy.

The terms "Mental Health Records" and "Psychotherapy Notes" have different meanings. "Mental Health Records" is not defined under Minnesota Law. It is a broad term that refers to information, whether oral or recorded, that relates to the past, present, or future mental health or condition of an individual. Minnesota has specific rules that apply to the disclosure of Mental Health Records in certain circumstances. Several examples of these circumstances are described in this Policy (Sections E-G).

In contrast, "Psychotherapy Notes" has a very specific definition under HIPAA and means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. "Psychotherapy Notes" excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following terms: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

C. Use or Disclosure of Psychotherapy Notes

[*Organization*] must obtain HIPAA authorization for any use or disclosure of Psychotherapy Notes. As described in Section B, the term "Psychotherapy Notes" is specifically defined under HIPAA.

However, authorization is not required for the following Uses and Disclosures of Psychotherapy Notes:

1. Use by the originator of the Psychotherapy Notes for treatment;
2. Use or disclosure by [*Organization*] for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
3. Use or disclosure by [*Organization*] to defend itself in a legal action or other proceeding brought by the individual;
4. Use or disclosure that is required by the Secretary to investigate or determine [*Organization*]'s compliance with the HIPAA Privacy Rule;
5. Use or disclosure that is Required by Law;
6. Use or disclosure by [*Organization*] for health oversight activities to health oversight agencies with respect to the oversight of the originator;
7. Use or disclosure about decedents to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; or
8. Use or disclosure to avert a serious threat to health or safety pursuant to 45 C.F.R. § 164.512(j)(1)(i).

For information regarding the content of the authorization and other information about HIPAA authorization forms, refer to policy number [Enter], Authorization for Use and Disclosure of PHI.

<u>Minnesota Law</u>. Minnesota law generally requires patient consent prior to disclosing Health Records, which includes Psychotherapy Notes. In situations where *[Organization]* is not required to obtain HIPAA authorization for the disclosure of Psychotherapy Notes, *[Organization]* must nonetheless address Minnesota law by either obtaining patient consent permitting the disclosure or meeting an exception to the consent requirement. If *[Organization]* obtains HIPAA authorization for the release of Psychotherapy Notes, this consent requirement is satisfied. However, the consent requirement is <u>not</u> satisfied when the disclosure scenario falls within an exception to the authorization requirement under HIPAA unless the basis for disclosure without authorization also qualifies as basis for a permitted disclosure without consent in Minnesota.

For more information on consent requirements under Minnesota law, refer to policy [enter], Consent to Use and Disclose Health Information Under Minnesota Law.

D. Use and Disclosure of Substance Use Disorder Records

If an individual's Mental Health Record contains substance use disorder information subject to 42 C.F.R. Part 2 (the federal *Confidentiality of Substance Use Disorder Patient Records* regulations), *[Organization]* must comply with the stricter Part 2 requirements for this information. Specifically, *[Organization]* may not use or disclose any information about an individual unless such individual has consented in writing on a form that meets the requirements of Part 2, or unless another limited exception applies. A Part 2 consent form is different from an authorization under the HIPAA Regulations—thus, *[Organization]* and its workforce must be sure to use the appropriate form.

Additional information can be found in policy number [Enter], Disclosures of Substance Use Disorder Patient Records.

E. Communicating with a Patient's Family, Friends, or Other Persons who are Involved in the Patient's Care

As described in Section I.B, Mental Health Records are subject to the same requirements related to consent as other types of Health Records. Minnesota law establishes several specific rules related to additional categories of disclosures of Mental Health Records, however. For example:

1. General Rule

Regardless of the general requirement under Minnesota Law to obtain consent for disclosing Health Records, when providing mental health care and treatment, *[Organization]* may disclose certain types of information to the patient's family member or other caretaker who requests the information when the following requirements are met:

1. The request is in writing;
2. The family member or other person lives with, provides care for, or is directly involved in monitoring the treatment of the patient;
3. The involvement of the family member or caretaker is verified by *[Organization]* or a person other than the person requesting the information, and is documented in the patient's medical record;
4. Before the disclosure, *[Organization]* informs the patient, in writing, of:
    a. The request;
    b. The name of the person requesting the information;
    c. The reason for the request; and
    d. The specific information being requested

5. The patient agrees to the disclosure, does not object to the disclosure, or is unable to consent or object, and the patient's decision or inability to make a decision is documented in their medical record; and
6. The disclosure is necessary to assist in the provision of care or monitoring of the patient's treatment.

The information that may be disclosed under this exception is limited to:

1. Diagnosis;
2. Admission to or discharge from treatment;
3. The name and dosage of the medications prescribed;
4. Side effects of the medication;
5. Consequences of failure of the patient to take the prescribed medication; and
6. A summary of the discharge plan.

However, if *[Organization]* reasonably determines that providing the above information would be detrimental to the physical or mental health of the individual whose information is to be disclosed, or is likely to cause the individual to inflict self-harm or harm to another, *[Organization]* must not disclose the information.

HIPAA. HIPAA allows providers to communicate with a patient's family members, friends, or other caretakers in certain circumstances. Specifically, if the patient is present and has capacity to make health care decisions, HIPAA permits a provider to disclose information to caretakers if the provider: (1) gives the patient the opportunity to object to the disclosure (and the patient does not object); (2) reasonably infers from the circumstances, based on professional judgment, that the patient does not object; or (3) the patient agrees to the disclosure.

If the patient is not present or is incapacitated, HIPAA permits providers to share information with caretakers if the provider determines, based on professional judgment, that sharing the information is in the best interests of the patient. In this scenario, the provider may only disclose information that is directly relevant to the caretaker's involvement with the patient's care or payment for care.

However, the HIPAA rules described above are limited by the Minnesota law requirements, described in Section E(1), on the disclosure of Mental Health Records. Consequently, *[Organization]* and its workforce must comply with Minnesota law prior to disclosing Mental Health Records to a patient's caretaker.

2. **Written Request of a Spouse, Parent, Child or Sibling**

Upon the written request of a spouse, parent, child, or sibling of an individual being evaluated for or diagnosed with mental illness, *[Organization]* must ask the individual

whether he/she wishes to authorize the spouse, parent, child, or sibling to receive information regarding the individual's current or proposed course of treatment.

If the individual so authorizes, the provider will communicate to the designated individual the person's current and proposed course of treatment. Such consent is valid for one year or for a period specified in the consent or for a different period provided by law.

F. Emergency Situations

1. Mental Health Records

[Organization] may disclose Mental Health Records without obtaining prior consent from the patient, or complying with rules set forth in Section E above, if the situation satisfies the "emergency exception" under Minnesota law. The "emergency exception" permits disclosure without patient consent if:

a. The patient is experiencing a medical emergency; and

b. *[Organization]* is unable to obtain the patient's consent to disclosure due to:

   a. The patient's condition; or

   b. The nature of the medical emergency.

If these elements are satisfied, *[Organization]* and its staff may disclose Mental Health Records without patient consent. However, if these elements are <u>not</u> satisfied *[Organization]* must obtain patient consent or fall within a different exception to the consent requirement under Minnesota law. For more information on consent requirements under Minnesota law, refer to policy [enter], Consent to Use and Disclose Health Information Under Minnesota Law.

2. Psychotherapy Notes

[Organization] may disclose Psychotherapy Notes in an emergency situation if:

a. *[Organization]* obtains HIPAA authorization; or
b. The disclosure falls within an exception to the HIPAA authorization requirement for psychotherapy notes and:
   i. The scenario qualifies as an "emergency exception" under Minnesota law, as set forth above in Section I.F.1;
   ii. The disclosure qualifies as a disclosure for which there is specific authorization in law pursuant to Minn. Stat. § 144.293, subd. 2(2); or
   iii. *[Organization]* obtains patient consent.

Exceptions to the HIPAA authorization requirement are set forth in Section I.C. The exception set forth in Section I.C.8 is particularly relevant in the context of an emergency (use or disclosure to avert a serious threat to health or safety pursuant to 45 C.F.R. § 164.512(j)(1)(i)). Under this authorization exception, *[Organization]* may disclose

Psychotherapy Notes without obtaining HIPAA authorization if *[Organization]*, in good faith, believes that the use or disclosure:

i. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
ii. Is to a person reasonably able to prevent or lessen the threat, including the target of the threat.

G. Disclosures to law enforcement

[Organization] must disclose Mental Health Records to a law enforcement agency if the law enforcement agency provides the name of the patient and communicates that:

1. The patient is currently involved in an emergency interaction with the law enforcement agency; and
2. The disclosure is necessary to protect the health or safety of the patient or another person.

If these requirements are satisfied, *[Organization]* must disclose the Mental Health Records. However, the disclosure must be limited to the minimum necessary for law enforcement to respond to the emergency.

If a disclosure is made the law enforcement agency is required to maintain a record that describes who made the request, the fact that *[Organization]* provided the information, and the patient's name. The health records will remain private data on individuals under the Minnesota Data Practices Act and cannot be used by law enforcement for any other purpose.

Substance Use Disorder Records. Special rules apply disclosures of substance use disorder records to law enforcement. Workforce should consult with the *[compliance officer/privacy officer/other designee]* prior to disclosing substance use disorder records to law enforcement.

II. Procedure:

Prior to disclosing Mental Health Records, *[Organization]* staff should do the following:

A. Determine what types of records are involved: (1) general Mental Health Records; (2) Psychotherapy Notes; and/or (3) substance use disorder records. Follow the procedures for each set forth below.

B. General Mental Health Records (without Psychotherapy Notes or substance use disorder records)

1. Obtain patient consent to the disclosure (or confirm whether existing consent addresses the disclosure);

a. Consent must be in writing, signed, and dated;

b. Make a copy of the consent form for the patient's chart/file

2. If patient consent cannot be obtained, determine whether the situation falls within an exception to the consent requirement;

a. If the situation does fall within an exception to the consent requirement, disclosure is permitted.

b. If the situation does not fall within an exception to the consent requirement, staff must not disclose the records.

C. Psychotherapy Notes

1. Authorization:

a. Complete *[Organization]*'s template Authorization Form assuring that all blanks are completed;

b. Review the form and rationale for use and disclosure of PHI with the patient;

c. Request that the patient sign and date the form; and

d. Make a copy of the completed and signed form for the patient's chart/file; or

e. If presented with a different authorization form from the requesting authority, verify that the form is valid and place in the patient's chart/file.

2. Exception to Authorization: determine whether provider qualifies for an exception as outlined in Section I.C of this policy and the Privacy Rule.

D. Substance Use Disorder Records

1. Obtain the patient's consent to disclosure that satisfies Part 2 requirements;

a. Make a copy of the consent form for the patient's chart/file

2. If Part 2 patient consent cannot be obtained, determine whether the situation falls within an exception to the Part 2 consent requirement;

a. If the situation does fall within an exception to the Part 2 consent requirement, disclosure is permitted.

3. If the situation does not fall within an exception to the Part 2 consent requirement, staff must not disclose the records.

B. Follow the procedures set forth in this policy for any unique disclosure scenarios.

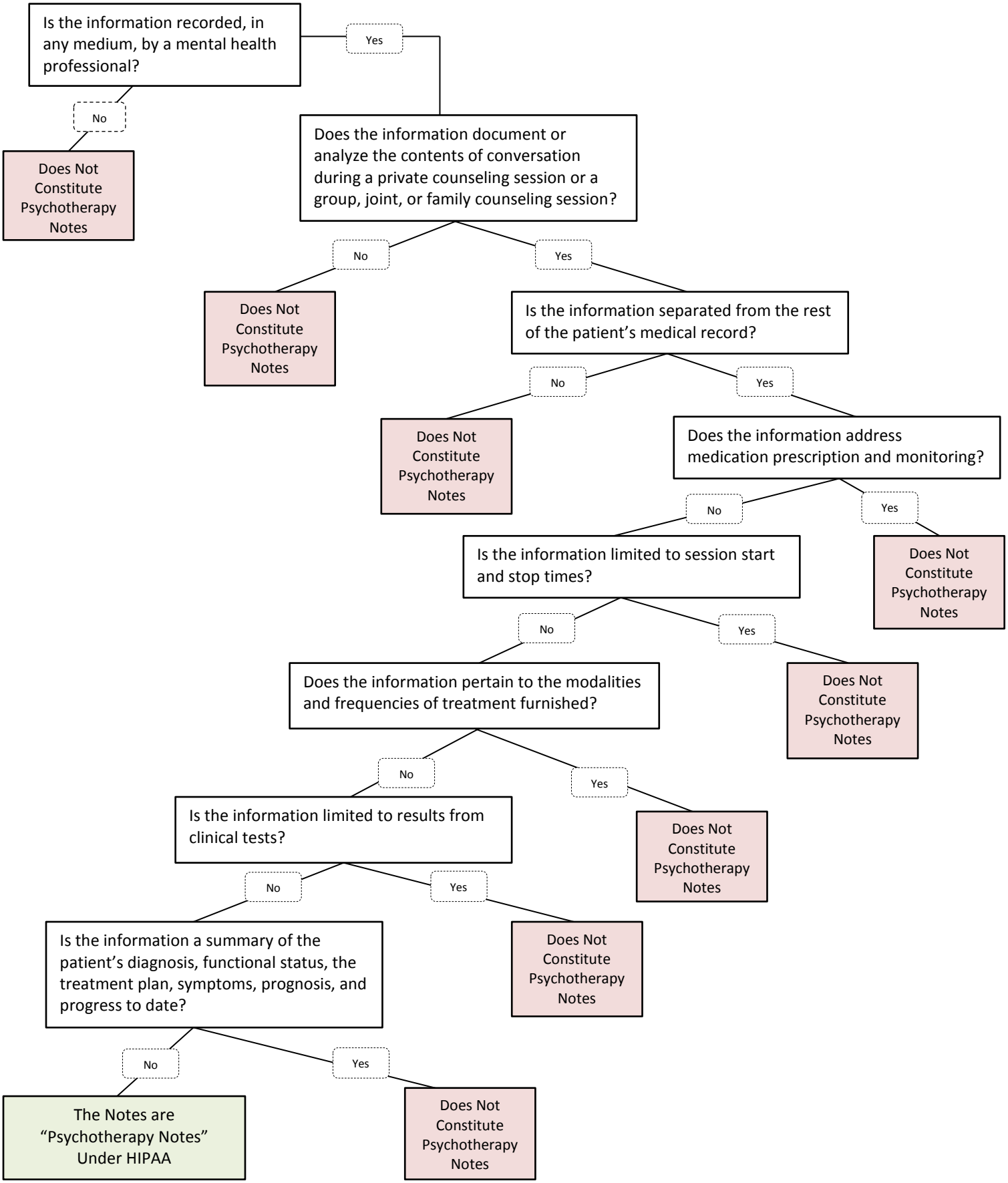
C. If a disclosure is made:

1. Make copies only of the information identified to be used or disclosed and agreed upon by the patient on their authorization/consent form;

2. Document the disclosure in the patient's record and/or on the *[Organization]* Accounting for Disclosure of PHI.

3. Provide the information to the requesting individual in a non-digital mode, i.e. fax or mail.

Are the Notes "Psychotherapy Notes" Under HIPAA?



[Enter Organization Logo]

MINIMUM NECESSARY FOR REQUESTS FOR, OR USES OR DISCLOSURES OF, PHI

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

The purpose of this policy is to limit the use and disclosure of PHI to only that which is needed for the purpose of the disclosure, in situations where the minimum necessary principle applies.

B. Policy Implementation – General Rule

When using or disclosing PHI or when requesting PHI from another covered entity or business associate, *[Organization]* or *[Organization]'s* business associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

For all uses, disclosures, and requests where the minimum necessary rule applies, [*Organization*] may not use, disclose, or request the entire medical record, unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

1. **Situations where the minimum necessary rule does not apply**

[*Organization*] and its workforce are not required to comply with the minimum necessary rule in the following situations:

a. Disclosures to a health care provider for treatment or requests by *[Organization]* for treatment;

b. Uses or disclosures to the individual that is the subject of the information as:

   i. Permitted under 45 C.F.R. 164.502(a)(1)(i);

   ii. Required upon request for access; or

   iii. Required under the individual's right to an accounting of disclosures.

c. Uses or disclosures pursuant to an authorization;

d. Disclosures made to the Secretary of the Department of Health and Human Services;

e. Uses and disclosures that are required by law; and

f. Uses and disclosures required for compliance with the requirements of the HIPAA Regulations.

2. **Minimum Necessary Uses of PHI**

[Organization] shall identify the job positions and/or persons in its workforce who need access to PHI to carry out their duties, along with the categories of PHI to which access is needed. For each position and/or person, *[Organization]* shall make reasonable efforts to limit access to only the categories of PHI to which access is needed.

3. **Routine and Recurring Disclosures or Requests**

For any type of disclosure or request made on a routine and recurring basis, *[Organization]* shall limit the PHI to the amount reasonably necessary to achieve the purpose of the disclosure or request. *[Organization]* has a procedure that limits the PHI disclosed to the amount that is reasonably necessary to accomplish the purpose of the disclosure or request.

4. **Other Disclosures or Requests**

For all other disclosures or requests, *[Organization]* must:

a. Develop criteria designed to limit the request for or disclosure of PHI to the information reasonably necessary to accomplish the purpose for which the request or disclosure is made.

b. Review requests for disclosure on an individual basis in accordance with such criteria.

5. **Disclosures where *[Organization]* may rely on a requested disclosure as the minimum necessary**

In certain circumstances, [*Organization*] may rely on the judgment of the person requesting the disclosure as to the minimum amount of information that is needed. In other words, [*Organization*] does not need to independently confirm that it is providing only the minimum amount of information necessary to accomplish the intended purpose. This reliance is permitted when the request is made by:

a. A public official or agency who states that the information requested is the minimum necessary for the stated purpose and the disclosure is for a purpose permitted under 45 CFR 164.512;

b. Another covered entity;

c. A professional who is a member of *[Organization]'s* workforce or a business associate of *[Organization]* when the purpose of the disclosure is to provide

professional services to *[Organization]*, if the professional represents that the information requested is the minimum necessary; or

d. A researcher with appropriate documentation or representations that comply with the HIPAA Regulations' requirements on uses and disclosures for research.

II. Procedure:

A. *[Organization]* and its workforce will apply the minimum necessary rules outlined in this policy to uses, disclosures, and requests for PHI.

B. The [*compliance officer/privacy officer/other designee*] shall review each non-routine and non-recurring disclosure of PHI prior to the disclosure to ensure that the disclosure complies with this policy;

C. The [*compliance officer/privacy officer/other designee*] shall identify and document which members of the workforce need access to PHI to carry out their duties, the type or category of PHI that is needed by those members of the workforce, and any conditions that are appropriate for their access to that PHI;

D. The [*compliance officer/privacy officer/other designee*] shall be responsible for implementing mechanisms and processes that limit workforce members' access to PHI to the minimum necessary to carry out their duties; and

E. The [*compliance officer/privacy officer/other designee*] shall ensure that employees are trained on the application of the minimum necessary rule and this policy.

ADDITIONAL REQUIREMENTS
UNDER THE
MINNESOTA DATA PRACTICES ACT

I. Application

The Foundations in Privacy Toolkit (the "Toolkit") contains template documents to address common issues faced by health care providers subject to HIPAA and the Minnesota Health Records Act. These template documents do not incorporate additional obligations that apply to providers subject to the Minnesota Government Data Practices Act (the "DPA"), such as governmental entities and private providers under contract with the state (collectively, "DPA Providers").

The purpose of this guidance document is to incorporate common DPA provisions into the template Toolkit documents. DPA Providers should revise the Toolkit documents as set forth below.

Disclaimer: This document includes only those provisions that are most commonly applicable to DPA Providers. It does not set forth every DPA provision that may apply and there are various scenarios that require further analysis and review. For example, the DPA sets forth a specific rule for directory information held by public hospitals (See Minn. Stat. § 13.384, subd. 2(c)). This guidance document does not address that rule. Similarly, this guidance document does not address those specific privacy duties that arise by virtue of a provider's licensure category. DPA Providers should review the DPA and make additional revisions to Toolkit documents, as applicable.

II. Toolkit Revisions

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
Policy: Disclosing Information to Business Associates		
Section B.4 Requirements for Business Associate Agreements	Minn. Stat. § 13.05, subd. 11 and subd. 6	Add new subsection (n): "*Provide that the Business Associate is subject to the Data Practices Act and will comply with its requirements with respect to the PHI.*"
Policy: Using and Disclosing Information in an Emergency		
Section I.B Policy Implementation—General Rule	Minn. Stat. § 13.46	If subject to § 13.46, add: "*Data on Individuals collected, maintained, used, or disseminated by a Welfare System are Private Data on Individuals and generally shall not be disclosed. However, [Organization] can disclose the*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		information in connection with an emergency if the disclosure is necessary to protect the health or safety of the patient or other persons."
Section I.B Policy Implementation—General Rule	Minn. Stat. § 13.384, subd. 3	Add new Section C (and adjust numbering): "***Medical Data.*** *Medical Data are Private Data on Individuals (unless the information is Summary Data or a statute specifically provides for a different classification). This means that Medical Data generally shall not be disclosed to others. However, Medical Data can be disclosed to communicate a patient's condition to a family member, health care agent, or other appropriate person in accordance with acceptable medical practice, unless the patient directs otherwise. In addition, Medical Data can be disclosed as required by law.*"
Policy: Using and Disclosing Information for Health Care Operations		
Section I.B Policy Implementation—General Rule ("Minnesota Law" box)	Minn. Stat. § 13.05	Add at the beginning of paragraph: "*Generally, [Organization] may not disclose identifiable private or confidential data on an individual unless it is permitted by the Minnesota Data Practices Act, authorized by the individual, or otherwise allowed by state or federal law. In addition, ...*" [Existing policy language should follow ("Minnesota law generally requires…")].
Policy: Disclosures of Alcohol and Drug Abuse Records		
Section I. Policy	Minn. Stat. § 13.383, subd. 11a(c)	Add new Section I: "***Alcohol and drug counselors subject to the Data Practices Act.*** *[Organization] and its workforce*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		must comply with the requirements for privacy and access to client records obtained in the course of alcohol and drug counseling set forth in Minnesota Statutes Sections 148F.13 and 148F.135."
Section I.E.1 Medical Emergencies	Minn. Stat. § 13.46	In gray "Minnesota Law" box, add following as a new paragraph: "*Pursuant to Minn. Stat. § 13.46, information maintained by the Welfare System can be disclosed in connection with an emergency if the disclosure is necessary to protect the health or safety of the patient or other persons.*"
Policy: Consent to Disclose Health Information Under Minnesota Law		
Section I.A Purpose	N/A	Replace with the following: "*This policy establishes consent requirements for the disclosure of health information as required by the Minnesota Health Records Act and the Minnesota Data Practices Act.*"
Section. I.C Policy Implementation—General Rule (Patient Consent Required)	Minn. Stat. § 13.04 Minn. Stat. § 13.05 Minn. R. 1205.1400	At the end of the section, add: "*To constitute valid consent, the consent must: (1) be voluntary and not coerced; (2) be in writing; (3) [Organization] must explain why the use or disclosure is necessary; and (4) prior to affixing a signature, identify the consequences of giving such consent. Under the Data Practices Act, [Organization] is permitted to interpret the silence of the patient as the giving of implied consent in accordance with Minnesota Rules 1205.1400.*" Add new Section D (and adjust numbering): "***Tennessen***

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		Warning. *[Organization] must provide individuals with a "Tennessen Warning" pursuant to section 13.04 of the Minnesota Data Practices Act. Generally, private data on individuals must not be collected, stored, used, or disclosed for any purposes other than those stated in the Tennessen warning.* *The Tennessen warning must address the following:* *1. The purpose and intended use of the requested data within the collecting government entity;* *2. Whether the individual may refuse or is legally required to supply the requested data;* *3. Any known consequence arising from supplying or refusing to supply private or confidential data; and* *4. The identity of other persons or entities authorized by state or federal law to receive the data."*
Section I.E Specific Authorization in Law	Minn. Stat. § 13.05	Add example of disclosure required by law under the DPA: *"For example, mandated reporters are required by law to disclose information to their local welfare agency when they have reasons to believe a child is being neglected or physically or sexually abused. Similarly, a local social services agency must disclose relevant private data on individuals to a mandated reporter who made the report and who has an ongoing responsibility for the health,*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		education, or welfare of a child affected by the data, in accordance with Minn. Stat. 626.556, subd. 10j." **GPM Note: DPA Providers should include a provision in their Tennessen Warning that states patient information may be disclosed as required by law.**
Section I.F Permitted Disclosures without a Consent	Minn. Stat. § 13.384 Minn. Stat. § 13.3805 Minn. Stat. § 13.46	Add permissible disclosures of Medical Data under Minn. Stat. § 13.384. Add permissible disclosures of Health Data under Minn. Stat. § 13.3805. If subject to § 13.46, add permissible disclosures of data on individuals by the welfare system under Minn. Stat. § 13.46.
Section I.H Duration of Consent	*See* Minn. Stat. § 13.386	Note: Special rules may apply to certain categories of information. For example, unless otherwise provided by law, consent to disseminate genetic information under the DPA is valid for one year or for a lesser period specified in the consent.
Section I.I Consent That Does Not Expire After One Year	Minn. Stat. 144.293, subd. 6	Add: "*3. The disclosure of health information to a program in the welfare system, as defined in section 13.46, to the extent necessary to coordinate services for the patient*."
Policy: Authorization for Use and Disclosure of PHI		
Section I.A ("Minnesota Law" box)	Minn. Stat. § 13.04, subd. 2 Minn. Stat. § 13.05 Minn. R. 1205.1400	Following the first paragraph, add: "*To constitute valid consent under the Minnesota Data Practices Act, the consent must: (1) be voluntary and not coerced; (2) be in writing; (3) [Organization] must explain why*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		the use or disclosure is necessary; and (4) prior to affixing a signature, identify the consequences of giving such consent. Under the Data Practices Act, [Organization] is permitted to interpret the silence of the patient as the giving of implied consent in accordance with Minn. Rules 1205.1400. However, HIPAA does not recognize this concept of implied consent. Thus, when [Organization] is required to obtain patient authorization under HIPAA it must be in writing and satisfy the elements set forth in Section I.F." Following the second paragraph, add: "*[Organization] must provide patients with a "Tennessen Warning" pursuant to section 13.04 of the Minnesota Data Practices Act. Generally, private data on individuals must not be collected, stored, used, or disclosed for any purposes other than those stated in the Tennessen warning. The HIPAA authorization obligations set forth in this policy are in addition to [Organization]'s obligation to provide a Tennesen warning.* *The Tennessen warning must address the following:* *1. The purpose and intended use of the requested data within the collecting government entity;* *2. Whether the individual may refuse or is legally required to supply the requested data;*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		3. Any known consequence arising from supplying or refusing to supply private or confidential data; and *4. The identity of other persons or entities authorized by state or federal law to receive the data."*
Policy: Breach of Unsecured PHI		
Introductory Gray Box	Minn. Stat. § 13.055	Add: "*Government and other entities subject to the Data Practices Act must comply with Minnesota Statutes Section 13.055.*"
Section II. Breach of the Security of the System Policy	Minn. Stat. § 13.055	Delete: "This policy is designed to explain the obligations of non-governmental health care providers." Add to Section II.B.2: "*The Data Practices Act uses a slightly different term: "breach of the security of the data," which has a similar meaning.* *Minn. Stat. § 13.055, subd. 1(a).*" Add to Section II.B.3: "*Such good faith acquisition is also not a breach of the security of the data within the meaning of the Data Practices Act."* Add to Section II.B.5: "*Entities subject to the Data Practices Act must inform all individuals who are the subjects of the data involved in the breach that a report will be prepared documenting an investigation and the final disposition of any disciplinary action imposed on an employee, contractor, or agent of the government entity*."

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		Add to Section II.B.6: *"The Data Practices Act also provides that government entities must notify consumer reporting agencies "without unreasonable delay" if the entity must notify more than 1,000 individuals pursuant to Minnesota Statutes Section 13.055."*
Policy: Minimum Necessary for Requests for, or Uses or Disclosures of, PHI		
Section I.B Policy Implementation—General Rule	Minn. Stat. § 13.05	Add: *"Collection and storage of all data on individuals and the use and disclosure of private and confidential data on individuals must be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government.*"
Section I.B.1 Situations where the minimum necessary rule does not apply	Minn. Stat. § 13.05	Add to introductory paragraph: "*Use and disclosure of private and confidential data on individuals must always be limited to that necessary for the administration and management of programs authorized by the legislature or local governing body or mandated by the federal government. However, if a patient provides valid informed consent, [Organization] is permitted to disclose information in accordance with such consent—which may permit disclosure beyond the minimum necessary. In addition, under HIPAA, ...*" [Existing policy language should follow ("*[Organization]* and its workforce are not required to comply. . . .")].

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
Policy: Disclosures for Judicial and Administrative Proceedings		
Section I.D Minnesota Law	Minn. Stat. § 13.384 Minn. Stat. § 13.46 Minn. Stat. § 13.03, subd. 6 Minn. Stat. § 13.39 Minn. Stat. § 13.04, subd. 3 Minn. Stat. § 13.3805	Replace the first sentence with the following: "*[Organization] may disclose PHI, including data on individuals collected, maintained, used, or disseminated by the welfare system as well as Medical Data, in the context of judicial and administrative proceedings pursuant to a valid court order. Minn. Stat. §§ 13.384, subd. 3 & 13.46, subd. 2.*" Add following the second paragraph: "*The Data Practices Act provides that if an individual is the subject of stored private or public data on individuals, including public health data, the individual may request—and within ten days must be shown—the data without charge and may receive copies of the data.*"
Policy: Use and Disclosure of Mental Health Records		
Section 1.B Policy Implementation—General Rule (Gray Box)	Minn. Stat. § 13.46, subd. 7	Add: "*Mental Health Data are private data on individuals; [Organization] must therefore comply with Section 13.46, subd. 7 of the Minnesota Data Practices Act (the "DPA") when disclosing such information. The DPA does set forth certain scenarios in which disclosure is permitted without patient consent. For example, the DPA permits [Organization] to disclose information to a health care provider governed by the Minnesota Health Records Act to the extent necessary to coordinate services. However, [Organization] must still comply with the consent requirements*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		under the Minnesota Health Records Act and applicable HIPAA requirements."
Policy: Use and Disclosure of PHI for Research Purposes		
Section I.B.1	Minn. Stat. § 13.04, subd. 2 Minn. Stat. § 13.05, subd. 4 Minn. R. 1205.1400 Minn. Stat. § 13.384, subd. 3 Minn. Stat. § 13.46, subd. 2, 5	Add: *"Entities subject to the DPA may use medical data or data on individuals collected, maintained, used, or disseminated by a welfare system for internal and external research purposes if consistent with HIPAA and the MHRA, and the informed consent requirements of the DPA. Such entities may also disclose "summary data" (for research or otherwise) as discussed in Section I.B.9 of this policy."*
Section 5	Minn. Stat. § 13.04, subd. 2 Minn. Stat. § 13.05, subd. 4 Minn. Stat. § 13.384, subd. 3 Minn. Stat. § 13.46, subd. 2, 5	Add following gray box: *"Entities subject to the DPA are required to obtain valid informed consent to disclose private data on individuals, which would include a disclosure for research. The provisions in the "Policy: Consent to Disclose Health Information Under Minnesota Law, Section I.C Policy Implementation—General Rule", as modified by this Additional Requirements Under the Data Practices Document, should be used to address securing appropriate informed consent from the patient in accordance with the DPA for the disclosure of private data on individuals for research".*
Section I.B.9— Limited data set and de-identified health information	Minn. Stat. § 13.05, subd. 7 Minn. R. 1205.0700, subp. 5	Add following gray box: *"Unless otherwise classified by Minnesota Statutes Section 13.06 or another statute, "summary data" as defined in Minnesota Statutes Section 13.02,*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		subdivision 9 is public data to be released upon the request of any person if the request is in writing and the cost of preparing the summary data is borne by the requesting person. The government entity may delegate the power to prepare summary data (1) to the administrative officer responsible for any central repository of summary data; or (2) to a person outside of the entity if the person's purpose is set forth, in writing, and the person agrees not to disclose, and the entity reasonably determines that the access will not compromise private or confidential data on individuals. The person's agreement described in the preceding sentence must contain the following: *A. A general description of the private or confidential data which is being used to prepare summary data;* *B. The purpose for which the summary data is being prepared; and* *C. A statement that the person understands he/she may be subject to the civil or criminal penalties in the event that the private or confidential data is disclosed.* *These terms may be included in a business associate agreement if the party subject to the DPA discloses PHI/private or*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		confidential data to a business associate to create de-identified information/summary data.
Section I.B.7—Alcohol and Drug Abuse Records	Minn. Stat. § 254A.09 Min. Stat. § 13.461	Add: *"The Data Practices Act incorporates other statutes which classify human services data as other than public. The Department of Human Services shall assure confidentiality to individuals who are the subject of research by a division of the Department of Human Services or are recipients of alcohol or drug abuse information, assessment, or treatment from a licensed or approved program. The Department of Human Services shall withhold from all persons not connected with the conduct of the research the names or other identifying characteristics of a subject of research unless the individual gives written permission that information relative to treatment and recovery may be released."*
Policy: Use and Disclosure of PHI for Fundraising		
N/A	Minn. Stat. § 13.792	Note that the DPA classifies certain government entities' data on prospective donors and donors' financial circumstances as private or nonpublic data. However, the names of donors and gift ranges are public data.
Section I.B.1 (Gray Box)	Minn. Stat. § 13.04 Minn. Stat. § 13.384, subd. 3	Add: "*The Data Practices Act requires entities subject to that law to provide an individual asked to supply private or confidential data concerning the individual with information regarding the purpose and the intended use of the requested data and to address the*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		disclosure by obtaining informed consent from the individual. See the provisions in the "Policy: Consent to Disclose Health Information Under Minnesota Law, Section I.C Policy Implementation—General Rule", as modified by this Additional Requirements Under the Data Practices Document, to address these requirements".
Policy: Use and Disclosure of PHI for Marketing		
Section I.B (Gray Box)	Minn. Stat. § 13.04	Add: "*The Data Practices Act also requires entities to inform individuals of the purpose and the intended use of requested data. If applicable, [Organization] should inform individuals of its intent to make disclosures for the activities described in section 3(2).*"
Template Agreement: Business Associate Agreement		
Section I	Minn. Stat. § 13.05, subd. 11	Add at the end of Section I: "*Business Associate acknowledges that it is subject to the Data Practices Act and agrees to comply with applicable Data Practices Act requirements as if it were a government entity.*"
Section I (definition of "Breach")	Minn. Stat. § 13.055	Note: The DPA requires government entities to provide notice to individuals upon a "breach of the security of the data", which is defined as "the unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data." "Unauthorized acquisition" means that a person has obtained, accessed, or viewed government

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		data without the informed consent of the individuals who are the subjects of the data or statutory authority, and with the intent to use the data for nongovernmental purposes. Importantly, "data maintained by a government entity" includes data maintained by a person under a contract with the government entity that provides for the acquisition of or access to the data by an employee, contractor, or agent of the government entity. Good faith acquisition of or access to government data by an employee, contractor, or agent of a government entity for the purposes of the entity is not a breach of the security of the data, if the government data is not provided to or viewable by an unauthorized person, or accessed for a purpose not described in the procedures required by section 13.05, subdivision 5. An unauthorized disclosure may constitute a "breach of the security of the data" but not rise to the level of a breach under HIPAA.
Section II.a	Minn. Stat. § 13.05, subd. 11	Add: "*Business Associate will not use or disclose PHI in a manner that would violate the Data Practices Act.*"
Template Agreement: Subcontractor Business Associate Agreement		
Section I	Minn. Stat. § 13.05, subd. 11	Add at the end of Section I: *"Prime Subcontractor acknowledges that it is subject to the Data Practices Act and agrees to comply with applicable*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		Data Practices Act requirements as if it were a government entity."
Section I (definition of "Breach")	Minn. Stat. § 13.055	Note: The DPA requires government entities to provide notice to individuals upon a "breach of the security of the data", which is defined as "the unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data." "Unauthorized acquisition" means that a person has obtained, accessed, or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority, and with the intent to use the data for nongovernmental purposes. Importantly, "data maintained by a government entity" includes data maintained by a person under a contract with the government entity that provides for the acquisition of or access to the data by an employee, contractor, or agent of the government entity. Good faith acquisition of or access to government data by an employee, contractor, or agent of a government entity for the purposes of the entity is not a breach of the security of the data, if the government data is not provided to or viewable by an unauthorized person, or accessed for a purpose not described in the procedures required by section

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		13.05, subdivision 5. An unauthorized disclosure may constitute a "breach of the security of the data" but not rise to the level of a breach under HIPAA.
Section II.a	Minn. Stat. § 13.05, subd. 11	Add: "*Prime Subcontractor will not use or disclose PHI in a manner that would violate the Data Practices Act.*"
Checklist: Business Associate Agreement Checklist—Required and Optional Terms		
Require Terms	Minn. Stat. § 13.05, subd. 11	Add: "***Data Practices Act:*** *Business Associate acknowledges that it is subject to the Data Practices Act and agrees to comply with applicable Data Practices Act requirements as if it were a government entity"*
Policy: Definitions		
N/A		Add the following Definitions: • ***Breach of the Security of the Data****: means unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data.* • ***Data on Individuals****: All government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual.* • ***Medical data****: Data collected because an individual was or*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		is a patient or client of a hospital, nursing home, medical center, clinic, health or nursing agency operated by a government entity including business and financial records, data provided by private health care facilities, and data provided by or about relatives of the individual. • ***Mental Health Data****: Data on individual clients and patients of community mental health centers, established under section 245.62, mental health divisions of counties and other providers under contract to deliver mental health services, or the ombudsman for mental health and developmental disabilities.* • ***Private data on individuals****: Data made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the individual subject of those data.* • ***[Public] Health Data****: are data on individuals created, collected, received, or maintained by the Department of Health, political subdivisions, or statewide systems relating to the identification, description, prevention, and control of disease or as part of an epidemiologic investigation the commissioner designates as necessary to analyze, describe, or protect the public health.*

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		• ***Summary data***. *Statistical records and reports derived from Data on Individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.* • ***Welfare system****: "Welfare System" includes the Department of Human Services, local social services agencies, county welfare agencies, private licensing agencies, the public authority responsible for child support enforcement, human services boards, community mental health center boards, state hospitals, state nursing homes, the ombudsman for mental health and developmental disabilities, and persons, agencies, institutions, organizations, and other entities under contract to any of the above agencies to the extent specified in the contract.*

[Enter Organization Logo]

CONSENT TO DISCLOSE HEALTH INFORMATION UNDER MINNESOTA LAW

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes consent requirements for the disclosure of health information as required by the Minnesota Health Records Act.

B. Background

[*Organization*] and its workforce are subject to many consent requirements under both state and federal law, which often creates confusion. For example, HIPAA and Minnesota law have different patient consent requirements and use different terminology. The general rule under HIPAA is that PHI may not be *used or disclosed* by *[Organization]* unless the use or disclosure is specifically permitted by HIPAA or authorized by the patient. "Patient Authorization" under HIPAA refers to a very specific type of patient consent. However, Minnesota Law only addresses the *disclosure* of information and generally requires patient consent prior to such disclosure (as opposed to patient authorization required by HIPAA).

[Organization] and its staff must use this policy to determine when "consent" is required under Minnesota law, understand how this is different than patient authorization required by HIPAA, and comply with other consent requirements under Minnesota law.

C. Policy Implementation - General Rule (Patient Consent Required)

Except as described in this policy or unless a disclosure is specifically authorized by law, *[Organization]* shall not disclose an individual's health information without a signed and dated consent authorizing the disclosure from the individual or the individual's legally authorized representative.

Obtaining consent for the disclosure of health information as required by Minnesota Statutes does not satisfy or eliminate the requirement of the HIPAA Regulations to obtain an authorization when such an authorization is required under HIPAA for certain disclosures of PHI.

However, obtaining a valid authorization under the HIPAA Regulations does satisfy the consent requirements under Minnesota Law.

D. Representation From Provider

[*Organization*] may disclose information when there is a representation from a provider that it holds a signed and dated consent from the patient authorizing the release, provided [*Organization*] documents:

- The provider requesting the health records;
- The identity of the patient;
- The health records requested; and
- The date the health records were requested.

E. Specific Authorization in Law

[*Organization*] may disclose health information without patient consent when it is required by law to do so. For example, birth and death records must be reported to the Department of Health. In addition, [*Organization*] is required to disclose instances of tuberculosis. [*Organization*] must document the release in the patient's health record.

F. Permitted Disclosures without a Consent

[Organization] may disclose health information without patient consent:

1. For a Medical Emergency when *[Organization]* is unable to obtain the individual's consent due to the individual's condition or the nature of the Medical Emergency;

2. To other health care providers within Related Health Care Entities when necessary for the current treatment of the individual;

3. To a health care facility licensed by Minnesota Statutes chapter 144, Minnesota Statutes chapter 144A, or to the same types of health care facilities licensed by chapter 144 and chapter 144A that are licensed in another state when a patient:

    a. Is returning to the health care facility and unable to provide consent; or

    b. Who resides in the health care facility, has services provided by an outside resource under 42 CFR section 483.75(h), and is unable to provide consent; or

4. When the disclosure is specifically authorized by law; and

5. When the disclosure is to the commissioner of health or the Health Data Institute under chapter 62J, provided that the commissioner encrypts the patient identifier upon receipt of the data.

6. When *[Organization]* is releasing a deceased patient's health care records to another provider for the purposes of diagnosing or treating the deceased patient's surviving adult child.

If *[Organization]* discloses health information without an individual's consent, and the disclosure was authorized by law, the disclosure must be documented in the individual's health record.

G. Patient Request for Release to Provider

If a patient requests in writing that [*Organization*] release the patient's health records to another provider, or a pertinent portion or summary of their health record, [*Organization*] must promptly comply with this request. The written request must include the name of the provider to whom the health record is to be furnished. [*Organization*] may retain a copy of the health records.

H. Duration of Consent

[GPM Note: Minnesota law allows providers to specify the duration of consent in their consent form. Providers can select any time period of their choosing; a period of longer than one year is permissible. However, it is generally best practice to obtain patient consent on an annual basis. The provision below is drafted to reflect this recommended practice, but can be revised if an organization is comfortable having their consent forms be valid for a period longer than one year.]

Except as described in this policy, consent is valid for:

1. One year, for the specific purposes permitted under the law; or

2. A period less than one year as specified in the consent; or

3. A different period provided by law.

I. Consent That Does Not Expire After One Year

The consent does not expire after one year if an individual explicitly gives informed consent to the disclosure of health information for the following purposes and subject to the following restrictions:

1. The disclosure of health information to a provider who is being advised or consulted in connection with the releasing provider's current treatment of the individual; or

2. The disclosure of health information to an accident and health insurer, health service plan corporation, health maintenance organization, or third-party administrator for the purposes of payment of claims, fraud investigation, or quality of care review and studies, provided that:

    a. The disclosure of the health information complies with the Minnesota Insurance Fair Information Reporting Act at Minnesota Statutes § 72A.49 to 72A.505;

    b. The further use or release of the health information to a person other than the individual who is the subject of the data is prohibited without the individual's consent; and

    c. The recipient of the PHI establishes adequate safeguards to protect the health information from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient.

J. Disclosure of Health Information for Medical or Scientific Research

When disclosing information for research purposes, *[Organization]* and its staff should follow policy number [Enter], Using and Disclosing Information for Research Purposes.

K. Record Locator Service

[*Organization*] may participate in a record locator service ("RLS"), which is an electronic index of patient information that directs providers in a health information exchange to the location of patient records.

1. Releasing Information

[*Organization*] may release patient information, including the location of an individual's health records, to an RLS without prior consent from the patient, provided each patient has had the opportunity to opt out of the RLS. [*Organization*] allows patients to opt out via its Notice of Privacy Practices and template consent form.

If a patient has elected to be excluded from the RLS, [*Organization*] and its staff must obtain patient consent prior to releasing any information to an RLS.

2. Obtaining Information

If [*Organization*] participates in a health information exchange that uses an RLS, [*Organization*] generally must obtain patient consent to access patient information and information about the location of the patient's health records from the RLS. However, [*Organization*] may access such information without patient consent during a Medical Emergency.

If a patient does consent to such access the consent does not expire, but the patient may revoke the consent at any time by providing written notice of the revocation to [*Organization*].

3. Excluding Patient Information from the RLS

[*Organization*]'s template consent form includes a check-box option that allows a patient to exclude all of the patient's information from the record locator service. If [*Organization*] receives a request to exclude all of the patient's information from the RLS, [*Organization*] and its staff must honor this request and may not release information to the RLS. In addition, if patient information was already released [*Organization*] must work with the entity operating the RLS to have the patient's information removed from the RLS.

L. [*Organization*] Warranties Regarding Consents, Requests, and Disclosures

When [*Organization*] and its workforce request health records on the basis that the patient provided signed and dated consent to the release, [*Organization*] and its workforce warrant that the consent:

1. Contains no information that is known to be false;
2. Accurately states the patient's desire to have health records disclosed or that there is specific authorization in law; and
3. Does not exceed any limits imposed by the patient.

When [*Organization*] and its workforce disclose health records, [*Organization*] and its workforce warrant that it:

1. Has complied with the requirements of the Minnesota Health Records Act regarding disclosure of health records;
2. Knows of no information related to the request that is false; and
3. Has complied with the limits set by the patient in the consent.

M. Documentation of Release

In addition to the documentation requirements specifically identified in this policy and other [*Organization*] policies, [*Organization*] must:

1. When releasing health records without patient consent as authorized by law, document the release in the patient's health record; and

2. When releasing mental health records to law enforcement according to Minn. Stat. § 144.294, subdivision 2, document the release in the patient's health record along with:
    a. The date and circumstances for the disclosure;
    b. The person or agency to whom the release was made; and
    c. The records that were released.

II. Procedure:

Except for disclosures permitted without consent, *[Organization]* shall obtain prior written consent for the disclosure of health information prior to disclosing such information. [*Organization*] workforce shall otherwise comply with this policy when using and disclosing information.

[Enter Organization Logo]

EXCHANGING INFORMATION WITH OUT-OF-STATE PROVIDERS

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes guidelines to be followed by *[Organization]*'s workforce when exchanging patient health information with out-of-state providers.

B. Policy Implementation—General Rule

Both *[Organization]* and an out-of-state provider are subject to federal laws, such as HIPAA. However, *[Organization]* and an out-of-state provider are subject to different state laws.

[Organization] must comply with Minnesota law when disclosing patient information to an out-of-state provider. Conversely, the out-of-state provider must comply with its state law when disclosing patient information to *[Organization]*.

C. Releasing Information to an Out-of-State Provider

[Organization] must comply with Minnesota law when releasing information to an out-of-state provider. *[Organization]* staff should refer to policy [enter], Consent to Use and Disclose Health Information under Minnesota Law, for more information about disclosures under Minnesota law.

D. Obtaining Information from an Out-of-State Provider

An out-of-state provider is required to comply with its state law when it releases information to *[Organization]*. This may cause operational barriers for *[Organization]*, as the out-of-state provider may be subject to rules and requirements that *[Organization]* is not familiar with.

It is ultimately the out-of-state provider's responsibility to understand and comply with its state law when disclosing information to *[Organization]*. However, to the extent it is feasible, *[Organization]* staff should facilitate the exchange when it is in the best interests of the patient. This may involve discussing the privacy laws applicable to the out-of-state provider, assessing whether *[Organization]*'s Template Authorization Form would satisfy those requirements, and otherwise assisting the out-of-state provider with meeting its state law requirements (for example, by reviewing the out-of-state provider's consent form with the patient and facilitating signature).

Privacy Laws in Other States. While *[Organization]* and out-of-state providers are all subject to federal privacy laws, such as HIPAA, state privacy laws vary. Some states do

not have a separate state law governing the confidentiality of health information that is more restrictive (i.e., protective of patient privacy) than HIPAA. In those states, the disclosure from the out-of-state provider to *[Organization]* could occur in accordance with HIPAA. For example, the out-of-state provider could release the patient's records, without patient authorization, to *[Organization]* for treatment purposes.

However, some states have privacy laws that are more protective than HIPAA. Minnesota is one example. Out-of-state providers from these states must comply with its state law when disclosing information to *[Organization]* (as well as in using information received from *[Organization]*).

II. Procedure:

Prior to exchanging health information with out-of-state providers, *[Organization]* staff must comply with the following:

A. *[Organization]* staff must comply with Minnesota law when releasing information to an out-of-state provider;

B. When *[Organization]* seeks to obtain information from an out-of-state provider, staff should:

1. Connect with the out-of-state provider to discuss the state privacy requirements applicable to the out-of-state provider;

2. Assess whether disclosure is permitted without patient consent or authorization;

3. If consent or authorization is required, assess whether *[Organization]* has a signed Authorization form on file that would satisfy the out-of-state provider's state law; and

4. Otherwise facilitate the exchange, if doing so is in the best interests of the patient.

[Enter Organization Logo]

USING AND DISCLOSING INFORMATION FOR PAYMENT PURPOSES

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes guidelines to be followed by *[Organization]'s* workforce when using and disclosing information for payment purposes.

B. Policy Implementation – Use of PHI for Payment Purposes

[*Organization*] may use PHI for payment purposes without obtaining prior HIPAA authorization from the patient. Note that use for payment in this context is limited to those internal activities undertaken to obtain reimbursement for the provision of health care services.

C. Disclosure of PHI for Payment Purposes

[*Organization*] is generally required to disclose PHI to obtain reimbursement for the treatment and services it provides. [*Organization*] may disclose PHI for payment purposes without obtaining HIPAA authorization from the patient. [*Organization*] may also disclose PHI to another covered entity or health care provider for the payment activities of that entity.

"Payment" includes activities undertaken by a health care provider, such as *[Organization]*, or a health plan to obtain or provide reimbursement for the provision of health care. In addition, "payment" includes the following activities:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
4. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

6. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
    a. Name and address;
    b. Date of birth;
    c. Social security number;
    d. Payment history;
    e. Account number; and
    f. Name and address of the health care provider and/or health plan.

This list of payment activities is not exclusive—additional activities may be performed to obtain reimbursement for [*Organization*]'s services. Workforce should consult with the [*compliance officer/privacy officer/other designee*] as appropriate.

<u>Minnesota Law</u>. Minnesota law generally requires [*Organization*] to obtain signed and dated patient consent prior to releasing health records, unless certain exceptions apply. [*Organization*] includes general language in its standard consent form indicating that [*Organization*] can disclose patient information for payment purposes. This satisfies the consent requirement under Minnesota law. [*Organization*] states in its Notice of Privacy Practices that it may use and disclose information for payment purposes; if there is language by which patient acknowledges and consents to the activities described as set forth in the Notice of Privacy Practices in *[Organization's]* consent form, this would be an alternative option for the patient to provide the necessary consent under Minnesota law.

<u>Alcohol and Drug Abuse Records</u>. Unique rules apply when [*Organization*] seeks to disclose alcohol and drug abuse records for payment purposes. *[Organization]* must generally obtain signed consent that satisfies Part 2 requirements prior to disclosing information for payment purposes, and each disclosure must be accompanied by a written statement that prohibits third party payers from redisclosing the records. This written statement language and the consent form requirements are set forth in policy number [Enter], Disclosures of Alcohol and Drug Abuse Records.

[*Organization*] may disclose payment information <u>without</u> patient consent to:

1. **A qualified service organization, provided certain requirements are met. Staff should review policy number [Enter], Disclosing Information to Business Associates, for more detail;**

2. **An entity with direct administrative control over [*Organization*]; or**

3. A person for audit and evaluation activities, including a third party payer, when the disclosure complies with the requirements set forth in 42 CFR § 2.53.

D. Disclosure of Minimum Necessary

When [*Organization*] and its workforce use and disclose PHI for payment purposes it must comply with the minimum necessary rule. This means that [*Organization*] can use or disclose only the information that is necessary to achieve the purpose of the disclosure (e.g., to obtain reimbursement for services).

II. Procedure:

When using or disclosing health information for payment purposes, *[Organization]* and its workforce shall:

A. Confirm that the tasks and activities are being performed to obtain reimbursement for the provision of services and constitute "payment" activities in accordance with this policy;

B. Ensure the patient has signed and dated *[Organization's]* consent form that includes language addressing the disclosure of health records for payment purposes or if not has signed and dated *[Organization's]* consent form that includes language acknowledging and consenting to the activities described in *[Organization]*'s Notice of Privacy Practices;

C. If alcohol or drug abuse records are involved, disclose information for payment purposes only in accordance with this policy.

[Enter Organization Logo]

USE AND DISCLOSURE OF PHI FOR RESEARCH PURPOSES

Policy Number: [Enter]
Effective Date: [Enter]

I. Policy:

A. Purpose

This policy establishes guidelines for [*Organization*]'s workforce to follow regarding the use or disclosure of PHI for research purposes.

B. Policy Implementation

1. Overview: Authorization generally required

The use/disclosure of PHI and health records for research purposes is subject to HIPAA and the Minnesota Health Records Act (the "MHRA"). Other requirements may also be relevant, depending on the type of information at issue. For example, if [*Organization*] maintains patient identifying information relating to substance use disorders, the federal Part 2 requirements will apply. *See* Policy Number [*Insert*], "Am I subject to 42 C.F.R. Part 2?" for additional information on Part 2.

Except as otherwise provided, HIPAA and this policy require [*Organization*] to obtain an individual's authorization prior to use or disclosure of that individual's PHI for research. Such authorization must be a signed document that meets the requirements of Policy Number [*insert*] regarding authorizations. The exceptions to this authorization requirement are outlined in Section I.B.4 of this policy. The MHRA does not require consent for [*Organization*] to use health records for [*Organization*]'s internal research. However, even in situations where HIPAA does not require a patient's authorization for disclosures of PHI for research, the MHRA generally requires [*Organization*] to obtain a specific form of consent from the patient prior to release of his or her health records to an external researcher. Finally, different rules will apply if the research involves information that meets the definition of a "limited data set" or "de-identified information." [*Organization*] may use and/or disclose a limited data set and de-identified data for research as permitted by Section I.B.10 of this policy.

2. "Research" defined

HIPAA defines *research* to mean a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Conducting quality assessment and improvement activities, including outcomes evaluation and the development of clinical guidelines is not "research" if the primary purpose of any studies resulting from such activities is not to obtain "generalizable knowledge." Such activities are "health care operations," for which [*Organization*] may use or disclose PHI as provided in Policy Number [*insert*].

3. **Minimum necessary**

[*Organization*] must limit its use and disclosure of PHI pursuant to this policy to the minimum necessary to accomplish the intended purpose of the use or disclosure, unless the minimum necessary requirement does not apply to the use/disclosure at issue or [*Organization*] is permitted to rely on a requested disclosure as meeting the minimum necessary standard. For example, the minimum necessary rule does not apply to uses and disclosures made pursuant to a valid authorization. Likewise, [*Organization*] is permitted to rely on a researcher's documentation of an IRB waiver of authorization (that meets the requirements below) that a requested disclosure satisfies the minimum necessary rule, assuming [*Organization*]'s reliance is reasonable under the circumstances. For information regarding the requirements of the minimum necessary rule and its various exceptions, refer to policy number [*Insert*], Minimum Necessary Requests for, or Uses or Disclosures of PHI.

4. **Exceptions to HIPAA authorization requirement**

[*Organization*] may use or disclose PHI for research without obtaining the individual's authorization only if any of the following are true:

(a) *Board Approval of Waiver of Authorization.* [*Organization*] obtains documentation—*that meets the requirements of Appendix A of this policy*—that an alteration to or waiver, in whole or in part, of the individual authorization required by this policy has been approved by either:

a. An Institutional Review Board ("IRB") that meets the requirements of applicable law, including those stated in 45 C.F.R. § 164.512(i); or

b. A privacy board that:

i. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

ii. Includes at least one member who is not affiliated with [*Organization*], not affiliated with any entity sponsoring the research, and not related to any person who is affiliated with any of such entities; and

iii. Does not have any member participating in a review of any project in which the member has a conflict of interest.

(b) *Reviews Preparatory to Research.* [*Organization*] obtains from the researcher representations that:

a. Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;

b. No PHI is to be removed from [*Organization*] by the researcher in the course of the review; and

c. The PHI for which use or access is sought is necessary for the research purposes.

(c) *Research on Decedent's Information.* [*Organization*] obtains from the researcher:

a. Representation that the use or disclosure sought is solely for research on the PHI of decedents;

b. Documentation, at the request of [*Organization*], of the death of such individuals; and

c. Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

The MHRA generally requires [*Organization*] to obtain signed and dated patient consent prior to releasing health records. However, the MHRA has additional requirements that apply to research disclosures. If the disclosure is to an external researcher solely for purposes of medical or scientific research, [*Organization*] should refer to the MHRA requirements for consent described in Section I.B.5 of this policy even where [*Organization*] qualifies for an exception to HIPAA's authorization requirement. In addition, in making a release of health records to an external researcher, the MHRA indicates that providers are to make a reasonable effort to determine that:

(a) The use or disclosure does not violate any limitations under which the record was collected;
(b) The use or disclosure in individually identifiable form is necessary to accomplish the research or statistical purpose for which the use or disclosure is to be made;
(c) The recipient has established and maintains adequate safeguards to protect the records from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient; and
(d) Further use or release of the records in individually identifiable form to a person other than the patient without the patient's consent is prohibited.

The MHRA does not dictate how these matters are to be ascertained or documented.

In addition, the MHRA does not provide that any form of patient consent is required for [*Organization*] to use health records within *[Organization]* for research. This is different than HIPAA, which requires authorization (or compliance with one of the exceptions to the authorization requirement) even if the activity is solely the internal use of PHI for research purposes and no external "disclosure" will occur.

In addition, if [*Organization*] is subject to 42 C.F.R. Part 2, it may only disclose patient identifying substance use disorder information for the purpose of conducting scientific research if consistent with Section I.B.7 of this policy.

5. **Minnesota law requires consent prior to release of health records to an external researcher**

The MHRA requires providers to obtain consent that meets certain requirements to release health records to an external researcher solely for purposes of medical or scientific research. If [*Organization*] obtains a valid authorization to use or disclose PHI for research as required by Section I.B.1 of this policy, the authorization should be able to satisfy the MHRA requirement regarding consent to release the patient's health records to an external researcher. [*Organization*] will also need to address compliance with the provision in subparagraph (c), noted below, which relates to advising the patient of certain information about the research.

Alternatively, if [*Organization*] does not obtain a HIPAA authorization, but meets one of the exceptions to HIPAA's authorization requirements (stated in Section I.B.4), then [*Organization*] may release health records to an external researcher as long as [*Organization*] obtains consent as follows:

(a) [*Organization*] must disclose in writing to patients currently being treated by the provider that health records, regardless of when generated, may be released and that the patient may object, in which case the records will not be released; and

(b) [*Organization*] must use reasonable efforts to obtain the patient's written general authorization that describes the release of health records for external research; and

(c) [*Organization*] must advise the patient that, at the request of the patient, [*Organization*] will provide information on how the patient may contact an external researcher to whom the health record was released and the date it was released.

The patient's consent described in this Section I.B.5 does not expire but may be revoked or limited in writing at any time by the patient or the patient's authorized representative.

If [*Organization*] meets one of the exceptions to the HIPAA authorization requirement in Section I.B.4 and desires to release health records to an external

researcher as described above, one option for addressing the MHRA requirements is by including a provision in *[Organization's]* standard consent form that meets these requirements. This could include an "opt out" provision under which the patient will consent to the research disclosures unless he or she affirmatively opts out of that disclosure. Alternatively, *[Organization]* could seek separate consent from the patient for the release.

6. **Exceptions to Minnesota consent requirement for external research**

If one of the exceptions stated in Section I.B.4 applies, [Organization] may release PHI for research purposes without the patient's authorization or consent, if:

(a) The health records were generated before January 1, 1997 and the patient has not, at any time, objected to their release; or

(b) [*Organization*] mailed a request for the patient's written general authorization at least two times to the patient's last known address with a postage prepaid return envelope and a conspicuous notice that the patient's medical records may be released if the patient does not object, and at least 60 days have expired since the second notice was sent.

7. **Substance Use Disorder Patient Records**

If [*Organization*] is subject to 42 C.F.R. Part 2, [*Organization*] must comply with this Section I.B.7 and 42 C.F.R. § 2.52. For guidance on Part 2 and what constitutes "patient identifying information," please see Policy Number [*Insert*], "Am I subject to 42 C.F.R. Part 2?" and 42 C.F.R. § 2.11**.**

(a) [*Organization*] may disclose patient identifying information for the purpose of conducting scientific research if the [*Organization*] [director] [chief executive officer] or their designee makes a determination that the recipient of patient information:

i. <u>If a HIPAA-covered entity or business associate</u>: has obtained and documented HIPAA authorization from the patient, or a waiver or alteration of authorization, as applicable.

ii. <u>If subject to the HHS regulations regarding the protection of human subjects (45 CFR part 46)</u>: either provides documentation that the researcher is in compliance with the requirements of the HHS regulations, including the requirements related to informed consent or a waiver of consent (found in 45 CFR 46.111 and 46.116), or that the research qualifies for exemption under the HHS regulations (found in 45 CFR 46.101(b)) and any successor regulations.

iii. If subject to both HIPAA and the HHS regulations regarding the protection of human subjects: has met the requirements for both (a) and (b) above.

iv. If subject to neither HIPAA nor the HHS regulations regarding the protection of human subjects: these rules governing disclosure of Part 2 data for research (42 CFR § 2.52) do not apply.

A person conducting research may disclose individual identifying information obtained under this policy only back to [*Organization*] and may not identify any individual in any report of that research or otherwise disclose an individual's identity.

(b) An individual or entity conducting research using patient identifying information obtained under paragraph (a) of this section:

i. Is fully bound by Part 2 and, if necessary, must resist in judicial proceedings any efforts to obtain access to substance use disorder patient records except as permitted by Part 2.

ii. Must not re-disclose patient identifying information except back to [*Organization*].

iii. May include part 2 data in research reports only in aggregate form in which patient identifying information has been rendered non-identifiable such that the information cannot be re-identified and serve as an unauthorized means to identify a patient, directly or indirectly, as having or having had a substance use disorder.

iv. Must maintain and destroy patient identifying information in accordance with the security policies and procedures established under 42 CFR § 2.16.

v. Must retain records in compliance with applicable federal, state, and local record retention laws.

8. **Other special rules: Data Linkages and Substance Use Disorder Records**

Researchers and Data repositories must comply with the following rules relating to data linkages.

(a) Researchers: Any individual or entity conducting scientific research using patient identifying information obtained under Section I.B.7(a) that requests linkages to data sets from a data repository holding patient identifying information must:

i. Have their request reviewed and approved by an Institutional Review Board registered with Department of Health and Human Services and the Office for Human Research Protections, in accordance with 45 CFR part 46; and

ii. Ensure that patient identifying information is not provided to law enforcement agencies or officials.

A researcher may not redisclose patient identifying information for data linkages purposes except as permitted by Part 2.

(b) Data Repositories: Data repositories are fully bound by Part 2 upon receipt of patient identifying data. Data repositories must:

i. After providing the researcher with the linked data, destroy or delete the linked data from its records, including sanitizing any associated hard copy or electronic media, to render the patient identifying information non-retrievable; and

ii. Ensure that patient identifying information is not provided to law enforcement agencies or officials.

9. **Other special rules: Psychotherapy notes**

Certain types of particularly sensitive PHI may be subject to special rules. For example, except as provided in 45 C.F.R. § 164.508(a)(2), [*Organization*] may not use or disclose psychotherapy notes without the patient's authorization. This means that [*Organization*] would not be permitted to rely on the exceptions to authorization described in Section I.B.4 to use/disclose psychotherapy notes for research. Rather, [*Organization*] would need to obtain the appropriate type of authorization for a use/disclosure of psychotherapy notes for research.

10. **Limited data set and de-identified health information**

(a) If consistent with Minnesota law and this section, [*Organization*] may use or disclose a "limited data set" for research purposes. A "limited data set" is defined in 45 C.F.R. § 164.514(e)(2) as PHI which excludes certain direct identifiers. Disclosures of a limited data set must be pursuant to a data use agreement substantially similar to [*Organization*]'s template data use agreement. *See* policy number [*Insert*], Template Data Use Agreement. [*Organization*] is not required to obtain HIPAA authorization for uses and disclosures of limited data sets that meet the requirements of 45 C.F.R. § 164.514(e).

(b) If consistent with Minnesota law, [*Organization*] may use or disclose information that qualifies as "de-identified" information, as provided in 45 C.F.R. § 164.514(a)-(c). [*Organization*] is not required to obtain HIPAA authorization for uses and disclosures of de-identified information that meets the requirements of 45 C.F.R. § 164.514(a)–(c).

Minnesota Law. A limited data set, although devoid of direct identifiers, is still PHI and arguably would still qualify as "health records" under the MHRA. De-identified information likely does not qualify as "health records" under the MHRA. Minnesota law generally requires [*Organization*] to obtain signed and dated patient consent prior to releasing health records and, as discussed in Section I.B.5, specific requirements exist for disclosures of health records to external researchers. A consent that meets the requirements of Section I.B.5 would be sufficient to establish consent to release a limited data set for research purposes.

11. **Other considerations.**

There are a number of other federal guidelines that may interact with the privacy requirements described in this policy, depending on how [*Organization*] operates. For example, the U.S. Department of Health and Human Services "Common Rule" (*See* 45 C.F.R. Part 46) outlines standards for the protection of human subjects in federally funded research. Likewise, U.S. Food and Drug Administration regulations set forth certain requirements for human research involving FDA-regulated products (*See* 21 C.F.R. Parts 50, 56). These regulations impose their own standards related to research, including the type of patient permission necessary for research and alternatives when patient permission is not available. A discussion of these guidelines is beyond the scope of this policy. However, for helpful tools to use in understanding how HIPAA relates to these other federal laws, please see: https://privacyruleandresearch.nih.gov/default.asp.

II. Procedure:

Prior to using or disclosing PHI for research, [*Organization*] staff should do the following:

A. Determine whether the information is (1) de-identified information; (2) a limited data set; (3) substance use disorder records; (4) psychotherapy notes; or (5) PHI that does not include information in categories (2), (3) or (4). Follow the procedures for each set forth below:

B. Note that depending on the scope of the research and the parties involved, other requirements may apply. For example, if *[Organization]* is using a business associate to create de-identified information or a limited data set for use by a third party researcher, [*Organization*]'s business associate agreement with the business associate will need to address the de-identification/limited data set.

C. De-identified Information:

1. Confirm that information meets the definition of de-identified information at 45 C.F.R. § 164.514(b).

2. Confirm that [*Organization*] meets HIPAA's requirements with respect to re-identification of de-identified information.

D. Limited Data Set:

1. Confirm that information meets the definition of a limited data set as outlined at 45 C.F.R. § 164.514(e)(2).

2. Confirm that [*Organization*] has a data use agreement with the recipient of the limited data set. *See* policy number [*Insert*], Template Data Use Agreement.

3. Confirm that the requirements of MHRA are met with respect to the limited data set.

E. Substance Use Disorder Records:

1. Determine if Part 2 applies to [*Organization*].

2. If Part 2 applies, confirm that the recipient of any patient identifying information meets the requirements of Section I.B.7 of this policy.

F. Psychotherapy Notes:

1. Confirm that a HIPAA compliant authorization exists to permit the use or disclosure of psychotherapy notes. *See* policy number [*Insert*], Use and Disclosure of Mental Health Records.

2. Confirm compliance with HIPAA compound authorization rule pursuant to which an authorization for use or disclosure of psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes. Additional information can be found at 45 C.F.R. § 164.508(b)(3).

G. Other Categories of PHI:

1. Determine whether the activity is a use or disclosure of PHI for research.

2. If the activity is a use of PHI for research, confirm that a HIPAA-compliant authorization exists or that one of the exceptions outlined in Section I.B.4 is satisfied.

3. If the activity is a disclosure of PHI to an external researcher solely for purposes of medical or scientific research, confirm that a HIPAA-compliant authorization exists or that one of the exceptions outlined in Section I.B.4 is satisfied.

4. If the activity is a disclosure of PHI to an external researcher solely for purposes of medical or scientific research and [*Organization*] is relying on one of the exceptions outlined in Section I.B.4, confirm that a valid consent exists under the MHRA (as

described in Section I.B.5) or that one of the exceptions to consent under the MHRA (as outlined in Section I.B.6) is met.

H. [*Organization*]'s Privacy Official or designee will comply with the above stated policy and ensure the compliance of other Workforce members.

I. [*Organization*]'s Privacy Official or designee will document any uses or releases pursuant to this policy in a manner that will allow [*Organization*] to provide an accounting of disclosures to patients (as may be required under applicable law). For example, an accounting of disclosures is not required for research disclosures made pursuant to an authorization or disclosures of a limited data set that occur in accordance with this policy.

J. [*Organization*]'s Privacy Official will confirm that [*Organization*] maintains documentation of IRB or Privacy Board alteration or waiver of authorization as required by this Policy (and described in Appendix A).

Appendix A

Documentation requirements for IRB or Privacy Board's alternation or waiver of authorization requirement

For a use or disclosure to be permitted by section I.B.4(a) of this policy, the documentation must include *all of the following:*

(a) *Identification and Date of Action*. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(b) *Waiver Criteria*. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

a. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

i. An adequate plan to protect the identifiers from improper use and disclosure;

ii. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

iii. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule;

b. The research could not practicably be conducted without the waiver or alteration; and

c. The research could not practicably be conducted without access to and use of the PHI.

(c) *PHI Needed*. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board.

(d) *Review and Approval Procedures*. A statement that the alteration or waiver of authorization has been reviewed and approved under either the normal or expedited review procedures, as follows:

a. An IRB must follow the requirements of the "Common Rule." *See, e.g.*, 45 C.F.R. §§ 46.108(b) & 46.110.

b. A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who is not affiliated with [*Organization*] or any entity sponsoring the research, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting unless the privacy board elects to use the "expedited review procedure" discussed directly below.

c. A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use or disclosure is being sought. If the privacy board elects to use this expedited review procedure, the review and approval of the alteration or waiver of the authorization may be carried out by the chair of the privacy board or one or more designated members of the privacy board.

(e) *Required Signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or privacy board, as applicable.

[Enter Organization Logo]

DISCLOSURES OF SUBSTANCE USE DISORDER PATIENT RECORDS

Policy Number: [Enter]
Effective Date: [Enter]

[GPM Note: In January 2017, the Department of Health and Human Services, Substance Abuse and Mental Health Services Administration ("SAMHSA") issued a final rule amending 42 CFR Part 2. See 82 Fed. Reg. 6115 (Jan. 18, 2017). The final rule became effective on March 21, 2017. This policy has been updated to incorporate these changes.]

I. Policy

A. Purpose

This policy establishes guidelines to be followed by [*Organization*]*'s* workforce when using or disclosing substance use disorder patient records. It sets forth the general rule for disclosures; because other exceptions may apply in unique scenarios, [*Organization*] staff should refer to additional policies when appropriate.

B. Applicability

The rules in this policy originate from 42 C.F.R. Part 2, the federal substance use disorder patient records rule ("Part 2"). Part 2 places restrictions on the use and disclosure of substance use disorder patient records and establishes specific consent standards. It applies to all records that would identify a patient as having a substance use disorder (either directly by reference or through verification), including identity, diagnosis, prognosis, or treatment information.

Part 2 applies to substance use disorder "programs" that are federally assisted. The term "Program" includes the following:

1. An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment;

2. An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or

3. Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

In addition, individuals or entities who receive patient records directly from a Program or other lawful holder of patient identifying information, and who are notified of the prohibition on re-disclosure, are subject to these restrictions on disclosure. **[GPM Note: Insert one of the following options: (1) [*Organization*] is a "program" because it falls within number one above; (2) [*Organization*] is a "program" because it falls within number two above; (3) [*Organization*]'s medical personnel are subject to Part 2 because they fall within number three above; OR (4) *[Organization]* is subject to the restrictions on disclosure because it receives patient records from part 2 programs or other lawful holders of patient identifying information]**. In addition, [*Organization*] is federally assisted pursuant to 42 C.F.R. § 2.12(b), and does not fall within any applicability exceptions. **[GPM Note: To help determine whether [*Organization*] and its workforce are subject to Part 2, use the Flow Chart: Am I Subject to 42 C.F.R. Part 2?]** For these reasons, [*Organization*] is subject to Part 2 and must comply with this policy when disclosing substance use disorder patient records.

It is important to note that not every entity or provider is subject to Part 2. For example, Part 2 does not apply to general medical facilities (although it may apply to an identified unit within a general medical facility). It does not apply to emergency room personnel who refer a patient to the intensive care unit for an apparent overdose (unless the primary function of such personnel is the provision of substance use disorder diagnosis, treatment, or referral and they are identified as providing such services, or the emergency room has promoted itself to the community as a provider of such services). For additional detail on the applicability of Part 2, refer to [*Organization*]'s Flow Chart: Am I Subject to 42 C.F.R. Part 2?

C. Policy Implementation—General Rule

The general rule is that [*Organization*] or its workforce may not say to a person outside of [*Organization*] that an individual receives care at [*Organization*] for substance use disorder, or disclose any information identifying the individual as a substance use disorder patient unless:

1. The patient consents in writing;

2. The disclosure is allowed by a court order; or

3. The disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation.

Part 2 prohibits the disclosure and use of substance use disorder patient records unless certain circumstances exist. If any circumstances exist under which disclosure is permitted, that circumstance acts to remove the prohibition on

disclosure, but it does not compel disclosure. Thus, *Part 2 does not require disclosure under any circumstances*.

D. Disclosures made pursuant to written consent

[*Organization*] may disclose substance use disorder patient records pursuant to written consent of the individual. A written consent to a disclosure must include:

1. The name of the patient;

2. The specific name(s) or general designation(s) of the Part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure;

3. How much and what kind of information is to be disclosed, including an explicit description of the substance use disorder information that may be disclosed;

4. One or more of the following:

    a. The names of the individuals to who a disclosure it to be made;

    b. If the recipient of the information has a treating provider relationship with the patient who information is being disclosed, such as a hospital or health care clinic, or a private practice: the name of that entity;

    c. If the recipient entity does not have a treating provider relationship with the patient whose information is being disclosed and is a third-party payer, the name of the entity;

    d. If the recipient entity does not have a treating or provider relationship with the patient whose information is being disclosed and is not covered by subsection 4(c) above (i.e., is not a third-party payer), such as an entity that facilitates the exchange of health information or a research institution, must include the name of the entity(ies) and either: (1) the name(s) of the individual participants; (2) the name(s) of an entity participants(s) that has a treating provider relationship with the patient whose information is being disclosed; or (3) a general designation of an individual or entity participant(s) or class of participants that must be limited to a participant(s) who has a treating provider relationship with the patient whose information is being disclosed.

        i. When using a general designation, a statement must be included on the consent form that the patient (or other individual authorized to sign in lieu of the patient), confirms their understanding that, upon their request and consistent with this part, they must be provided a list of entities to which their information has been disclosed pursuant to the general designation.

5. The purpose of the disclosure. Note that the disclosure must be limited to that information which is necessary to carry out the stated purpose.

6. A statement that the consent is subject to revocation at any time except to the extent that the part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer.

7. The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is provided.

8. The signature of the patient and, when required for a patient who is a minor, the signature of an individual authorized to give consent under 42 CFR § 2.14; or, when required for a patient who is incompetent or deceased, the signature of an individual authorized to sign under 42 CFR § 2.15. Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.

9. The date on which the consent is signed.

Each disclosure made pursuant to written consent must be accompanied by the following written statement:

> This information has been disclosed to you from records protected by federal confidentiality rules (*42 CFR part 2*). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is *NOT* sufficient for this purpose (see §2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§2.12(c)(5) and 2.65.

E. Disclosures that may be made without written patient consent

[*Organization*] may make disclosures without written consent according to the following circumstances:

1. Medical emergencies

[*Organization*] may disclose information to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent

cannot be obtained. The treating provider is responsible for determining whether a bona fide medical emergency exists. Immediately following disclosure, [*Organization*] must document the following in the individual's records:

a. The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;

b. The name of the individual making the disclosure;

c. The date and time of the disclosure; and

d. The nature of the emergency.

2. Research activities

[*Organization*] may disclose patient identifying information for the purpose of conducting scientific research if the [*Organization*] [director] [chief executive officer] or their designee makes a determination that the recipient of patient information:

a. If a HIPAA-covered entity or business associate: has obtained and documented HIPAA authorization from the patient, or a waiver or alteration of authorization, as applicable.

b. If subject to the HHS regulations regarding the protection of human subjects (45 CFR part 46): either provides documentation that the researcher is in compliance with the requirements of the HHS regulations, including the requirements related to informed consent or a waiver of consent (found in 45 CFR 46.111 and 46.116), or that the research qualifies for exemption under the HHS regulations (found in 45 CFR 46.101(b)) and any successor regulations.

c. If subject to both HIPAA and the HHS regulations regarding the protection of human subjects: has met the requirements for both (a) and (b) above.

d. If subject to neither HIPAA nor the HHS regulations regarding the protection of human subjects: these rules governing disclosure of Part 2 data for research (42 CFR § 2.52) do not apply.

A person conducting research may disclose individual identifying information obtained under this policy only back to [*Organization*] and may not identify any individual in any report of that research or otherwise disclose an individual's identity.

Minnesota law sets forth specific rules for the disclosure of health records for external research. In regards to records generated on or after January 1, 1997, [*Organization*] must:

1. Disclose in writing to patients currently being treated by [*Organization*] that health records, regardless of when they were generated, may be released

and that the patient may object, in which case [*Organization*] will not release the records;

2. Use reasonable efforts to obtain the patient's written general authorization that describes the release of records; and

3. Advise the patient of his/her right to receive information on how the patient may contact the external researcher and the date information was released, and provide such information when requested.

Because Minnesota law is more restrictive than Part 2 in this regard, [*Organization*] must comply with this rule when disclosing information to an external researcher. Minnesota law does not set forth specific requirements for disclosures to internal researchers; thus, [*Organization*] must follow the general rule and obtain patient consent prior to such disclosures.

For more information, [*Organization*] staff should refer to policy number [Enter], Using and Disclosing Information for Research Purposes.

3. Audit and evaluation activities

[*Organization*] may disclose substance use disorder patient records, without patient consent, for audit and evaluation activities as follows: If records are not downloaded, copied or removed from [*Organization*]'s premises or forwarded electronically to another electronic system or device, individual identifying information may be disclosed in the course of a review of records on [*Organization*]'s premises to any individual or entity who agrees in writing to comply with the limitations on re-disclosure and use and who:

a. Performs the audit or evaluation activity on behalf of any federal, state, or local government agency which provides financial assistance to [*Organization*] or is authorized by law to regulate its activities, or to any individual or entity who provides financial assistance to [*Organization*], which is a third party payer covering patients at [*Organization*], or which is a quality improvement organization performing a utilization or quality control review; or

b. Is determined by [*Organization*] to be qualified to conduct an audit or evaluation of [*Organization*].

Records may be copied or removed from [*Organization*]'s premises or downloaded or forwarded to another electronic system or device from [*Organization*]'s electronic records by any individual or entity who:

c. Agrees in writing to maintain and destroy the information in a manner consistent with the policies and procedures established under 42 CFR 2.16;

retain records in compliance will applicable federal, state, and local record retention laws; and comply with the limitations on disclosure and use; and

d. Performs the audit or evaluation on behalf of any federal, state, or local government agency or individual or entity that meets the requirements of (a) above.

[*Organization*] may also disclose patient identifying information to any individual or entity for the purpose of conducting a Medicare, Medicaid, or Children's Health Insurance Program (CHIP) audit or evaluation, including an audit or evaluation necessary to meet the requirements for a CMS-regulated ACO or similar CMS-regulated organization, provided that the individual or entity agrees in writing to the requirements set forth at 42 CFR 2.53(c). The audit or evaluation must be conducted in accordance we the requirements set forth at 42 CFR 2.53(c). These requirements contain significant detail related to the parameters of permitted audit/evaluation activities. A Medicare, Medicaid, or CHIP audit or evaluation includes a civil or administrative investigation of [*Organization*] by any federal, state, or local government agency with oversight responsibilities for Medicare, Medicaid, or CHIP and includes administrative enforcement, against [*Organization*] by the government agency, of any remedy authorized by law to be imposed as a result of the findings of the investigation.

Except as permitted by Part 2, identifying information disclosed pursuant an audit/review may be disclosed only back to [*Organization*] and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by a court order.

F. Disclosures and uses which may be made with an authorizing court order

[*Organization*] may disclose identifying information pursuant to a court order. Workforce should refer to [*Organization*]'s policy on Disclosures for Judicial and Administrative Proceedings (policy number [Enter]).

G. Other exceptions

There are a number of other exceptions to the general rules set forth in this policy. For example, [*Organization*] may disclose information without patient consent to a qualified service organization, provided certain requirements are met. Staff should review policy number [Enter], Disclosing Information to Business Associates, for more detail.

In addition, Part 2 permits [*Organization*] to exchange substance use disorder patient records without patient consent to [*Organization*] personnel who have a need for the information in connection with their duties, and to an entity with direct administrative control over [*Organization*]. Part 2 also permits [*Organization*] to communicate with law enforcement officials or agencies about crimes that occur on [*Organization*]'s premises or against [*Organization*] personnel, or to report incidents of suspected child

abuse or neglect. These exceptions are narrow, and [*Organization*] staff should consult with the [*compliance officer/privacy officer/other designee*] prior to any disclosure. Minnesota law may require patient consent for some, but not all, of these exceptions.

Because this policy applies to those situations in which other exceptions do not apply, staff should refer to other applicable policies, and/or consult with [*Organization*]'s [*compliance officer/privacy officer/other designee*] to determine whether a disclosure of substance use disorder patient records is permitted without patient consent.

H. Minimum necessary

Any disclosure made under Part 2 must be limited to that information which is necessary to carry out the purpose of the disclosure.

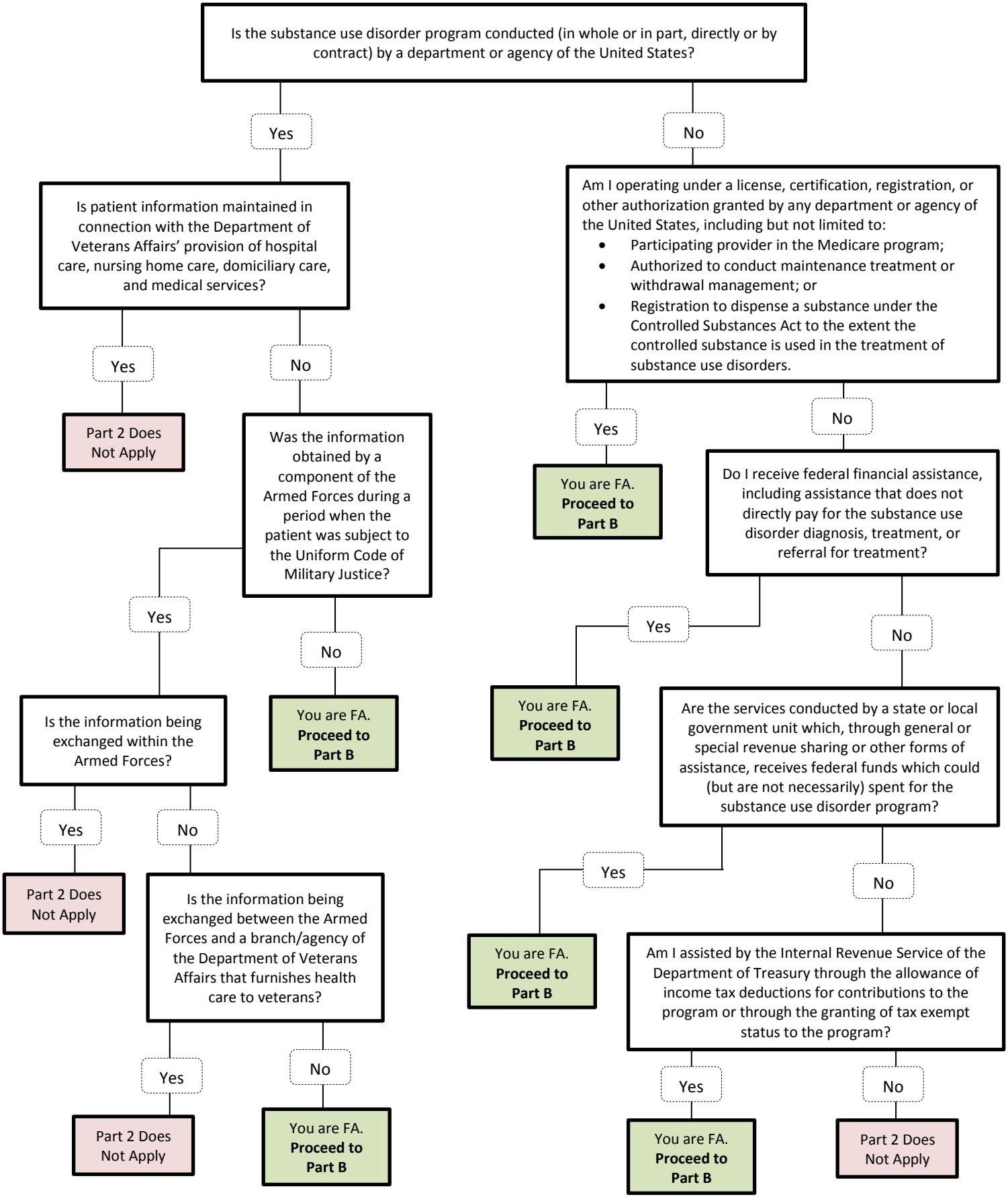
II. Procedure

[*Organization*] and its workforce will adhere to this policy when disclosing substance use disorder patient records, and will adhere to other relevant policies referencing Part 2 requirements, when applicable.

Confidentiality of Substance Use Disorder Patient Records

Am I Subject to 42 CFR Part 2?

Part A: Am I federally assisted ("FA")?



Confidentiality of Substance Use Disorder Patient Records

Am I Subject to 42 CFR Part 2?

Part B: Am I a "Program"?

1. Do I provide substance use disorder diagnosis, treatment, or referral for treatment?
   - No → Not Subject to Part 2
   - Yes → 2. Am I, or do I work in, a general medical facility?
     - No → 3. Do I hold myself out as providing substance use disorder diagnosis, treatment, or referral for treatment?
       - No → Not Subject to Part 2
       - Yes → I am a "Program" and therefore subject to Part 2; Proceed to the "Exceptions" Chart
     - Yes → 4. Am I an identified unit within the general medical facility?
       - Yes → Go to #3
       - No → 5. Am I medical personnel or other staff whose primary function is the provision of substance use disorder diagnosis, treatment or referral for treatment?
         - No → Not Subject to Part 2
         - Yes → 6. Am I identified as a provider whose primary function is the provision of substance use disorder diagnosis, treatment or referral for treatment?
           - No → Not Subject to Part 2
           - Yes → I am a "Program" and therefore subject to Part 2; Proceed to the "Exceptions" Chart

Exceptions

Does one of the following scenarios apply? If so, while Part 2 is still applicable the identified uses/disclosures are not subject to Part 2

Disclosure within Program
Information is being exchanged between personnel within the program, and such personnel have a need for the information in connection with their job duties.

Or

Disclosure to Parent Entity
Information is being exchanged between personnel at the program and personnel at an entity that has direct administrative control over the program, and such personnel have a need for the information in connection with their job duties.

Or

Disclosure to Qualified Service Organizations
Information is being exchanged between the program and a Qualified Service Organization, and the Qualified Service Organization needs such information to provide services to the program.

Or

Crime-related Uses/Disclosures
Information communicated between program personnel and law enforcement agencies/officials, and such information: (a) relates to a patient's commission of a crime against program personnel, on program premises, or to a threat to commit such crime; and (b) is limited to the circumstances of the incident

Or

Child Abuse Disclosures/Uses
Information is being disclosed to report suspected child abuse and neglect as permitted under state law

- Yes → **Identified Activities Not Subject to Part 2**
- No → **Subject to Part 2**