

**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
<b><i>Policy: Disclosing Information to Business Associates</i></b>		
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.”
<b><i>Policy: Using and Disclosing Information in an Emergency</i></b>		
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
		<i>information in connection with an emergency if the disclosure is necessary to protect the health or safety of the patient or other persons.”</i>
Section I.B Policy Implementation—General Rule	Minn. Stat. § 13.384, subd. 3	Add new Section C (and adjust numbering): <b>“Medical Data.</b> <i>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.”</i>
<b><i>Policy: Using and Disclosing Information for Health Care Operations</i></b>		
Section I.B Policy Implementation—General Rule (“Minnesota Law” box)	Minn. Stat. § 13.05	Add at the beginning of paragraph: <i>“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, . . . .”</i> [Existing policy language should follow (“Minnesota law generally requires...”)].
<b><i>Policy: Disclosures of Alcohol and Drug Abuse Records</i></b>		
Section I. Policy	Minn. Stat. § 13.383, subd. 11a(c)	Add new Section I: <b>“Alcohol and drug counselors subject to the Data Practices Act.</b> <i>[Organization] and its workforce</i>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<i>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.”</i>
Section I.E.1 Medical Emergencies	Minn. Stat. § 13.46	In gray “Minnesota Law” box, add following as a new paragraph: <i>“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.”</i>
<b><i>Policy: Consent to Disclose Health Information Under Minnesota Law</i></b>		
Section I.A Purpose	N/A	Replace with the following: <i>“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.”</i>
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: <i>“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.”</i>  Add new Section D (and adjust numbering): <b><i>“Tennessee</i></b>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<p><b>Warning.</b> <i>[Organization] must provide individuals with a “Tennessee 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 Tennessee warning.</i></p> <p><i>The Tennessee warning must address the following:</i></p> <ol style="list-style-type: none"> <li><i>1. The purpose and intended use of the requested data within the collecting government entity;</i></li> <li><i>2. Whether the individual may refuse or is legally required to supply the requested data;</i></li> <li><i>3. Any known consequence arising from supplying or refusing to supply private or confidential data; and</i></li> <li><i>4. The identity of other persons or entities authorized by state or federal law to receive the data.”</i></li> </ol>
Section I.E Specific Authorization in Law	Minn. Stat. § 13.05	<p>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,</p>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<p><i>education, or welfare of a child affected by the data, in accordance with Minn. Stat. 626.556, subd. 10j.”</i></p> <p><b>GPM Note: DPA Providers should include a provision in their Tennessee Warning that states patient information may be disclosed as required by law.</b></p>
Section I.F Permitted Disclosures without a Consent	Minn. Stat. § 13.384 Minn. Stat. § 13.3805 Minn. Stat. § 13.46	<p>Add permissible disclosures of Medical Data under Minn. Stat. § 13.384.</p> <p>Add permissible disclosures of Health Data under Minn. Stat. § 13.3805.</p> <p>If subject to § 13.46, add permissible disclosures of data on individuals by the welfare system under Minn. Stat. § 13.46.</p>
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. <i>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.</i> ”
<b>Policy: Authorization for Use and Disclosure of PHI</b>		
Section I.A (“Minnesota Law” box)	Minn. Stat. § 13.04, subd. 2 Minn. Stat. § 13.05 Minn. R. 1205.1400	<p>Following the first paragraph, add: “<i>To constitute valid consent under the Minnesota Data Practices Act, the consent must:</i></p> <p><i>(1) be voluntary and not coerced;</i></p> <p><i>(2) be in writing; (3)</i></p> <p><i>[Organization] must explain why</i></p>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<p><i>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.”</i></p> <p>Following the second paragraph, add: “[Organization] must provide patients with a “Tennessee 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 Tennessee warning. The HIPAA authorization obligations set forth in this policy are in addition to [Organization]’s obligation to provide a Tennessee warning.</p> <p><i>The Tennessee warning must address the following:</i></p> <ol style="list-style-type: none"> <li><i>1. The purpose and intended use of the requested data within the collecting government entity;</i></li> <li><i>2. Whether the individual may refuse or is legally required to supply the requested data;</i></li> </ol>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<p>3. Any known consequence arising from supplying or refusing to supply private or confidential data; and</p> <p>4. The identity of other persons or entities authorized by state or federal law to receive the data.”</p>
<b><i>Policy: Breach of Unsecured PHI</i></b>		
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	<p>Delete: “This policy is designed to explain the obligations of non-governmental health care providers.”</p> <p>Add to Section II.B.2: “<i>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).</i>”</p> <p>Add to Section II.B.3: “<i>Such good faith acquisition is also not a breach of the security of the data within the meaning of the Data Practices Act.</i>”</p> <p>Add to Section II.B.5: “<i>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.</i>”</p>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		Add to Section II.B.6: <i>“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.”</i>
<b><i>Policy: Minimum Necessary for Requests for, or Uses or Disclosures of, PHI</i></b>		
Section I.B Policy Implementation—General Rule	Minn. Stat. § 13.05	Add: <i>“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.”</i>
Section I.B.1 Situations where the minimum necessary rule does not apply	Minn. Stat. § 13.05	Add to introductory paragraph: <i>“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, . . . .”</i> [Existing policy language should follow (“[Organization] and its workforce are not required to comply. . . .”)].



Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
<b><i>Policy: Disclosures for Judicial and Administrative Proceedings</i></b>		
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	<p>Replace the first sentence with the following: “[<i>Organization</i>] 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 &amp; 13.46, subd. 2.”</p> <p>Add following the second paragraph: “<i>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.</i>”</p>
<b><i>Policy: Use and Disclosure of Mental Health Records</i></b>		
Section 1.B Policy Implementation—General Rule (Gray Box)	Minn. Stat. § 13.46, subd. 7	Add: “ <i>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</i>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<i>under the Minnesota Health Records Act and applicable HIPAA requirements.”</i>
<b><i>Policy: Use and Disclosure of PHI for Research Purposes</i></b>		
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: <i>“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.”</i>
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: <i>“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”.</i>
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: <i>“Unless otherwise classified by Minnesota Statutes Section 13.06 or another statute, “summary data” as defined in Minnesota Statutes Section 13.02,</i>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<p><i>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:</i></p> <p style="padding-left: 40px;"><i>A. A general description of the private or confidential data which is being used to prepare summary data;</i></p> <p style="padding-left: 40px;"><i>B. The purpose for which the summary data is being prepared; and</i></p> <p style="padding-left: 40px;"><i>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.</i></p> <p><i>These terms may be included in a business associate agreement if the party subject to the DPA discloses PHI/private or</i></p>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<i>confidential data to a business associate to create de-identified information/summary data.</i>
Section I.B.7—Alcohol and Drug Abuse Records	Minn. Stat. § 254A.09 Min. Stat. § 13.461	Add: <i>“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.”</i>
<b><i>Policy: Use and Disclosure of PHI for Fundraising</i></b>		
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: <i>“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</i>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<i>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”.</i>
<b><i>Policy: Use and Disclosure of PHI for Marketing</i></b>		
Section I.B (Gray Box)	Minn. Stat. § 13.04	Add: <i>“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).”</i>
<b><i>Template Agreement: Business Associate Agreement</i></b>		
Section I	Minn. Stat. § 13.05, subd. 11	Add at the end of Section I: <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.”</i>
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
		<p>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.</p> <p>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.</p> <p>An unauthorized disclosure may constitute a “breach of the security of the data” but not rise to the level of a breach under HIPAA.</p>
Section II.a	Minn. Stat. § 13.05, subd. 11	Add: <i>“Business Associate will not use or disclose PHI in a manner that would violate the Data Practices Act.”</i>
<b>Template Agreement: Subcontractor Business Associate Agreement</b>		
Section I	Minn. Stat. § 13.05, subd. 11	Add at the end of Section I: <i>“Prime Subcontractor acknowledges that it is subject to the Data Practices Act and agrees to comply with applicable</i>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<i>Data Practices Act requirements as if it were a government entity.</i>
Section I (definition of “Breach”)	Minn. Stat. § 13.055	<p>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.”</p> <p>“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.</p> <p>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</p>

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: “ <i>Prime Subcontractor will not use or disclose PHI in a manner that would violate the Data Practices Act.</i> ”
<b>Checklist: Business Associate Agreement Checklist—Required and Optional Terms</b>		
Require Terms	Minn. Stat. § 13.05, subd. 11	Add: “ <b><i>Data Practices Act:</i></b> <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</i> ”
<b>Policy: Definitions</b>		
N/A		Add the following Definitions: <ul style="list-style-type: none"> <li>• <b><u>Breach of the Security of the Data:</u></b> <i>means unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data.</i></li> <li>• <b><u>Data on Individuals:</u></b> <i>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.</i></li> <li>• <b><u>Medical data:</u></b> <i>Data collected because an individual was or</i></li> </ul>



Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<p><i>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.</i></p> <ul style="list-style-type: none"> <li>• <b><u>Mental Health Data:</u></b> <i>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.</i></li> <li>• <b><u>Private data on individuals:</u></b> <i>Data made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the individual subject of those data.</i></li> <li>• <b><u>[Public] Health Data:</u></b> <i>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.</i></li> </ul>

Toolkit Reference	Applicable Minnesota Data Practices Act Section	Toolkit Revision
		<ul style="list-style-type: none"> <li>• <b><u>Summary data.</u></b> <i>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.</i></li> <li>• <b><u>Welfare system:</u></b> <i>“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.</i></li> </ul>