Health Law Alert: Top 10 Takeaways from Alessandra Swanson & MSBA HIPAA Discussion

March 17, 2015

Top 10 Takeaways from Alessandra Swanson & MSBA HIPAA Discussion

by Jennifer Reedstrom Bishop, Tim Johnson, and Julia Marotte

On Feb. 13, the Health Law Section of the Minnesota State Bar Association (MSBA) sponsored an event on HIPAA enforcement in 2015. The MSBA hosted Alessandra Swanson of the Office for Civil Rights, U.S. Department of Health & Human Services (OCR). Swanson provided an inside perspective on OCR enforcement, discussed trends and key developments, and answered questions from attendees.

In case you were unable to attend, here are the ***top 10 takeaways*** from the event:

1. Covered Entities should know where protected health information (PHI) is held and stored.
    - Keeping tabs on PHI is essential to remaining HIPAA compliant. Covered entities should know where PHI is being stored, including the various electronic devices that are used throughout the organization that may host PHI and the daily work habits of employees. For example, do employees take PHI home with them via their cell phone or tablet? Do they take paper files out of the office? Knowing the location of *all* PHI is critical.
2. Covered Entities should foster a culture of compliance.
    - Swanson noted that when investigating a breach, OCR looks for a "culture of compliance." While there are many ways to achieve this, Swanson emphasized that an organization's policies and procedures should be living, breathing documents. In addition, employees should feel comfortable expressing concerns, reporting breaches, and asking questions.
3. There are no safe havens for stolen laptops.
    - Laptop thefts are an all-too-common breach scenario. Although organizations are often the victim of a crime, Swanson clarified there is no safe haven for these situations. OCR looks at the holistic picture surrounding the breach and considers the organization's media/mobile device policy, the risk analysis in place, and the specific circumstances surrounding the theft.
4. Covered entities should *always* report a breach.

- Covered entities often worry that reporting multiple breaches will draw attention to their organization and cast the organization in bad light. However, Swanson noted OCR has a good sense as to how many breaches occur within entities of various sizes. OCR knows what is reasonable and takes this into account—in fact, it is a far bigger problem to under-report.

5. OCR does not always respond to a self-reported breach.
   - OCR is obligated to respond to any breach affecting more than 500 people. When it comes to smaller breaches, OCR is primarily looking for trends. If an organization does not hear from OCR after self-reporting a breach affecting less than 300 people, this is not uncommon. However, OCR takes notice of every breach that is reported.
6. Covered entities are under a continuing obligation to conduct risk analyses.
   - Best practices dictate that organizations conduct a risk analysis every three years. However, when an organization undergoes a system change, such as converting to a cloud-based system, the organization should conduct a risk analysis as soon as reasonably possible.
7. Covered entities must address the risks identified in the risk analysis.
   - It is not enough to simply identify risks and vulnerabilities to PHI held by the covered entity—the covered entity must address those risks. Swanson noted that covered entities often tell her they knew of the risk and intended to address it, but had not gotten to it yet. This is not permissible, and can be an aggravating factor in OCR enforcement.
8. Respond to bad actors in a deliberate and proactive fashion.
   - When a breach results from a bad actor, firing the bad actor is not enough. Organizations should have a sanction policy in place and should follow that policy. In addition, the organization should perform measures to ensure the act is not repeated by others in a similar position. This could include retraining the workforce, discussing the breach, conducting random audits, or limiting access to PHI.
9. Addressable implementation specifications are not optional.
   - Swanson stressed that "addressable" does not mean the specification is optional. If an organization does not adopt the specification or one of its alternatives, the organization must document what it is doing instead to achieve the standard.
10. Call OCR with questions.
    - OCR rarely issues written opinions, and hesitates to put informal thoughts in writing. However, OCR frequently answers questions over the phone. Swanson encouraged attendees to call OCR with questions, and emphasized that it is okay to pose questions as a hypothetical.

If you have questions regarding HIPAA compliance, please contact Jennifer Reedstrom Bishop at jennifer.bishop@lathropgpm.com (612.632.3060), Tim Johnson at timothy.johnson@lathropgpm.com (612.632.3208), or Julia Marotte at julia.marotte@lathropgpm.com (612.632.3280).