Published on *The National Law Review* https://natlawreview.com

OCR Identifies Continuing HIPAA Enforcement Issues, Areas of Future Guidance and Regulations

Article By:

Health Law Practice

Health Care Compliance Association hosted its annual "Compliance Institute." Iliana Peters, HHS Office for Civil Rights' Senior Advisor for *HIPAA* Compliance and Enforcement, provided a thorough update of HIPAA enforcement trends as well as a road map to OCR's current and future endeavors.

Continuing Enforcement Issues

Ms. Peters identified key ten enforcement issues that OCR continues to encounter through its enforcement of HIPAA. These issues include:

1. Impermissible Disclosures. HIPAA's Privacy Rule prohibits covered entities and business associates from disclosing PHI except as permitted or required under HIPAA. Impermissible disclosures identified by Ms. Peters all center on the need for authorization, and include:
    - Covered entities permitting news media to film individuals in their facilities prior to obtaining a patient's authorization.
    - Covered entities publishing PHI on their website or on social media without an individual's authorization.
    - Covered entities confirming that an individual is a patient and providing other PHI to reporters without an individual's authorization.
    - Covered entities faxing PHI to an individual's employer without the individual's authorization.
2. Lack of Business Associate Agreements. OCR continues to see covered entities failing to enter into business associate agreements.
3. Incomplete or Inaccurate Risk Analysis. Under HIPAA's Security Rule, covered entities are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI (ePHI).

According to Ms. Peters, organizations frequently underestimate the proliferation of ePHI throughout their environment, including into systems related to billing, faxing, backups, and medical devices, among others.

4. Failure to manage identified risks. HIPAA requires regulated entities to put in place security measures to reduce risks and vulnerabilities. According to the presentation, several OCR breach investigations found that the causes of reported breaches were risks that had previously been identified in a risk analysis but were never mitigated. In some instances, encryption was included as part of the remediation plan, but was never implemented.

5. Lack of transmission security. While not required in all cases, HIPAA does require that ePHI be encrypted whenever it is deemed appropriate. The presentation identified a number of applications in which encryption should be considered when transmitting ePHI, including email, texting, application sessions, file transmissions (e.g., FTP), remote backups, and remote access and support services (e.g., VPNs).

6. Lack of Appropriate Auditing. HIPAA requires the implementation of mechanisms (whether hardware, software or procedural) that record and examine activity in systems containing ePHI. HIPAA-regulated entities are required to review audit records to determine if there should be additional investigation. The presentation highlighted certain activities that could warrant such additional investigation, including: access to PHI during non-business hours or during time off, access to an abnormally high number of records containing PHI, access to PHI of persons for which media interest exists, and access to PHI of employees.

7. Patching of Software. The use of unpatched or unsupported software on systems which contain ePHI could introduce additional risk into an environment. Ms. Peters also pointed to other systems that should be monitored, including router and firewall firmware, anti-virus and anti-malware software, and multimedia and runtime environments (e.g., Adobe Flash, Java, etc.).

8. Insider Threats. The presentation identifies insider threats as a continuing enforcement issue. Under HIPAA, organizations must implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI and to prevent those workforce members who do not have access from obtaining such access. Termination procedures should be put in place to ensure that access to PHI is revoked when a workforce member leaves.

9. Disposal of PHI. HIPAA requires organizations to implement policies and procedures that ensure proper disposal of PHI. These procedures must guarantee that the media has been cleared, purged or destroyed consistent with NIST Special Publication 800-88: Guidelines for Media Sanitization.

10. Insufficient Backup and Contingency Planning. Organizations are required to ensure that adequate contingency planning (including data backup and disaster recovery plans) is in place and would be effective when implemented in the event of an actual disaster or emergency situation. Organizations are required to periodically test their plans and revise as necessary.

Upcoming Guidance and FAQs

OCR also identified upcoming guidance and FAQs that it will use to address the following areas:

- Privacy and security issues related to the Precision Medicine Initiative's *All of Us* research program
- Text messaging
- Social media
- Use of Certified EHR Technology (CEHRT) & compliance with HIPAA Security Rule (to be release with the Office of the National Coordinator for Health Information Technology (ONC))
- The Resolution Agreement and Civil Monetary Penalty process
- Updates of existing FAQs to account for the Omnibus Rule and other recent developments
- The "minimum necessary" requirement

Long-term Regulatory Agenda

The presentation also identifies two long-term regulatory goals to implement certain provisions of the HITECH Act. One regulation will relate to providing individuals harmed by HIPAA violations with a percentage of any civil monetary penalties or settlements collected by OCR, while the second will implement a HITECH Act provision related to the accounting of disclosures of PHI.

Audit Program Status

The presentation discussed the current status of OCR's audit program. OCR is in the process of conducting desk audits of covered entities and business associates. These audits consist of a review of required HIPAA documentation that is submitted to OCR. According to Ms. Peters, OCR has conducted desk audits of 166 covered entities and 43 business associates. Ms. Peters also used the presentation to confirm that on-site audits of both covered entities and business associates will be conducted in 2017 after the desk audits are completed. We will continue to follow and report on developments in the audit program.

Commentary

The list of continuing enforcement issues provides covered entities and business associates with a helpful reminder of the compliance areas that are most likely to get them in compliance trouble. Some of the enforcement issues may require HIPAA-regulated entities to revisit decisions that they previously made as part of a risk analysis. Transmission security (#5, above) is an example of such an area that may warrant reexamination. In the past, encrypting data was often too expensive or too impracticable for many organizations. However the costs of encryption have decreased while it has become easier to implement. A covered entity or business associate that suffers a breach due to transmitting unencrypted PHI over the internet will likely garner little sympathy from OCR going forward. The presentation is also notable for the long list of guidance and FAQs that OCR will be publishing, as well as their plan to issue regulations to address changes ushered in by the HITECH Act that were not captured by the 2013 Omnibus Rule. These regulations, particularly the regulations

related to accounting for disclosures of PHI, could have a far-reaching impact on how covered entities and business associates comply with HIPAA in the future.

National Law Review, Volume VII, Number 94