Compliance and Enforcement Related to Privacy, Security, and Breach Notification Rules

OCR Will Continue to Identify and Investigate “High-Impact” Cases that Send a Strong Enforcement Message

Lori J. Strauss

In the last issue of the Journal of Health Care Compliance, I addressed the Report to Congress on Breaches of Unsecured Protected Health Information, including the types and numbers of breaches reported in calendar years 2011 and 2012 as well as the actions that covered entities (CEs) and business associates (BAs) took in response to the reported breaches. This article will focus on the other required report issued to Congress in June 2014 — compliance and enforcement activities regarding the Health Insurance Portability and Accountability Act (HIPAA) privacy, security, and breach notification rules. BAs were not required to comply with the provisions of the HIPAA privacy and security rules until September 23, 2013, and as this report addresses enforcement activities for calendar years 2011 and 2012, enforcement actions with BAs are not included.

The Health Information Technology for Economic and Clinical Health (HITECH) Act identifies requirements that the Department is to provide in the annual report related to the complaints that the Office for Civil Rights (OCR) received in the calendar years as well as for the compliance reviews that were started during those years. These requirements include the:

- number of complaints;
- number of complaints that were informally resolved with a summary of such complaints and the number of CEs that the Secretary provided technical assistance to for compliance and the type of assistance provided;
- number of complaints resulting in civil monetary penalties (CMPs) or that were resolved through monetary settlements, including the type of the complaint and the amount paid in each penalty or settlement;
number of compliance reviews done and their outcomes;
- number of subpoenas or inquiries issued;
- number of audits performed with a summary of the findings; and
- the Secretary’s plan to improve compliance with and enforcement of identified findings for the following year.

OCR enforces the HIPAA rules by investigating written complaints filed with OCR, and OCR conducts compliance reviews for situations brought to the OCR’s attention by other means, such as through a breach report, to determine if the CE or BA is in compliance with the rules. OCR compliance activities include auditing CEs and providing education and outreach to assist the CE or BA to comply with the rules. OCR can only take action on complaints that meet the following criteria:

- The alleged violation took place after compliance with the rules was required.
- The complaint must be filed against a CE that is required by law to comply with the rules.
- The complaint must describe an activity that would violate the HIPAA rules.
- With few exceptions, the complaint must be filed within 180 days of when the person submitting the complaint knew or should have known about the situation that is the subject of the complaint.

To investigate a complaint or to begin a compliance review, OCR will gather evidence as all compliance and privacy professionals do when conducting investigations. OCR reports that the majority of complaints are resolved within one year after OCR receives them. Possible actions that can result from OCR initiating an investigation from a complaint or from OCR initiating a compliance review brought to the OCR by another means include:

- Refer criminal issues to the Department of Justice for investigation.
- Close the case based on the evidence finding the CE or BA did not violate the requirement of the HIPAA rules.
- For findings of noncompliance, OCR usually will attempt to resolve the case informally with the CE or BA through voluntary compliance with corrective actions that may include a resolution agreement. For egregious circumstances, OCR can proceed directly to CMPs.
- OCR must obtain documentation and other evidence to show that the CE or BA undertook the required corrective actions to resolve the allegations, and in most situations through voluntary cooperation and corrective actions, CEs or BAs are able to demonstrate compliance with the HIPAA rules.
- For findings of noncompliance involving willful neglect or if the nature and scope of the noncompliance warrants other enforcement actions, OCR pursues a resolution agreement with a payment of a settlement amount and an obligation to complete a corrective action plan. Often, OCR sends a letter to the CE or BA with their findings and OCR’s preparedness to assess CMPs. OCR will continue to communicate its willingness to negotiate the terms of the resolution agreement and the corrective action plan to resolve the noncompliance with the rules. These settlement agreements usually involve payment of some amount that is a fraction of the possible CMPs that the CE or BA is liable for in the case. Additionally, resolution agreements often include a corrective action plan that requires the CE or BA to fix any remaining compliance issues and typically requires the CE or BA to undergo monitoring of its compliance with the HIPAA rules for a period of time. This type of resolution is still considered informal action by OCR.
- The last type of enforcement action by OCR results if OCR and a CE or BA cannot reach satisfactory agreement to resolve the matter informally or if a CE or BA breaches the terms of a resolution agreement. OCR in these circumstances may pursue formal enforcement for violation of the HIPAA rules and impose
CMPs. The CE or BA can request a hearing with the Department's administrative law judge if the CE or BA does not agree that the penalties match the evidence in the case.

COMPLAINTS AND COMPLIANCE REVIEWS 2011 AND 2012
Complaints: OCR received 19,476 new complaints during calendar years 2011 and 2012, not counting the 5,324 complaints in 2011 and the 5,983 complaints in 2012 that carried over from previous years. Over both years:
- 17,771 complaints were resolved;
- OCR did not have jurisdiction in 9,534 cases due to the complaint not meeting a requirement to file a complaint as listed above;
- 8,237 complaints were investigated with no violation found in 2,281 investigations; and
- 5,956 investigations resulted in a corrective action plan and/or technical assistance being provided.

RESOLUTION AGREEMENTS
OCR enacted seven resolution agreements during calendar years 2011 and 2012 ranging in resolution amounts from $50,000 to $1.7 million. The incidents resulting in these agreements involved:
- General Hospital Corporation & Massachusetts General Physicians Organization, Incorporated (Mass General) — loss of 192 patients' protected health information (PHI) from an infectious disease outpatient practice including patients with HIV/AIDS when an employee left documents on a subway that were never recovered. OCR found Mass General failed to implement reasonable and appropriate safeguards to protect the privacy of protected health information (PHI) when the information was removed from its premises and lost. Mass General was to implement a detailed corrective action plan, engage an internal monitor, provide periodic reports to OCR for three years, and paid $1 million resolution amount.
- University of California at Los Angeles Health System (UCLAH) — result of two separate complaints filed by celebrity patients of workforce members looking at their PHI without a work-related need. OCR found employees repeatedly accessed PHI without a work-related need. UCLAH was to implement a corrective action plan to remedy gaps in its HIPAA compliance program, engage a third-party monitor, provide periodic reports to OCR for three years, and paid $865,500 resolution amount.
- Blue Cross Blue Shield of Tennessee (BCBST) — first enforcement action from a reported breach of 500 or more individuals due to a theft from a leased facility of 57 unencrypted computer hard drives containing PHI of over one million individuals. OCR found BCBST failed to implement appropriate administrative safeguards to protect information at leased facilities by not performing the required security evaluation in response to operational changes and it failed to implement appropriate physical safeguards by not having adequate facility access controls. BCBST implemented a corrective action plan to remedy gaps in its HIPAA compliance program, engaged a monitor to review BCBST compliance, and paid $1.5 million resolution amount.
- Phoenix Cardiac Surgery, P.C. (Phoenix Cardiac) — report that a physician practice was posting clinical and surgical appointments for its patients on a publicly accessible Internet-based calendar. OCR found Phoenix Cardiac implemented few policies and procedures to comply with the rules and had limited safeguards to protect PHI. Phoenix Cardiac was to implement a detailed corrective action plan to safeguard PHI and paid $100,000 resolution amount.
- Alaska Department of Health and Social Services (DHSS) — from a self-reported
breach to OCR, due to the theft from an employee’s vehicle of a USB hard drive that possibly contained ePHI. OCR investigation found Alaska DHSS did not have adequate policies and procedures to safeguard ePHI, it had not completed a risk analysis, implemented risk management measures, done security training for its employee, implemented device and media controls, nor addressed encryption. Alaska DHSS submitted a strong corrective action plan that included addressing all of the findings while safeguarding ePHI for its Medicaid patients, engaging third-party monitoring, providing periodic reports to OCR for three years, and paid $1.7 million resolution amount.

- Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Incorporated (MEEI) — from a self-reported breach to OCR, due to the theft of an unencrypted laptop containing ePHI of MEEI patients and research subjects. OCR found MEEI failed to comply with certain HIPAA security rule requirements such as conducting a risk analysis, implementing security measures to ensure confidentiality of ePHI, and lacked certain policies and procedures. MEEI submitted a strong corrective action plan to address the findings to safeguard ePHI, identify a security official, engage a third-party monitor, provide periodic reporting to OCR for three years, and paid $1.5 million resolution amount.

- Hospice of North Idaho (HONI) — from a self-reported breach to OCR, due to the theft of an unencrypted laptop computer with ePHI of 441 patients. OCR found HONI had not done a risk analysis to safeguard ePHI nor did HONI have policies or procedures on mobile device security. HONI submitted a corrective action plan to safeguard ePHI, including periodic reports to OCR for two years, and paid $50,000 resolution amount.

The theme in these resolution agreements is consistent, and compliance and privacy professionals can use the corrective actions to assess that their shops are in order. To summarize the corrective action plans, CEs should ensure that they have:

- written policies and procedures on physical removal and transport of PHI; encryption for devices; restricting access to ePHI for work-related reasons and sanctioning employees that do not comply; restricting access to ePHI to authorized users of portable devices; PHI safeguards; and security incident identification, reporting, and response;
- distributed policies and procedures and trained its workforce on its policies and procedures;
- regular review, revision, distribution, and training on all HIPAA privacy and security policies and procedures;
- regular and robust training for all employees addressing employee responsibilities under HIPAA;
- designated a security official;
- conducted a risk analysis that complies with the HIPAA security rule; and
- a risk management plan as required by the HIPAA security rule to address risks noted in the risk analysis.

Civil Monetary Penalties (CMPs)
Cignet Health of Prince George's County (Cignet) was the first and only case during calendar years 2011 and 2012 where CMPs were issued by the Department for violations of the HIPAA privacy rule. The Department imposed $4.3 million CMPs to Cignet for violating 41 patients' rights by denying them access to their medical records when requested and for Cignets' refusal to respond and cooperate with the investigation. The patients individually filed complaints with the Department, and that initiated the investigation into each complaint. OCR found Cignets' failure to

Continued on page 69
Electronic Health Record

making the entry to ensure accuracy as well as a description of repercussions for improper use.4

- **Training.** Providers and other staff documenting and reviewing medical records should be trained on proper and improper use of the copy and paste function. Additionally, compliance officers should receive thorough training on their institution’s EHR system and should become involved in developing training protocols for staff regarding its proper use.

- **Auditing.** Organizations should develop an audit plan. First, organizations should determine the extent to which usage of the copy and paste function can be tracked to create an audit trail. Testing should then be conducted to determine what can and cannot be audited, consulting with information technology (IT) staff and system vendors.

Although the use of the copy and paste function in the EHR is a hot button issue for the OIG, compliance officers can take steps to discourage misuse of the function. Organizations should establish guidelines to clearly outline the appropriate use of the function, highlighting the provider’s responsibility for ensuring accuracy in the record and sanctions for misuse. Training and auditing will also help to mitigate the risks of using the copy and paste function. Additionally, consulting with the organization’s IT staff and EHR system vendor can help determine optimum use of audit log functions.

---

**Endnotes:**


---

**Compliance and Enforcement (Continued from 26)**

cooperate as willful neglect to comply with the HIPAA rules resulting in greater CMPs.

**Subpoenas**

OCR issued an investigative subpoena to a social networking Web site company for documents in its possession for any accounts held by a particular physician for a specified period of time. OCR was investigating a complaint alleging that the physician had impermissibly disclosed a patient’s PHI by posting a photograph of the patient on the Web site with a statement about the patient’s health condition. The company produced the requested information, and OCR found that there was insufficient evidence to support the allegations.

**Audits**

The HITECH Act authorizes and requires the Department to conduct periodic audits of CEs and BAs. Being selected for an audit is based on objective criteria and is not the result of a complaint investigation or a compliance review. OCR plans to share best practices it learns through the audit process and to develop guidance documents for CEs and BAs on compliance challenges. OCR has a comprehensive audit protocol...
for privacy, security, and breach notification that can be found at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html. CEs and BAs are encouraged to use this tool to assess their compliance and implement program gaps so that the CE or BA will be prepared should they be selected for an audit.

By December 2012, OCR had completed its pilot audit program of 115 CEs (47 health plans, 61 health care providers, and 7 health care clearinghouses). Thirteen of the CEs had no findings or observations; providers had the greatest percentage of findings and observations, security accounted for the majority of findings and observations, and small CEs continued to show deficiencies in all areas — privacy, security, and breach notification.

The privacy rule findings of the CEs audited included shortcomings for the rights of individuals to receive a notice of privacy practices of the CE, access to their PHI, and in authorizing disclosure of their PHI. The findings from the audited CEs included lack of security rule compliance related to assessing the risks to their ePHI, implementing protections for removable media that stores ePHI, and controlling and monitoring access to ePHI. The Breach findings were discussed in the other report to Congress. OCR focused its outreach and technical assistance to address these areas.

In 2013, OCR engaged an audit firm to evaluate its audit program, and OCR is using these findings and recommendations for its future auditing program. OCR is updating the audit protocol and will post it on its Web site for CEs and BAs to conduct internal assessments using the updated protocol.

**FUTURE ENFORCEMENT ACTIONS**

OCR has limited resources and therefore plans to focus its resources on “cases that provide OCR with the maximum opportunity to effect change within the health care industry.” OCR will continue to review all complaints and determine if the complaint meets criteria for an investigation or if the complaint can be resolved through technical assistance to the CE or BA without an investigation. OCR will continue to identify and investigate “high-impact” cases that send strong enforcement messages for HIPAA rule compliance. OCR works with other agencies to enforce the HIPAA rules including the Federal Trade Commission, the Department of Justice, the Office of the Inspector General, and State Attorneys General.

**REFERENCE:**


**FIVE QUESTIONS TO ASK CONTINUED FROM 30**

- **Determine System for Handling Notifications:** Mishandling notifications can lead to fines and other unbudgeted expenses, as well as a negative impact to brand reputation and customer loyalty. There is generally little time to verify addresses, print and mail notification letters, and set up a call center and other services for impacted stakeholders. Thus, the company should identify a vendor — in advance of a breach — that has the resources and capabilities to establish call centers and notify thousands, or even millions, of individuals by mail or email. Also, the company should consider creating a dark Web site around a breach, which would go live if the real thing occurs.

- **DO YOU HAVE A CULTURE OF COMPLIANCE?**

Beyond establishing policies, procedures, and codes of conduct, management should assure that the workforce and business associates clearly understand what relevant laws, regulations, and rules mean in a work-a-day world. In essence, a company
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.