HCCA™

hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

MAY 2018

Ensuring that rules and regulations are met

an interview with **Lynda S. Hilliard**

by Emmelyn Kim, MA, MPH, CCRA, CHRC; and Cynthia Hahn

Best practices for handling large-scale HIPAA breaches in research

» Assemble a task force involving multiple stakeholders to handle large-scale breaches.

» Plan ahead for any required notifications to required entities.

» Develop a robust corrective and preventive action plan.

» Prepare for Office for Civil Rights (OCR) investigations and interactions.

» Continue to monitor and evaluate organizational risks.

***Emmelyn Kim** (ekim@northwell.edu) is Assistant Vice President, Research Compliance & Privacy Officer at The Feinstein Institute for Medical Research, Northwell Health in Great Neck, NY.*

***Cynthia Hahn** (chahn@intresearchstrategy.com) is President of Integrated Research Strategy, LLC in East Northport, NY.*

linkedin.com/in/emmelynkim *http://bit.ly/in-CynthiaHahn*

Kim

Hahn

Research organizations that are considered covered entities as defined by the Health Insurance Portability and Accountability Act (HIPAA) must establish effective programs that regularly evaluate and mitigate HIPAA Privacy and Security risks. The advancement of technologies requires entities to deploy increasingly sophisticated strategies to effectively monitor and secure their information to minimize exposure. Although many covered entities have developed programs to mitigate these risks, they continue to experience breaches as a result of hacking or IT incidents, improper disposal, loss, unauthorized access or disclosure, or theft.[1] Covered entities should be prepared to investigate and handle any HIPAA breach notifications that may arise (including those from business associates) to ensure prompt reporting to the Office for Civil Rights (OCR) and applicable research-related regulatory authorities, sponsoring agencies, and any affected research participants within specified time periods. In the case of large-scale breaches that impact more than 500 individuals, additional steps are necessary that require a response team to effectively meet requirements of the HIPAA Breach Notification Rule under the Health Information Technology for Economic and Clinical Health (HITECH) Act.[2] This article highlights best practices and practical planning considerations for research organizations to effectively handle large-scale breaches.

Too large to handle? Assemble a task force

Ensuring that potential HIPAA breaches are reported to responsible organizational officials as soon as possible is critical in order for organizations to quickly gather facts and perform a HIPAA breach analysis, because the clock starts ticking at the point of discovery. When it is evident that a large-scale breach is at hand, a review of the events, recommended corrective and disciplinary actions in compliance with institutional policy, a gap analysis, and development of preventive action plans can feel daunting. Assembling a task force allows multiple stakeholders to work on various aspects of the case simultaneously. This team approach facilitates coverage and coordination of multiple requirements over a short amount of time. Each task force member is given an assignment and required to report back during status updates, which provides greater flow of communication and cohesiveness. Task force members oversee specific aspects of the investigation, provide updates to the appropriate institutional parties, and plan and determine next steps.

Gathering facts and data to inform the breach analysis and for required reporting to the OCR is an important part of the internal investigation. During the initial assessment period, remember that any actions taken should be meaningful and practical. Although Compliance may be involved in the investigation, gathering all of the essential information may be complex and require assistance from members of the task force. For example, in the case of a breach due to theft, Corporate Security may need to contact local or federal law enforcement and be involved in conducting interviews and sequestering materials or documents. Information Technology (IT) Security may need to evaluate hardware and software, review similar pieces of equipment or a copy of the data that was lost, or retrieve emails. Human Resources (HR) may need to assist in reviewing employment files, agreements signed by individuals, and disciplinary actions. This information may be requested by the OCR during their investigation. In a research setting, the Institutional Review Board (IRB) and the Grants or Contracts office may need to assist in identifying any impacted research studies and evaluating sponsor notification requirements. In general, a task force will gather all necessary facts, such as understanding what happened, who and what was involved (including whose data was potentially compromised), and where, when, and how it occurred. The task force should include senior representatives with decision-making authority to ensure that actions can be taken quickly and effectively.

Consider including representatives from the following areas:

- Research/Corporate Compliance
- Legal Affairs
- IT Security
- Facility/Corporate Security
- Human Resources
- Public Relations
- Institutional Review Board/Human Research Protection Program
- Research/Institutional Administration or Operations
- Finance, Grants, or Contracts
- Policy and Training
- Risk Management

Executive and facility leadership/Institutional officials

Notifications of affected individuals will require assessment of whether any outside resources may be needed. For example, seeking outside legal counsel may be beneficial if the breach notification is required for individuals residing in other states or countries. For any breaches involving PHI of more than 500 individuals, it is essential to plan ahead for individual and media notifications by involving the Public Relations (PR) department. Keep in mind that a task force may last for many years and will likely be involved during any investigations, resolution, and corrective actions required by the OCR.

Plan ahead for notifications

Establish a notification timeline by working backwards from the 60-day notification period for individuals to ensure that you meet the HIPAA Breach Notification Rule requirements. Keep in mind that notification of other entities may be required and may not only involve affected individuals or the OCR. This may include notifying institutional committees or officials; other institutions; state, federal, and international agencies; and the media. It may be advisable to work with your Communications or PR department to develop a media kit that includes contact information for appropriate institutional officials and basic talking points, which can be provided to departments or individuals responding to individual or public media inquiries. This prevents callers from being "passed around" and allows for simple questions to be answered. Media and website notifications should be planned as well and should include review and direction from the PR department.

When research studies are impacted, notifications to relevant research committees and offices are essential to ensure the institution meets required reporting obligations. Institutional research administrative offices can assist in coordination of effort, which may include the institutional Human Research Protection Program (HRPP), and identifying any reviewing IRBs, the Grants and Contracts office, and any other relevant research office or committee within the organization. The IRB is responsible for reviewing and approving human subjects research, including communications to research participants, and will also need to facilitate notification of any agencies that regulate research as appropriate, such as the Office for Human Research Protection (OHRP) and the Food and Drug Administration (FDA). Checking with the office that handles research grants and contracts regarding any required notices to sponsoring agencies is another important step. Therefore, additional time should be factored into the timeline to ensure appropriate notifications are reviewed in time by all parties.

...notifications to relevant research committees and offices are essential to ensure the institution meets required reporting obligations.

Prior to individual notification, establish a resource plan, such as staffing or procuring services from a call center and a mail clearinghouse, implementing procedures to handle inquiries, or offering credit monitoring. A toll-free number should be provided that's answered by a live person with a dedicated after-hours voicemail that is checked regularly. Once the procedures are set up and the notification letters are approved, they should be tracked with a quality-check component embedded within the process. OCR will ask for the number of notifications that were sent out and undeliverable, how many calls were received, the nature of the calls, and their resolution.

Expect hundreds of calls as a result of individual, media, and website notifications, possibly from people not directly impacted, but who had seen the news and were concerned or curious. Developing a detailed standard operating procedure (SOP) and escalation process for concerned callers or individuals who indicate that they may have been the victim of identity theft is helpful. It is important to investigate and document all complaints to determine whether there was any harm to any individuals and whether any further actions are warranted.

Develop a robust corrective and preventive action plan

First, conduct a root cause analysis with the task force, listing factors that contributed to the event and reviewing existing organizational policies and procedures. Review resources that may be needed to take action, and tighten up internal controls to prevent recurrence. It is important to consider external resources (e.g., an IT security firm, outside counsel) if the organization does not have the expertise or experience in handling certain aspects of the investigation. Initial corrective actions should focus on identification and remediation of effects and risks directly related to the incident. Disciplinary actions and re-education or retraining for individuals or departments may be required. As you work through the investigation, it may also be necessary to broaden any corrective actions, such as expanding efforts to an entire facility or institution (e.g., retraining the workforce, rolling out larger scale efforts around encryption, and tracking of all devices). Broader efforts will also require increased planning and tracking to ensure that all proposed corrective actions were completed.

Aside from immediate corrective actions, consider improvements in policies and controls that may be needed to prevent recurrence of issues. Anticipate reviewing relevant policies and ensure that HIPAA training is comprehensively embedded in ongoing activities and communications. This will require departments or committees that track relevant HIPAA and research policies to work collaboratively to ensure that the policies are reviewed and updated regularly. Education and training programs may need to be reviewed, and possibly enhanced, to ensure they are frequent enough, robust, and reach the right members of the workforce. This may include training during new employee orientation, online and in-person research education trainings, and verbal and written communications during departmental and institution-wide research meetings. Consider creating various tools and guidance documents that contain HIPAA Privacy, Security, and breach notification reminders to distribute to researchers and staff. Frequent communication and dissemination of information is necessary, due to both changes in personnel and changes to the physical and technical environment that may present new risks.

In general, embedding practical and applicable HIPAA tips and reminders into training heightens awareness of vulnerable areas and promotes greater dialogue around these topics with staff. Tracking and documenting efforts are also necessary, because they will need to be included in any correspondence or reporting to the OCR. In addition, institutional research offices or committees and reviewing IRBs will need to be informed of the corrective and preventive actions taken.

Prepare for OCR investigations and interactions

OCR investigations may take years to complete and involve a number of inquiries, on-site interviews, and requests for documents and information. The task force should be involved in reviewing any requests for information and documents submitted to the OCR, and they should be updated regarding OCR communications. The requests may be rather complicated and require completion within a short period of time; therefore, a central point of contact (usually a senior representative from legal counsel or Compliance) should be tasked with communicating with the OCR. Key individuals can be tasked with drafting any responses when they have knowledge of where to obtain the information and the authority to request needed documentation. An organized system for maintaining documentation associated with the investigation and with OCR communications is necessary, because you will likely need to refer to prior responses when you work on subsequent requests for information.

On-site OCR interviews require ample planning to ensure that staff are present and accurate information is available if requested by investigators. Working with Legal Affairs will be essential to this process as well as during subsequent interactions. During the resolution stage, any monetary penalties, agreement terms, and corrective action plans will need to be carefully reviewed and negotiated with your legal counsel and institutional officials. Corrective action plan terms can span over a few years, and it's likely that the task force will need to oversee implementation and reporting to OCR over that period of time.

Monitor and evaluate risks

Ensure that your organization takes proactive steps to monitor and evaluate risks on a regular basis. There are a variety of ways to do this, and there are likely departments that are already involved in actively monitoring risks. Compliance departments typically incorporate HIPAA assessments into their ongoing reviews and are involved in evaluating and trending data.

Research institutions can also consider preventive controls, such as reviewing proposed research plans before initiation.

Research institutions can also consider preventive controls, such as reviewing proposed research plans before initiation. For example, evaluating HIPAA privacy and security controls (regardless of the IRB that is used) as part of an institutional approval process for clinical research studies may be a beneficial step. This will also enable researchers to think about the PHI they plan to collect and how they will collect, transfer, and disclose the information. Compliance should then evaluate adherence to the research plan during routine, post-approval reviews. Organizations should offer consultations to the IRB and researchers by their IT security group to ensure adherence to security requirements.

Regular evaluations of organizational risks by formal committees made up of individuals from various parts of the organization are necessary. Risk governance committees can review the results of audits or assessments to evaluate trends and the resultant vulnerabilities and impacts to the organization. They can agree upon corrective and preventive actions, any proposed compensating controls, and any required escalation of the issues detected. Committees can also evaluate regulatory and market trends to identify areas where further research and development and policy revisions are needed. Interviewing stakeholders (e.g., researchers, administrative office staff, and departmental administrators) to obtain further insight into vulnerabilities and concerns should be part of risk assessments. The results of the assessments should be used to inform future reviews, education and training efforts, and policy development. Working collaboratively with other departments and stakeholders, such as IT Security and Compliance, in addition to obtaining feedback from the workforce, will help you effectively evaluate organizational HIPAA risks and implement stronger internal controls.

Conclusion

Keeping up with HIPAA compliance requirements in a research environment is an ongoing challenge that will require involvement by many organizational stakeholders. One of the inherent qualities that researchers bring to institutions is innovation, which often encompasses the use of new technologies that the IT group may not have evaluated or implemented policies or adequate controls for. This is complicated by the fact that exchange of information in a research environment is often multi-directional, may cross state and international borders, and often involves various entities (e.g., sponsors, collaborators, central coordinating centers).

Complex medical devices are increasingly more common, consisting of multiple components that may collect data directly from patients and send data to various destinations, including tablets reviewed by physicians, the electronic medical record, or an external cloud-hosted platform. The use of non-standard equipment, social media, apps developed by researchers, and devices provided to research participants may also present challenges around encryption and other types of security controls. Therefore, research organizations must be vigilant and take actions to regularly evaluate and mitigate HIPAA compliance risks. It takes a large effort to monitor and implement controls while allowing research and business activity to occur uninterrupted; organizational risks constantly evolve and, therefore, it requires a collaborative effort for effective and successful risk management.

1. Office for Civil Rights (OCR) Breach Portal: Cases Currently Under Investigation. Available at http://1.usa.gov/1yY3CaK
2. 45 CFR §§ 164.400-414 (HIPAA Breach Notification Rule, Subpart D, Administrative requirements and burden of proof)