COSMOS
Navigate the Compliance Universe

Compliance Today - May 2018
Best practices for handling large-scale HIPAA breaches in research

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

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
- linkedin.com/in/cynthia-hahn-288a556

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