COSMOS
Navigate the Compliance Universe

Compliance Today - June 2022
Incorporating research compliance into healthcare privacy and security risk management programs

By Emmelyn Kim, MA, MPH, MJ, CHRC, and Hamangi Patel, LMSW, CCRP, RQAP-GCP, CHRC

Emmelyn Kim (ekim@northwell.edu) is VP, Research Compliance & Privacy Officer, and **Hamangi Patel** (hpatel17@northwell.edu) is Director, Research Compliance, The Feinstein Institutes for Medical Research, Northwell Health, New York.

- linkedin.com/in/emmelynkim
- linkedin.com/in/hamangipatel

Emmelyn Kim

Hamangi Patel

Healthcare environments are extraordinarily complex and heavily regulated through a variety of local, state, and federal rules. Privacy and security are major risk areas, especially given the increase in cybersecurity threats and attacks.[1] Healthcare organizations often have an array of ongoing research activities to utilize the rich data sources provided by direct access to patients and medical records. However, the use and disclosure of protected health information (PHI) in healthcare environments for research require special attention, not only to the Health Insurance Portability and Accountability Act (HIPAA) rules, but to the research provisions within the rules and other research requirements. This requires coordination with research stakeholders such as institutional review boards (IRBs) that often act as privacy boards, privacy officers, and human research protection programs (HRPPs).

Over the past decade, better technology and computing capabilities have resulted in an increase in research activities using digital health technologies such as artificial intelligence, devices and applications, and data mining software that searches electronic health records for potential research participants, among many others. Technology has also enabled remote clinical trials to be offered in communities outside of healthcare facilities. All of this has changed the research landscape and the overall risk profiles at healthcare systems, particularly privacy and security risks.

Since research activity in healthcare organizations often involves the use and disclosure of PHI outside of treatment, payment, and healthcare operations, it requires special attention to ensure that the uses and disclosures comply with HIPAA rules and determinations of the reviewing IRB or privacy board. Additionally, research often involves many other rules outside of healthcare that govern the activity. Ensuring that organizations are meeting other applicable regulatory requirements in the research space, such as those enforced by the Food and Drug Administration and the Office for Human Research Protections and requirements by funding agencies and sponsors, is also important. Therefore, compliance programs should incorporate research risks into their overall risk assessment to assess organizational risk accurately and effectively. This article will provide considerations and best practices for incorporating research compliance into the healthcare privacy and security risk management framework.

Assessing your research organizational structure and portfolio

The first step is to get a sense of common research activities using data containing PHI (in both paper and

electronic form) that occur at your healthcare organization. Requirements for research data involving the use and disclosure of PHI by a covered entity depend on how the organization is structured (i.e., single covered entity, participating in an organized healthcare arrangement, or hybrid entity), whether there is an academic component that encourages research activities, and whether the organization further segregates the research data that is not derived from healthcare services or payments. Keep in mind that there is often multidirectional data sharing in the research environment among internal and external research collaborators, sponsors, vendors, data coordinating centers, and participants. Data sources may vary and can be generated by researchers and research participants (through surveys, devices or apps, electronic data capture systems, or case report forms) from electronic health record data retrieved by research or informatics groups or from data repositories or secondary data sources that were previously collected for research purposes.

There is a variety of pathways under HIPAA for the use and disclosure of PHI for an array of research purposes. This can include preparatory research activities that often involve review of medical records to determine whether there are enough patients with certain conditions and/or characteristics prior to proposing a research study or to aid in study recruitment. Research often involves the retrospective review of PHI that requires a waiver or alteration of HIPAA authorization by the IRB or privacy board. Limited data sets that exclude direct PHI identifiers are another mechanism used for research pursuant to a data use agreement. Another common activity involves prospective research that requires seeking HIPAA authorizations from research participants or their legally authorized representatives. Understanding the various pathways for the use of data with PHI in research is key.

When you assess your organizational research structure, it is important to take note of the factors listed in Table 1.

Human subjects or clinical research	Research infrastructure
• HRPP/IRB/privacy board • Types of research • Location/setting of research (e.g., local, national, or global) • Clinical data groups/programs • Clinical informatics/data science • IT security • Data repositories, data lakes • Data governance and strategy • Health information exchanges/networks	• Research administration, operations, research support, regulatory and compliance offices, privacy officer(s), committees, legal, etc. • Institutional research approval processes • Electronic data management systems (capture/storage/transfer) • Monitoring or auditing, reporting, and management of privacy and security concerns in research • Training and educational/academic components • System-level research privacy and security committees

Table 1: Factors to consider when assessing your organizational research structure