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

Integrating research compliance into the risk management framework

Research compliance programs vary across organizations and are dependent on the research portfolio, including the nature and scope of research activity, size of the healthcare organization, and resources. These programs have a specific focus on the rules and regulations pertaining to research activities, collaborations, sponsor or funding requirements, and governmental assurances. Such programs seek to reduce organizational risks by monitoring compliance, ensuring issue escalation, and providing education and consultation for researchers. Research compliance programs focus on a unique and evolving area within the healthcare environment and, as a result, can create a more comprehensive healthcare compliance program.

Creating research compliance programs requires an investment in resources, such as in staff with research expertise, experience, and knowledge to effectively monitor research activities and troubleshoot. Organization-wide research policies are important in establishing compliance authority, roles, and responsibilities. However, incorporating research compliance into the risk management framework involves creating a seat at the table with direct and regular reporting of compliance matters and risks to management and a governance board alongside corporate healthcare compliance partners, especially for large research programs. Providing regular research insights for risk management as part of an enterprise risk management framework is also important.

Program effectiveness is often dependent upon communication channels and establishing relationships. Regular communication with key stakeholders in privacy and security in the healthcare and research areas is crucial. Integrating compliance processes into the HRPP/IRB and privacy board processes is also necessary and can enhance communication channels. Acting as a compliance liaison between research and healthcare areas can be helpful.

See examples of ways to integrate research compliance into the privacy and security risk management framework in Table 2.

Liaison with HRPP/IRB/researchers	Liaison with corporate compliance

• Privacy and security incidents related to research reported to HRPP/IRB routed to research compliance for investigation and breach reporting (if applicable) • Institutional approval process directs global research to research compliance for international privacy and data protections review • Access to HRPP/IRB systems to confirm research studies, approvals, and personnel • Privacy and security of research reviewed during audits with incidents reported to HRPP/IRB • Notification to research participants regarding any breaches require coordination with IRB of record/HRPP for review of incident and correspondence	• Compliance hotline calls and investigations involving research routed to research compliance for further review or joint investigation and coordination with HRPP/IRB if needed • Incidents handled through a uniform compliance process, including documentation and reporting • Large-scale investigations and notifications to local and federal agencies and international authorities regarding breaches require coordination with corporate compliance, legal, risk management, IT security, research leadership, and other stakeholders • Research-related incidents included in overall compliance metrics • Research representation in corporate compliance committees

Table 2: Ways to integrate research compliance into the privacy and security risk management framework

Identifying and managing unique research risk areas locally and globally

For compliance programs to successfully identify unique research risk areas, it would be best to start with the organization's research portfolio and review risk areas such as complexity of studies, participant enrollment targets, locations where the study is conducted, and reach. The clinical care scope of most US-based healthcare organizations is primarily local, whereas research, global collaboration, funding source, and target population may require the organization to identify and assess risk based on regulatory, financial, and legal aspects of global compliance. Advanced technology has also enabled researchers to collect and share large data sets with various collaborators in real time, requiring implementation of enhanced processes and safeguards. As clinical trials increasingly provide opportunities for individuals to participate locally or overseas, the use of smartphones and tablets and collection of data from devices, implanted or worn, cannot be managed with the same risk management framework that has been previously employed. Researchers are building collaborative relationships, looking to work with organizations and colleagues within their specialty areas, domestic and international, to engage populations that were previously limited to research studies available within the confines of their local areas. Sharing of data must be assessed in conjunction with the organization's IT security teams and legal affairs to ensure platforms used between individuals or organizations and any agreements have been reviewed and vetted.

Along with multidirectional data sharing, research may include sharing of samples, specimens, images, and technology platforms provided by vendors, which are added risks that may affect the privacy and confidentiality of research participants. Compliance programs should ensure there is communication with researchers to assess their needs through surveys and consultations. Working with key stakeholders within research and corporate partners such as legal, risk management, technology transfer, and IT security is essential to appropriately identifying, assessing, and mitigating risks. Compliance programs should also implement checkpoints and

provide education through guidance material and resources on how to ensure compliance. Collective efforts promote effective sharing of information across a wide range of team members throughout the organization and with external collaborators.

Integrating privacy and security reviews into research

Privacy and security reviews should be integrated into areas that involve research and may not be covered by standard healthcare compliance reviews to ensure that research studies are conducted appropriately locally and globally. Reviews of research study approvals, HIPAA authorizations or waivers, agreements, consent forms, and research protocols that outline study procedures and information collected and approved under the organization's institutional approval process and reviewing IRB and privacy board are important. Incorporating these elements into research conduct reviews can help ensure study teams are appropriately protecting the privacy of research participants enrolled in studies and the security of the information. Reviews also ensure that research teams are aware of the appropriate escalation process if a privacy or security incident were to occur. During these reviews, the researchers should also be reminded of the appropriate steps to take when transmitting data to research study sponsors or collaborators as they may require only deidentified data. Additional investigation of privacy and security safeguards can be conducted upon receipt of an incident that is reported to the research compliance program, IRB, HRPP, or corporate compliance hotline. In addition, on-site reviews at research facilities or areas where clinical research visits occur can help assess whether physical safeguards are appropriately implemented. This also provides an opportunity for researchers to inquire with research compliance staff about new research studies that may be starting or potential areas for review to ensure compliance.

Regular auditing, in combination with privacy monitoring and data loss prevention systems that provide alerts based upon algorithms, can help compliance efforts. These systems alert compliance staff when data sets containing PHI or other sensitive information are shared outside the organization's network or when there may be inappropriate electronic health record access. The system alert would prompt an investigation, mitigation, and reeducation of policies and best practices when accessing and working with sensitive data. This is especially important as healthcare workers continue to work in a hybrid environment. If warranted, further reviews of other research-approved databases and individual interviews can help confirm whether access to or sharing of PHI in relation to their professional responsibilities in research was appropriate. A combination of software monitoring and routine reviews helps research compliance program staff assess risks simultaneously across the organization. Compliance program staff should review audit and monitoring findings on a quarterly basis to identify trends and high-risk areas and provide education, training, and guidance to researchers to reduce risks.

Global engagement considerations

Understanding international business activities and the reach of an organization can provide insight into potential global research activities. Since this area can rapidly change, compliance staff should frequently survey researchers to gauge potential and ongoing global engagements. The COVID-19 pandemic played an integral part in fostering international collaborations to gather and disseminate worldwide data. This required organizations to review their international business activities and consider global privacy and data protection laws and regulations like the General Data Protection Regulation. This is due to the extraterritorial scope built into such regulations that may extend to US-based institutions.

Researchers who plan to process personal data from individuals or data subjects based in countries with data protection laws or regulations will need to determine up front whether they are subject to those rules by virtue of their activities and contractual arrangements. Research involving recruitment of participants internationally requires additional privacy education to ensure the research team is aware of their responsibilities, limitations of

collected data, and how to address inquiries regarding data subject rights. These checkpoints can be incorporated into the institutional approval or IRB approval process, screening of international work arrangements, and reviews of research agreements. Healthcare organizations that support researchers wishing to collaborate with colleagues and organizations overseas must be aware of such regulatory requirements, create specific policies, set up the appropriate review processes and safeguards to escalate incidents, as well as address data subject rights in a timely manner.

International remote work and travel involving employees, visiting scientists, and scholars should also be considered, as some may choose to return to their home countries to continue their work or may be required to work abroad for periods of time. This can present other complexities and compliance risks outside of privacy and security. Compliance programs should consider gathering key stakeholders and using system-wide committees to ensure checkpoints and review procedures are implemented in support of global engagements.

Other considerations

Incorporating research compliance into healthcare compliance programs requires structure, standardization, communication, and strategic planning. Create standardized checklists, analysis tools, and standard operating procedures for compliance teams. Review audit findings for privacy and security trends and high-risk areas to pay close attention to to inform development of educational materials. Review institutional policies regularly to include regulatory updates, integrate them into communications, and modify and update compliance tools regularly to keep up with the changing regulatory environment.

Create a variety of privacy and security resources for researchers. This can include clear and simple guidance documents, checklists for study teams, interactive compliance training or educational sessions (in person or virtual), regular meetings with management, and regular research communications that include compliance contact information. These tools can help foster a more transparent relationship between researchers and compliance staff, facilitate proactive incident reporting, and promote preventive behaviors.

Work with other stakeholders to better monitor and manage risks. Participating in organization-wide committees that include stakeholders can help facilitate greater communication and awareness of privacy and security issues in the research space. Committees can be at an executive or management level, organization-wide, or research focused. They should optimally be focused on assessing privacy and security vulnerabilities, impact, and overall risks and provide a forum to discuss issues.

Conduct annual research risk assessments to effectively develop compliance work plans. This is done by interviewing certain stakeholders (e.g., researchers and staff, research leadership and administrators, organizational leaders, research support, and IT security) and evaluating internal and external compliance trends. For example, review hotline call volumes, incidents and audit findings within the organization, and news articles pertaining to breaches outside the organization to assess any current trends in the field. Evaluating regulatory agency enforcement and priority areas is critical to determining priority risk areas, which can help compliance departments assess needs and determine whether additional resources are required or need to be considered in the budget.

Conclusion

As healthcare organizations continue to undergo digital transformation at a faster pace than ever before, their risk profiles are evolving. This requires compliance departments to adapt, advance, and work with a wider range of partners to effectively manage risk. Continual assessments of research portfolios, digital health technologies, and data flows, in combination with regular evaluation of local and global activities, are essential to categorizing varying levels of risk. In addition, governmental efforts to bolster national security and integrity of federally

sponsored research and development will require certain research organizations to strengthen their research security programs.[2] Considering research programs typically introduce innovative technologies, this requires healthcare organizations to stay ahead of the curve. The healthcare risk landscape continues to shift in this new pandemic era, and privacy and security will remain critical focus areas, particularly as cybersecurity threats and public demand for privacy protections increase. Healthcare compliance programs would be best equipped to handle and mitigate these evolving risks by incorporating research compliance into their overall risk management approach.

Takeaways

- Recognize how protected health information (PHI) is used and disclosed for research purposes, which may differ from treatment, payment, and healthcare operations.
- Assess common research activities involving data containing PHI in relation to your research organizational structure and portfolio.
- Implement effective ways to integrate research compliance into the healthcare compliance framework.
- Identify and manage unique privacy and security risk areas locally and globally in research.
- Work with other stakeholders in research to better monitor and manage risks.

1 Cybersecurity & Infrastructure Security Agency, "Ransomware Activity Targeting the Healthcare and Public Health Sector," Alert (AA20-302A), last revised November 2, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-302a.
2 National Science and Technology Council, Joint Committee on the Research Environment, Subcommittee on Research Security, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*, January 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.