Northwell Health®

R12B Incorporating Research Compliance into Privacy and Security Risk Management for Healthcare Organizations

HCCA Research Compliance Conference ◆ Virtual◆ June 16, 2021

Emmelyn Kim, MA, MPH, MJ, CHRC
AVP, Research Compliance & Privacy Officer

Hamangi Patel, LMSW, CCRP, RQAP-GCP, CHRC
Director, Research Compliance

1

Objectives

- Implement effective ways to integrate research compliance into the healthcare compliance framework
- Identify and manage unique areas locally and globally in research pertaining to privacy and security
- Work with other stakeholders in research to better monitor and manage risk at healthcare organizations

2

2

3

Research Challenges in Healthcare Environments

- ✓ High risk due to highly regulated environment layered on top of healthcare
- ✓ Requirements for research data with PHI use and disclosure depends on how the organization is structured (e.g., OHCA, Hybrid)
- ✓ Multi-directional data sharing among research collaborators, sponsors, vendors, data coordinating centers, etc.
- ✓ Decentralized and many grey areas (quality improvement vs. research)
- ✓ Privacy and security considerations for innovative and international activities

Research does not often fit neatly into regulations or established healthcare environments or systems

4

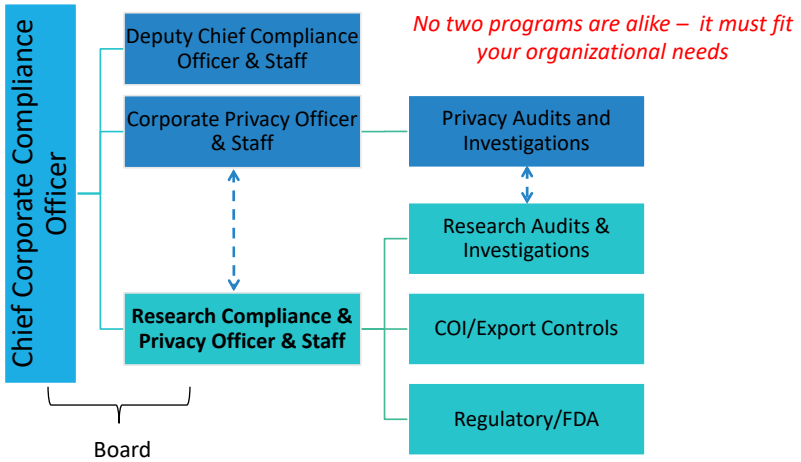
4

Research Compliance Programs

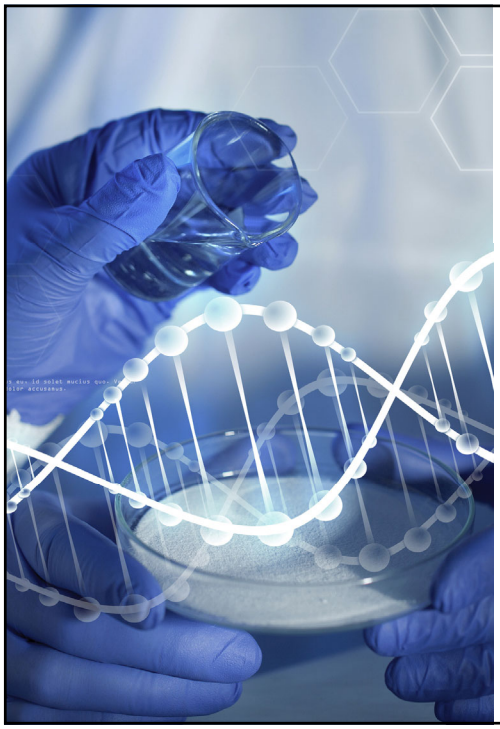
- ✓ Ensure compliance with research regulatory requirements in addition to those in healthcare
- ✓ Reduce organizational risks, ensure human research protections and the integrity of the research
- ✓ Essential to research program accreditation and federal assurances
- ✓ Provide structure for responding to agency investigations, inspections or audits of research activities and sites
- ✓ Focus on a unique and evolving area & provide education on policies and standards
- ✓ Create a more comprehensive healthcare compliance program for organizations conducting research

5

Organizational Structure Example



6



Common Research Activities Involving Data with PHI

- Reviews preparatory to research, retrospective chart reviews
  - Manual review of records or data pulls from EHRs or other data sources by an informatics group
  - Retrospective in nature, no direct interaction with research participants
- Observational studies, surveys, outcomes research, clinical trials, repositories
  - Prospective, interventional or direct interaction with research participants
  - Electronic and/or paper research documentation maintained and shared
- Advanced technology, computing and digital health trends:
  - Large data sets that utilize more sophisticated software, artificial intelligence
  - Electronic consent (e-consent) and data capture processes, remote interventions, video
  - Wearable or mobile devices with 3rd party software or apps, networked, remote monitoring

7

7

Understand and Evaluate Your Healthcare Organization's Research Portfolio & Infrastructure

Clinical Research

- HRPP/IRB/Privacy Board
- Type of research
- Location/setting of research studies
  - Local/national/international

Clinical Data Groups/Programs

- Clinical Informatics/Data Science
- IT Security
- Data Repositories
- Data Strategy and Governance
- Health Information Exchanges

Infrastructure

- Research administration, operations, research support offices, regulatory and compliance committees/offices, legal, etc.
- Institutional research approval processes
- Electronic systems, data management (capture/storage/transfer), sharing
- Monitoring or auditing, reporting and management of privacy and security concerns in research and education
- System level research privacy & security committees

8

Integrating Research Compliance into the Risk Management Framework

- Invest in resources/staff with experience, knowledge and expertise to effectively cover research activities
- Create policies that establish authority, roles and responsibilities
- Create a seat at the table with direct reporting to the board for large research programs
- Ensure regular communication with key stakeholders in privacy and security
- Liaise between research and corporate areas

9

Examples of Integrating Research Compliance into the Privacy and Security RM Framework

Liaison with HRPP/IRB/Researchers

- Privacy & security incidents related to research reported to HRPP/IRB routed to Research Compliance for investigation and breach reporting (if app).
- Access to IRB systems & partner with IT Investigations for security issues.
- Privacy and security of research reviewed during audits and incidents are reported to HRPP/IRB.
- Notification to research participants regarding any breaches require coordination with IRB of record/HRPP for review of incident and correspondence.

Liaison with Corporate Compliance

- Research related incidents from the Compliance Help Line or detected from compliance monitoring/investigations routed to Research Compliance for further investigation.
- Large scale investigations and notifications to state and federal agencies regarding breaches require coordination with the Corporate Compliance Privacy Officer, Legal, Risk Management, IT Security and Research Leadership.
- Incidents included in overall metrics

10

Identify and manage unique areas locally and globally in research pertaining to privacy and security

11

11

Privacy & Security in Research Areas

- Clinical Research & Outcomes Research
- Global and International Activities
- Policies and Procedures
- System Level Committees
- Education & Training
- Auditing/Monitoring

12

12

Privacy & Security Considerations

- Using and disclosing PHI for research purposes is NOT considered Treatment, Payment or Operations (TPO)
- Minimum necessary standard applies to research
- HIPAA authorizations, waivers by the Privacy Board and Reviews Preparatory to Research
- Other types of agreements may be needed: Data Use Agreement (DUA) for limited data sets
  - Accounting of PHI disclosures without the individual's authorization is required except for DUAs

- Who is the study sponsor, collaborator, data coordinating center?
- How will the information be used/stored/transferred/shared?
- Consent form/HIPAA authorization language and requirements?
- Other international privacy requirements?

13

Integrating Privacy & Security Reviews into Research

Research Audits	• Review of research study agreements, documents & institutional approval • Assessment of privacy & security compliance and incidents
HIPAA Review/Rounding	• Rounding at research facilities that are also engaged in clinical activities • Assessment of safeguards for PHI, staff knowledge of HIPAA policies & procedures
DLP Monitoring	• Monitoring the movement of sensitive and highly sensitive ePHI over networks • Algorithm set by IT security and compliance based on risk
Sponsor Monitoring	• Monitoring external study sponsor access to EHR systems & activity • Assessment of IT requisition process & signed confidentiality agreements
Review of data pull & use	• Ensure minimal necessary data is pulled and shared by informatics groups • Review data use agreements with data pulls
Breach Reporting	• Ensure researchers are aware of methods and contacts to report potential breaches

14

14

Global Engagement Considerations

- ✓ Understanding organizational global business activities and reach
- ✓ Surveying research community members
- ✓ Creating specific policies and procedures
- ✓ International remote work and travel involving employees, visiting scientists, scholars, etc.
- ✓ Utilizing system wide committees
- ✓ Setting up check points with study teams and committees
- ✓ Evaluating global privacy regulations
- ✓ Assessing exports of goods and services

15

15

Internal GDPR Assessment Example

Intake Process

- Centralized checkpoint & process
- Review via checklist/ guidance document

Applicability Analysis

- Processing personal data of data subjects in scope?
- Territorial Scope: In territory OR outside territory offering goods or services and/or monitoring behavior of data subjects in territory?

Implementation

- If within scope, determine the institution's role & requirements (Controller and/or Processor role, legal basis, data flow assessment, Data Protection Officer, Data Subject Rights, etc.)

16

Tools and SOPs for the Compliance Team

- Create standardized checklists, analysis tools and SOPs
- Review audit findings for trends and high risk areas
- Review institutional policies regularly to include regulatory updates
- Modify and update tools to keep up with the changing environment

17

Resources for Researchers

- Clear and simple guidance documents
- Checklists for study teams
- Interactive training sessions
- Education sessions offered by all offices
- Monthly meetings with management/service-line directors
- Bi-monthly research update emails
- Contact information posted where research is conducted
- Year-end risk assessment with key stakeholders

18

Conduct a Research Risk Assessment

- Interview stakeholders (e.g., investigators, research staff, administrators, research support staff and organizational leaders)
- How compliant is the organization?
  - History of breach reporting
  - Auditing and monitoring results/trends
- Evaluate regulatory agency priority areas and concerns
- Determine need and high risk areas to inform resources and budget development

Likelihood severity occurs	Potential Severity Rating: Minor	Moderate	Significant	Catastrophic
Very Likely	Moderate	High	Extreme	Extreme
Likely	Low	Moderate	High	Extreme
Unlikely	Very Low	Low	Moderate	High
Rare	Very Low	Very Low	Low	Moderate

19

20

Stakeholders

21

Committees

22

Compliance Work Plan & Program Development

- Based on internal and external risk assessment
- Covers high risk and priority areas
- Incorporate into the annual Corporate Compliance work plan
- Present to the board for approval & disseminate to leadership
- Implement the work plan & evaluate results
- Adjust where needed and repeat cycle

23

Final Takeaways

- Regularly evaluate research compliance needs and adjust based on changes to the organization's research program and portfolio
- Privacy and security will continue to become more complex so integrating research into compliance will help to manage risk for local and global activities
- Keep an eye on emerging technology and big data which will require working closely with key stakeholders outside of Compliance

24

Thank You – Questions?

Emmelyn Kim

AVP, Research Compliance & Privacy Officer

Office of Research Compliance

Northwell Health

Phone: (516) 266-5024

Email: ekim@northwell.edu

Hamangi Patel

Director, Research Compliance

Office of Research Compliance

Northwell Health

Phone: (516) 266-5026

Email: hpatel17@northwell.edu

25