University of California
2019 Ethics, Compliance and Audit Symposium
REACHING NEW HEIGHTS

Research Privacy
Trends & Challenges in Clinical Research

Mary Alexander, CHPC, CHRC, CIP, *Research Compliance Officer, UC Irvine Health*

C. Brandi Hannagan, JD, CHC, *Senior Regulatory Specialist, UC Davis Health*

UNIVERSITY OF CALIFORNIA Ethics, Compliance & Audit Symposium
REACHING NEW HEIGHTS

Privacy Principles

Privacy

- Human-centric
- Control over extent, timing, and circumstances of sharing oneself
- Right to be free and protected from unauthorized and/or unreasonable intrusion into private life

Confidentiality

- Data-centric
- Treatment of information that an individual has disclosed in a relationship of trust
- Expectation that information will not be disclosed to other


HIPAA
HITECH
Research Privacy
PHI
CMIA
Big-Data
De-identified
Confidentiality

Regulatory Background

- Common Rule (45 CFR 46) & FDA (21 CFR 50 and 56)
- HIPAA Privacy & Security 45 CFR 164
- The Belmont Report
- Confidentiality of Medical Information Act (CMIA)
- Information Practices Act (IPA)
- National Institutes of Health (NIH) Certificates of Confidentiality (CoC)
- National Institute of Justice (NIJ) Privacy Certificate

A Changing Landscape

- Intersection of responsibility
  - IRBs/Privacy Boards
  - Privacy Offices of Covered Entities
  - Institutional Leadership – Risk Decisions
- Data requests have gotten ahead of:
  - Laws/regulations
    - *Example:* De-identification under "Safe-Harbor"
    - Regulations do not manage research ethics
  - Societal acceptable expectations/actions

Contributing to societal good

Protecting patient rights

Exploring Current Trends

- Single IRB/Privacy Boards (Common Rule update)
- Navigating hybrid entities
- HIPAA Authorization
- Sharing with third parties
- De-identification Defined
- Changing privacy laws
- Ease of and access to rapidly evolving technology
- Big-data requests using clinical data/PHI

Challenges & Risks in Current Trends

- Single IRB
  - Central IRBs issuing waivers (removed from CE interests)
  - Commercial IRBs serving as the Privacy Board
    - How are IRBs defining their role as a Privacy Board?
    - What does this mean for the IRB/Privacy Office relationship?
    - Local context requirement
- Navigating hybrid entities
  - *Example*: Academic Medical Centers and Universities
  - Sharing PHI between covered and non-covered components
  - Sharing research between covered and non-covered components
  - Sharing both in a health system of hybrid entities

Challenges & Risks in Current Trends

- HIPAA Authorization Forms
  - IRB or Privacy Office oversight?
- Sharing with third parties
  - Sponsors or affiliates
  - Example: Transportation services
- De-identification defined
  - HIPAA Regulations
  - OHRP

Challenges & Risks in Current Trends

- Changing privacy laws
  - California Privacy Laws
  - Public Awareness and Expectation of Privacy
  - *Dinerstein v. Google, LLC, and the University of Chicago Medical Center, et al.*
  - GDPR
- Ease of and access to technology
  - Data extraction
  - Patient access to publicly available data
  - Study teams' interest & use of cutting-edge technology

Challenges & Risks in Current Trends

- Big-data requests for clinical data
  - How are IRBs managing?
    - What is "sufficient IRB member experience and expertise" for big-data?
    - Adequacy of traditional protocol templates
    - Public vs. non-public information
      - Research with sensitive data?
  - Identified vs. De-identified
    - Can big-data really be de-identified?
      - "the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify and individual who is the subject of the information." 45 CFR 164.514(b)(2)(ii)
      - *Dinerstein v. Google, LLC, and the University of Chicago Medical Center, et al.*
    - Human Subjects Research (HSR) vs. Non-HSR & Self-Certification

Challenges & Risks in Current Trends

- Big-data Requests for clinical data, cont'd
  - Minimum necessary rule
  - Who are "organizational stewards?"
    - Who decides for identified PHI?
      - Waivers provide the legal protection, but who makes ethical consideration?
    - Who decides for de-identified data?
    - Who can provision data?
      - Who *should* provision data?

Consider: In addition to confidentiality, does the activity support the institutional mission?

Key Building Blocks

- Keeping up with Laws & Trends
- Adequate Policies
- Research Data Oversight
- Robust Training
- Adequate Resources
- Stakeholder Buy-in and Involvement
- Align w/ Institutional Mission, Vision, and Values
- Cultivate Strong Relationships with Key Players
- Gap Analysis

Focused Building Blocks

Keeping up with Laws & Trends

- Local/institutional subject-matter workgroups
- National professional organizations
- List serves
- Local monitoring of trends

Adequate Policies

- Flexible enough to keep up with uncertainty but have guardrails
- Broad enough to keep up with rapid change
- Empower workforce members and support their work
- Develop a plan to ensure review of policies for updates

Focused Building Blocks

Research Data Oversight

- Data stewards
  - Approval of big- or de-identified data requests
  - Data Governance Board
- Access to and Storage of
- Sharing with third parties
  - Collaborative research
  - Industry

Robust Training

- Ensure employee awareness of policies and procedures, including updates
- Ongoing training
- Routine updates to training material
- Consider newsletters or other forms of outreach

Focused Building Blocks

Adequate Resources

- Resources to obtain & store research data
  - Law & institutional policy
- Resources are necessary to ensure compliance
- Resources must be:
  - Available
  - Advertised
  - Accessible

Stakeholder Buy-in and Involvement

- Ensure the right stakeholders are at the table
  - Contracting Departments
  - IRB
  - IT Security
  - Data Analytics
  - Compliance
  - Clinical Department Representatives

Focused Building Blocks

Align w/ Institutional Mission, Vision, and Values

- Regulatory approval does not infer institutional approval
- Consider guidelines to ensure that research aligns with the mission, vision, and values of the institution
  - *"Does the research aim to advance individual and population health?"*

Cultivate Strong Relationships with Key Players

- Privacy SME on the IRB & other data use committees
- IT Security: available tech & risks
- Clinical Departments: workflows, functionality needs, and trends
- Compliance: big picture regulatory risks
- Contracting Departments: 3rd party request
- IRB: trends, guardrails on design & implementation
- Data extraction teams: oversight challenges creating uncertainty

Focused Building Blocks

Gap Analysis

- Identify scope of assessment (e.g. clinical research)
- Take institutional inventory
- Process mapping
- Conduct gap analysis
- Close the gaps

Sample Process Mapping Tool

Clinical Research Process	Industry Standard/Current Practice	Regulatory Implication	Department Responsible for Oversight	Gap Analysis
Development of Protocol	• Protocol includes privacy protection measures and confidentiality maintenance	• Safeguarding	Clinical Research Operations	
Submission and Review	• IRB review of privacy protection measures and confidentiality maintenance review	• Adequate provisions to protect the privacy/ maintain the confidentiality • Risks minimized • Risks reasonable in relation to benefit	IRB/Privacy Board	
	• IRB Informed Consent review	• Description of confidentiality maintenance	IRB/Privacy Board	
	• HIPAA Authorization/Waiver requirements (Privacy Board)	• Permission to Use and/or Disclose	IRB/Privacy Board	Sample Analysis: Privacy Office inclusion in oversight
	• Review Preparatory to Research and Decedent Research	• Permission to Use and/or Disclose	Compliance and Privacy Office	
Activation	• Data Transfer and Use Agreements (DTUAs)	• Safeguarding • Breach and Reporting	Sponsored Projects Administration	
	• Clinical Trial Agreements (CTAs)	• Safeguarding • Breach and Reporting	Sponsored Projects Administration	
	• Materials Transfer Agreements (MTAs)	• Safeguarding • Breach and Reporting	Applied Innovation	

Clinical Research Process	Industry Standard/Current Practice	Regulatory Implication	Department Responsible for Oversight	Gap Analysis
Conduct	• Recruitment of Research Subjects	• Permission to Use and/or Disclose	Clinical Research Operations	
	• Obtaining consent and HIPAA Authorization	• Permission to Use and/or Disclose	Clinical Research Operations	
	• E-Consent	• Permission to Use and/or Disclose • Safeguarding	Clinical Research Operations Information Security	
	• Access provisioning for researchers and monitors	• Safeguarding	Information Services	
	• Requesting reports with PHI	• Permission to Use and/or Disclose	Data Analytics and Informatics	
	• Storing PHI (electronic systems such as CTMS, REDCap)	• Safeguarding	Data Analytics and Informatics Information Security	
	• Disclosing PHI to sponsors (Case Report Forms) or collaborators	• Permission to Use and/or Disclose • Safeguarding	Clinical Research Operations Information Security	

Clinical Research Process	Industry Standard/Current Practice	Regulatory Implication	Department Responsible for Oversight	Gap Analysis
Oversight	• Breach investigation and reporting	• Review of unanticipated problems and/or serious/continuing noncompliance • Breach and reporting to participants OHRP, FDA, OCR, CDPH	IRB/Privacy Board Compliance and Privacy Office	
Data Analysis and Publication	• De-identification of data	• Safeguarding	Clinical Research Operations	
Closeout and Record Retention	• Access termination	• Safeguarding	Information Services	
	• Record retention	• Covered Entity Organizational Requirements • IRB Records	Medical Records Clinical Research Operations	
Future Research	• Registries/Repositories/Stored data	• Compound authorizations • Future Research consent requirements	Data Analytics and Informatics IRB/Privacy Board	

Open Discussion