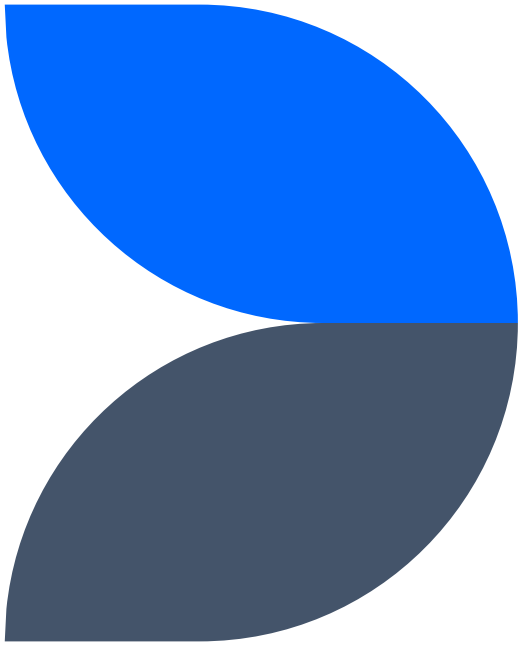
Investigator Seminar Series – Privacy and Confidentiality Requirements in Human Subjects Research - The Common Rule and Beyond

Heather Bridge, OHSRP

Primary goals of this presentation

To help investigators understand:

- The regulatory landscape of Privacy regulations that impact NIH research
- What is expected of investigators
- Who they can turn to for help



Agenda

Baseline Expectations – A refresher on the Common Rule and Policy 107

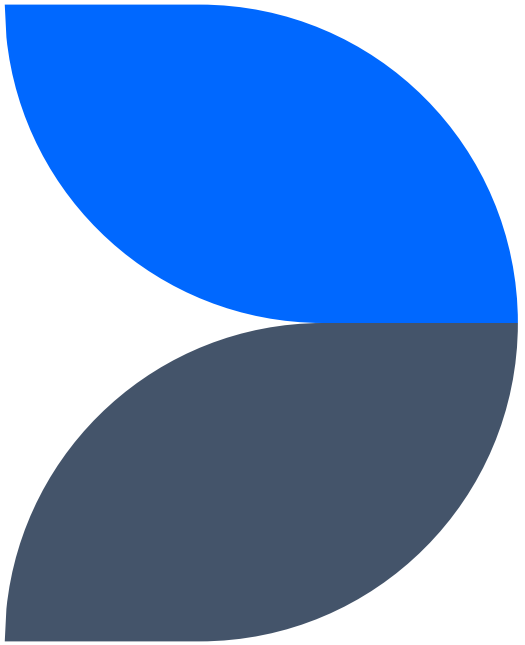
Additional Protections – Privacy Act and Certificates of Confidentiality (COCs)

Outside Requirements – How to manage HIPAA, EU GDPR and similar foreign privacy requirements

Introduction

Protecting privacy and confidentiality in research is an ethical imperative that goes beyond regulatory requirements. Respecting privacy of participants and protecting the confidentiality of their data is essential to engender their **trust** in researchers and the research process, and to facilitate the gathering of **accurate** research data.

Baseline expectations - What we follow in the HRPP



Common Rule (45 CFR 46)- Key Definitions

Private information *includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record).*

Identifiable private information *is private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.*

Back to Basics – Common Rule (CR) Requirements

The criteria for approval at 45 CFR 46.111(a)(7) requires, "*adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.*"

The regulation also requires, "*The Secretary of HHS will, after consultation with the Office of Management and Budget's privacy office and other Federal departments and agencies that have adopted this policy, issue guidance to assist IRBs in assessing what provisions are adequate to protect the privacy of subjects and to maintain the confidentiality of data.*"

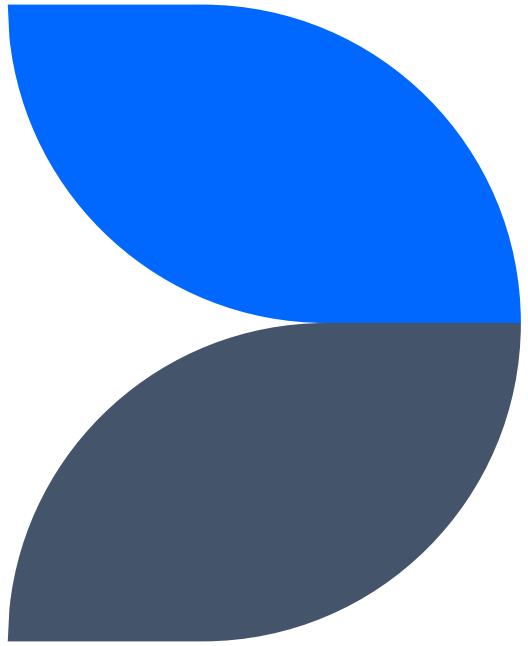
Back to Basics – NIH Policy 3014-107 Privacy and Confidentiality Requirements

Per Policy 107, the IRB requires Principal Investigators to identify in the protocol and consent(s), the procedures they will undertake to protect the confidentiality of participant data. This is required for research conducted at an NIH site, or if the research data will be entered into an NIH Privacy Act system

Policy 107 reminds us that the NIH as a federal agency is also subject to additional regulations and policy to protect the privacy of its participants and the confidentiality of their data, namely:

- The Privacy Act of 1974, and
- The terms of the Certificate of Confidentiality (CoC) issued to the NIH Intramural Research Program (IRP)

Additional Protections -What we follow at the NIH



Privacy Act of 1974 (Privacy Act)- Key Definitions

- ***Individual*** *means* ***a living person who is a citizen of the United States or an alien lawfully admitted for permanent residence****. It does not include persons such as sole proprietorships, partnerships, or corporations. A business firm which is identified by the name of one or more persons is not an individual within the meaning of this part.*
- ***Record*** *means any item, collection, or grouping of information about an individual that is maintained by the Department, including but not limited to the individual's education, financial transactions,* ***medical history****, and criminal or employment history and* ***that contains his name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.*** *When used in this part, record means only a record which is in a system of records.*

Privacy Act – Policy Term – *Personally Identifiable Information*

Our use of the term *Personally Identifiable Information* is aligned with the purpose of the Privacy Act of 1974:

Personally Identifiable Information (PII) *– Information about an individual maintained by an agency, including, but not limited to, education, financial transactions,* ***medical history****, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. (Policy 3014-107 Privacy and Confidentiality)*

Additional Protections – Privacy Act (5 USC 552a implemented at HHS at 45 part 5b)

The Privacy Act is a federal law which establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of **personally identifiable information** about individuals that is maintained in systems of records that are held by federal agencies such as the NIH.

Who to contact for more information about the PA, contact your IC Privacy Coordinator

Additional Protections – Privacy Act Requirements

Policy 107 reminds us that the Privacy Act (PA, The Act) prohibits disclosure of personally identifiable records without the written consent of the individual(s) to whom the records pertain

The PA includes procedures for:

1) Protecting records that can be retrieved by personal identifiers such as a name, social security number, or other identifying number or symbol
2) Individuals to access their identifiable records and to request correction(s) of these records.

Lastly, The Act specifies permissible uses and disclosures of such records

Certificates of Confidentiality (CoCs)- Key Definition – *Identifiable, Sensitive Information*

"Identifiable, sensitive information (ISI)* *means information about an individual that is gathered or used during the course of biomedical, behavioral, clinical, or other research, where the following may occur:*

- *An individual is identified; or*
- *For which there is* ***at least a very small risk****, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual."*

*Types of ISI include: All information (data), biospecimens and documents that were collected, created or compiled for the purposes of the research, including copies of this information

Regulatory Information – CoCs (21 Century Cures Act implemented under Public Health Service Act)

- Certificates of Confidentiality (CoCs) protect “Identifiable, Sensitive Information” (ISI) collected on federally funded human subjects research
- Current CoCs are required by the 21st Century Cures Act, and
- Are issued by the Secretary HHS (via NIH) under the authority of the Public Health Service Act:
  - Effective for research commenced or ongoing on or after 12/13/2016
- Are implemented by NIH via the Guide Notice NOT-OD-17-109

Additional Protections – The Purpose of CoCs

Generally, Certificates of Confidentiality (Certificates, CoCs) protect the privacy of research participants by prohibiting disclosure of **identifiable, sensitive** research **information** to anyone not connected to the research except when the participant consents or in a few specific situations discussed later

Specifically, CoCs **protect against disclosure** of Identifiable, Sensitive Information (ISI) **in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding***

* i.e., legal proceedings

Additional Protections – About CoCs

The CoC protects ISI “in perpetuity” including by

- Recipients of ISI (e.g., sponsors, collaborators, or manufacturers)

CoCs are issued “automatically”* for federally funded biomedical, behavioral, clinical, or other human subjects research that collects or uses (receives) ISI (covered information)

- NIH has discretion whether to cover non-federally funded research and whether to issue Certificates

*NIH Policy on Issuance of Certificates of Confidentiality

What Types of Research are covered under a COC?

- **Human subjects research** as defined in 45 CFR 46, including exempt research
    - Except for exempt research involving de-identified information when there is no access to the code key, or when information is collected without identifiers
- Research involving the **collection or use of biospecimens that are identifiable** or **for which there is at least a very small risk that some combination** of the biospecimen, a request for the biospecimen, and other available data sources could be used to deduce the identity of an individual

What Types of Research are Covered under a CoC? – Continued

- Research that involves **the generation of individual level, human genomic data from biospecimens**, or the use of such data, **regardless of whether human subjects can be identified**, or the identity of the human subjects can readily be ascertained
- Any other **research that involves information about an individual for which there is at least a very small risk, as determined by current scientific practices or statistical methods,** that some combination of the information, a request for the information, and other available data **could be used to deduce the identity of an individual**

What is excepted from coverage under a CoC?

CoCs protect against disclosure of ISI in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding, unless:

- Explicit consent is given (by the subject of the ISI) for release of information
- Is revealed by the subject of the ISI

However, disclosure is permitted when:

- **Required by Federal, State, or local laws** (e.g., required reporting of communicable diseases to State/local health departments).
- So long as it **does not** involve disclosure in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding

What is else is excepted from coverage under a CoC?

- **Necessary for medical treatment** and **consent is obtained** from the individual
- It **is used for other scientific research** so long as **that research is in compliance with applicable Federal regulations** for the protection of human subjects
- Once Federal funding ends any new information collected *is not* protected (more applicable to NIH grantees/contractees, **not** the IRP)

Implications for Investigators of Coverage under a CoC?

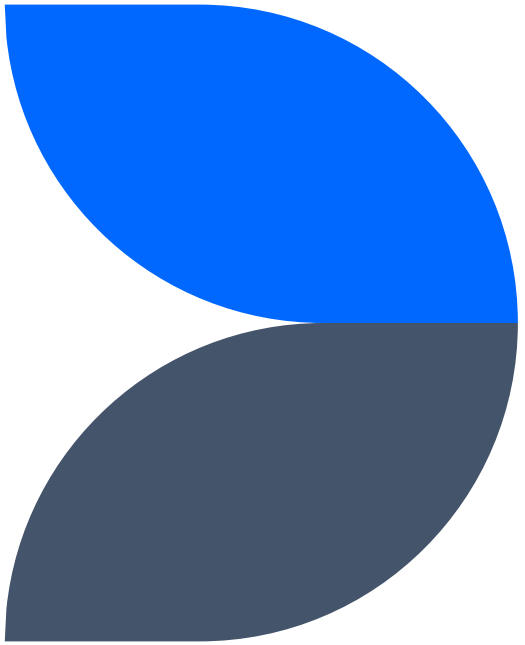
- ISI encompasses a broader set of information than other privacy regs (e.g., CR: Identifiable private information/biospecimens or HIPAA: private health information)
- CoCs permit sensitive research to proceed (e.g., stigma such as addiction or mental health, or sensitive groups like Sexual Gender Minorities)
- Informed consents should reveal the protections conveyed, and limitations of, CoCs to participants (NIH consent templates already include required language about CoCs)
- Secondary research with ISI: Any recipients of ISI or copies of ISI, must comply with the terms of the CoC (at NIH, we developed required tech transfer clauses to convey these requirements)

CoC Resources

- CoC webpage: https://grants.nih.gov/policy/humansubjects/coc/information-protected-coc.htm
- Guide Notice: https://grants.nih.gov/grants/guide/notice-files/NOT-OD-17-109.html
- Section 301 of the Public Health Service Act (42 U.S.C. 241)
- NIH Policy on Issuance of Certificates of Confidentiality
- See Policy 107 Privacy and Confidentiality for DDIR Desk to Desk Memo regarding IRP implementation of CoCs (10/13/2017)

Who can help? Heather Bridge OHSRP (heather.bridge@nih.gov)

Outside Requirements - What others follow that might impact your research



Health Information Portability and Accountability Act (HIPAA, Privacy Rule)– Key Definitions

"**Individually identifiable health information**" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition
- the provision of health care to the individual
- the past, present, or future payment for the provision of health care to the individual

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

HIPAA - Key Definitions - Continued

"Protected Health Information (PHI) all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information."

"Covered Entities" are individuals and organizations, including healthcare providers, health plans, healthcare clearinghouses, or business associates who electronically transmit **individually identifiable health information** in connection with certain transactions, such as claims or eligibility inquiries, referral authorizations, data analysis, utilization review, billing, etc."

The Privacy Rule (45 CFR parts 160 and 164)

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996
- The final regulation, the Privacy Rule, was published by HHS December 28, 2000
- The Privacy Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions ("covered entities")
- **NIH is not a Covered Entity and is not subject to the Privacy Rule**

The Privacy Rule and Human Subjects Research

- The Privacy Rule specifies an individuals' right to understand and control how their health information is used.
- Individuals must provide signed authorization before a Covered Entity can access, use or disclose their PHI, including for research purposes
- However, under certain circumstances, a Covered entity may use or disclose PHI without a signed authorization, so long as a **Privacy Board** approves a **HIPAA waiver**
- Some Covered Entities use the IRB to serve as the Privacy Board or form a separate convened Privacy Board.
- **NIH is not a Covered Entity and is not subject to the Privacy Rule, therefore the NIH IRB will not serve as a Privacy Board**

Collaborating Researchers and The Privacy Rule

- Researchers working at a Covered Entity are subject to the Privacy Rule when conducting Human Subjects Research or providing clinical care
- If these researchers wish to share their data with an outside collaborator, they will typically seek authorization for sharing data from their research participants, or seek a HIPAA waiver or alteration from their Privacy Board
- The use or disclosure of information in violation of HIPAA can result in substantial penalties to the covered entity.

Implications for NIH Investigators when collaborating with Covered Entities

- In order to send PHI research data from a Covered Entity (e.g., US universities and hospitals), these entities (or their investigators) may request that the recipient sign a Business Associate Agreement (BAA) asking them to abide by the terms of the Privacy Rule.
- Because the NIH is not a Covered Entity and is not subject to the Privacy Rule, NIH Principal Investigators **should not agree to any HIPAA terms or sign or execute a BAA** with collaborating institutions. (See Policy 107)
- **Who can help if you are asked to sign a BAA?** Reach out to NIH Office of General Counsel (OGC) for advice if asked to sign a Business Associate Agreement.

Implications when the NIH IRB is the Reviewing IRB for Covered Entities

- **NIH IRB may not act as a Privacy Board for relying institutions** Because the NIH is not a Covered Entity and is not subject to the Privacy Rule. When NIH is the Reviewing IRB, it may review protocols for institutions that are subject to HIPAA, but relying institutions must still serve as their own Privacy Boards according to the terms of our reliance agreements
- NIH investigators should not imply or commit the NIH to serve in the capacity of a Privacy Board when establishing multisite research and when the NIH IRB will be the Reviewing IRB
- **Who can help?** Reach out to IRBO for assistance with reliance agreements

HIPAA Resources

- HHS Clinical Research and the HIPAA Privacy Rule (February 2004) NIH Publication #04-5495
- HHS HIPAA webpage Research (HIPAA as it relates to research) (Revised December 2017)
- HHS Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule Health Services Research and the HIPAA Privacy Rule (NIH Publication #03-5388)
- HHS Research Repositories, Databases, and the HIPAA Privacy Rule (January 2004) NIH Publication #04-5489 In accordance

European Union (EU) General Data Protection Regulation (GDPR) – Key Definitions

*"**identifiable natural person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

"**personal data** means any information relating to an identified or identifiable natural person ('**data subject**')."

"**pseudoanymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

EU GDPR – Key Definitions – Continued

“**data subject** individual whose personal data is being processed.”

“**controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”

“processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”

Outside Requirements – EU GDPR (EU 2016/679)

- The EU GDPR is one of the strongest privacy and data security laws in effect
- It was adopted in the European Economic Area (EEA) in 2016 and became effective on May 26, 2018
- The EU GDPR governs how the personal data of individuals (data subjects) in the EU may be collected, processed (used) and transferred
- Additional protections for sensitive data (e.g., race, ethnic origin, sex/sexual orientation, health data, biometric data and genetic data)
- EU GDPR specifies:
  - Rights of individuals (subjects) to control and access their data
  - Obligations of data controllers and processors
  - Methods of compliance and sanctions for those who are non-compliant

Outside Requirements – EU GDPR – Obligations of Data Controllers and Processors

- Data controllers for our purposes are EEA based Pharma Co./Sponsors
- Data processors for our purposes are NIH investigators

The EU GDPR specifies the obligations of data controllers and/or processors:

- To provide and implement appropriate data security measures
- To provide notification of data breaches
- Appoint a “Data Protection Officer”

Outside Requirements – EU GDPR – Implications for Human Subjects Research

The EU GDPR:

- Is problematic for retention of certain research data which must be retained by other research regulations for specified timeframes e.g., for purposes of validity and/or in support of marketing applications such as for the FDA or EMA
- Can inhibit research collaborations outside EU Member States/EEA
- Transfer of data: explicit consent for collection and use of data **is likely not** sufficient to facilitate transfer of data from the EEA because each Member State can interpret the EU GDPR differently/more conservatively
- Similarly, the US government **cannot** agree to key contract clauses of the EU GDPR to needed to transfer data to the US

Outside Requirements – EU GDPR – Transfer of Data outside the EU

Other requirements for transfer of data outside the EEA/EU:

- The European Commission assesses the level of protection by any given non-EU country – **It has not deemed US Privacy regulations to be equivalent to the EU GDPR protections**
- Pseudo-anonymized data (i.e., coded data) is subject to EU GDPR transfer requirements
- Only fully anonymized data is not subject to the EU GDPR

The US government is NOT subject to the EU GDPR

Outside Requirements – EU GDPR – Implications for NIH Investigators

If you are working with a Sponsor located in the EEA, the Sponsor:

- Is the Data Controller
- Views the NIH Investigator as the Data Processor
- Will likely include required EU GDPR information in the master consent

But, the **US government is NOT subject to the EU GDPR**, therefore:

- NIH Investigators **may not** sign anything indicating compliance with the EU GDPR
- **May not** provide advice or guidance related to EU GDPR
- NIH consents **may not** contain any EU GDPR language

Outside Requirements – EU GDPR – So, What Should NIH Investigators Do?

If you are working with a Sponsor and the Sponsor:

- Asks you to sign anything indicating compliance with the EU GDPR – **Contact NIH OGC**
- Provides you a Master consent that contains EU GDPR language – **Contact Heather Bridge (heather.bridge@nih.gov) for assistance**
- Asks you to be the point of contact for EU GDPR purposes, NIH investigators **may not** serve in this capacity- **Contact Heather Bridge**

Outside Requirements – EU GDPR – Data Privacy Notice for EU Sponsors

NIH investigators are permitted to provide a Data Privacy Notification on behalf of the Sponsor to research participants. This notice must be cleared by Heather Bridge (working with OGC). This notice typically informs research participants:

- What type of data will be retained by the Data Controller
- How long the data will be retained (typically for 30 years)
- Who the Data Controller may share their data with (business partners)
- What rights data subjects have regarding their data
- Who to contact to exercise their rights (the Data Protection Officer for the Controller)

- Contact Heather Bridge (heather.bridge@nih.gov) for assistance in developing such a notice

Outside Requirements – EU GDPR – How to Request a Data Privacy Notice (DPN)

- The DPN can be developed in parallel with the IRB submission
- However, first the investigator should submit a copy of the consent form(s) that includes EU GDPR language in it to Heather
- Strip the EU GDPR language from the informed consent before submitting it to the IRB
- Notify the Sponsor, CRO or Coordinating Center that the NIH site consent will vary from the master consent and why
- Heather will work with the Sponsor to finalize the contents of the DPN and clear it with OGC if necessary (we have standard DPN language for some Sponsors already)
- Changes to the DPN must be cleared by Heather

Outside Requirements – Other Privacy Regulations

Ten (10) other countries have new privacy laws, and more are likely coming

Reminder: As employees of a Federal Agency, you **cannot**:

- Agree to abide by foreign regulations
- Sign anything indicating compliance with foreign regulations
- Include information about foreign regulations in NIH consents

- **Contact OGC** for assistance with compliance statements or signing agreements

- **Contact Heather Bridge (**heather.bridge@nih.gov**)** for assistance with DPNs for other countries

Summary

NIH Investigators must comply with the Common Rule, Privacy Act, Certificate of Confidentiality and HRPP Policy requirements

NIH Investigators may not sign agreements/agree to comply with:

- HIPAA or Business Associate Agreements
- Any foreign regulations such as EU GDPR

NIH investigators must seek assistance if asked to comply with HIPAA or foreign privacy regulations

Thank you

Heather Bridge

OHSRP

heather.bridge@nih.gov