Data Access Training

Data Stewardship Training for Access to Identifiable Cancer Data

Revised July 22, 2021

FRED HUTCH
CURES START HERE™

Purpose of this Training

- Explain principles of handling strictly confidential data (Stewardship).
- Describe Protected Health Information (PHI).
- Discuss the Consortium MOU and the roles and responsibilities for individuals accessing and using this data.
- Understanding appropriate research use of MOU governed data.

Stewardship

FRED HUTCH
CURES START HERE™

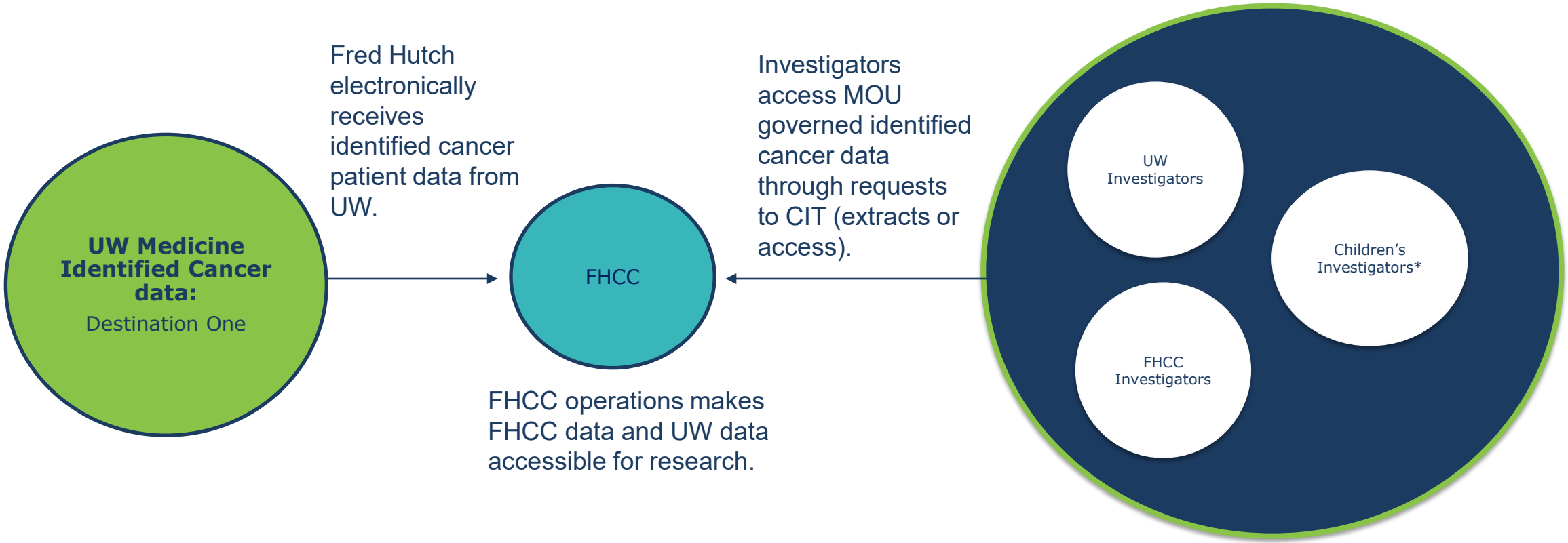
Cancer Consortium Memorandum of Understanding (MOU)

Through various Consortium agreements including a 2021 Memorandum of Understanding (MOU) among UW and Fred Hutch, Fred Hutch electronically receives identified patient data from UW.

This data is distributed by CIT to Consortium researchers through data extracts or ongoing access.

The MOU, along with its security agreement and Business Associate Agreement, describes the terms and conditions under which this data can be accessed and used. This training will help researchers better understand how to use this data.

Stewardship and Where the Data Come From



*FHCC provides requested data under a separate agreement and conduit.

What is identified human data?

Identifiable data in health care and health/medical research either

1. directly identify an individual through one of the 18 HIPAA, **or**

2. enable someone to conclude *on a reasonable basis* the data can be used to identify an individual, including coded health information.

Importance of Good Data Stewardship

- Identified human data stored in Fred Hutch archives and repositories constitute valuable, and represent patient/participant loaned, assets; they must be protected from unauthorized and unsecured access as per regulatory, institutional and ethical requirements.

- Under the Fred Hutch Information Security Policy and Standards, Fred Hutch identified data is classified as Restricted Information (SCI) and should be handled accordingly.

- Individuals who access this data must understand their roles and responsibilities, including the use of safeguards based on the nature of the data, the data's criticality, and the level of risk associated with its improper access and use.

- Approval processes for data access will help ensure safeguards are in place and followed.

Restricted Information

Restricted Information requires special protection. Unauthorized access, disclosure, destruction, or alteration of Restricted information may constitute a violation of law or contractual or ethical obligations. Such violations or breaches could cause serious to catastrophic harm to Fred Hutch or your institution, including severe financial loss, legal liability, public distrust, or harm to reputation. Unauthorized use of Restricted Information could also severely harm the individual about whom the data refers. Examples of such data include:

- Protected Health Information or PHI
- Research Participant information
- Proprietary business information
- Computer passwords/encryption keys

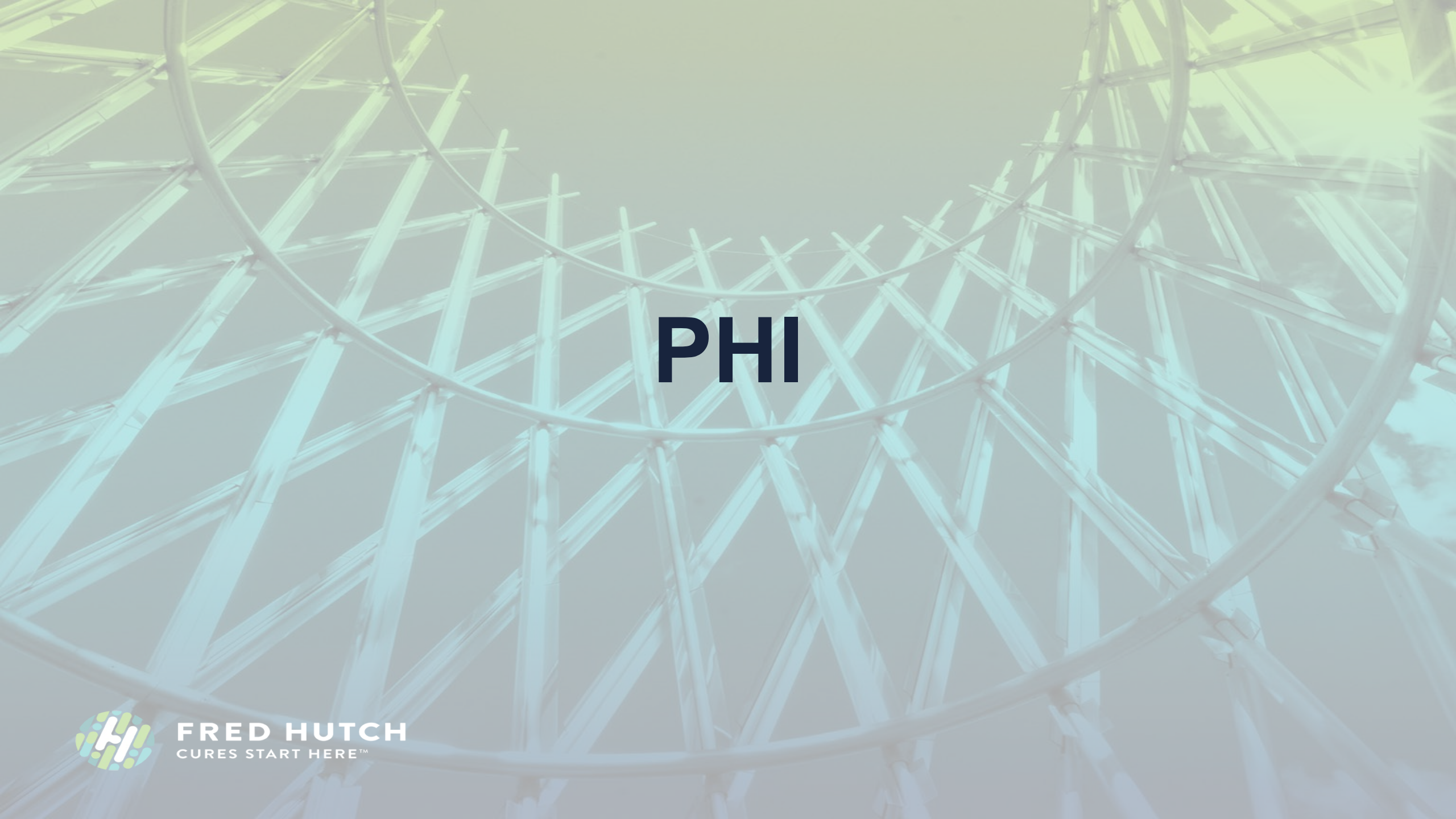
Principles that apply to access/use of Restricted Data

- ❑ Must be handled by Fred Hutch employees and non-employees according to Fred Hutch ISO Policy.
- ❑ Should only be accessed and/or used for an approved purpose.
- ❑ Must be **securely** maintained and transmitted:
  - Password Protected
  - Access controlled
  - Encrypted in transit and rest
  - Audited access and logging
- ❑ Cannot be shared with others not authorized to receive it.
- ❑ Loss or suspected loss should be reported immediately to the Fred Hutch Help Desk at 206.667.5700.

Noncompliance in Handling Confidential Information

- Inappropriate access, use, or disclosure of Restricted information, and loss or theft of unencrypted information, can result in individual or institutional fines and penalties, personal liability, and disciplinary action up to and including termination.

PHI



FRED HUTCH
CURES START HERE™

PROTECTED HEALTH INFORMATION (“PHI”)

- Protected Health Information (“PHI”) is individually identifiable health information generated by a Covered Entity. Examples typically include Medical Records, clinical billing or health insurance information.

- A Covered Entity (i.e., physician, hospitals, health insurance company) can provide under an agreement PHI to a non-covered entity, such as FH. FH holds and manages some PHI in various areas of the institution.

- Generally, individuals must specifically **authorize** others to access their PHI for its use in research.

- Misuse/Unauthorized use of PHI in research may require notification to the Institution Review Board (IRB), which has discretionary authority to pause or cease a research protocol.

PROTECTED HEALTH INFORMATION ("PHI")

Levels of PHI

Use, access, and disclosure of PHI is highly regulated by HIPAA. In most states (including Washington state), the use, access and disclosure of "individually identifiable information" relating to health care is also regulated in a manner similar to federal regulation under HIPAA. The regulatory rigor is determined by the nature of the PHI:

- *De-identified Information– Least Regulated*
- *Limited PHI (aka "Limited Data Set") - Specific Use Regulation*
- *Identified/Full PHI and Restricted PHI – Most Highly Regulated*

De-Identified Data

Least regulated, easiest to access – De-identified data does not contain any of the 18 HIPAA identifiers.(e.g., names, social security numbers, medical record numbers, DOB) or has been determined to be de-identified by an expert statistical analysis.

- Identifiers may be masked/coded for use in data reviews, reports, and exempt research.
- Data results or extracts may be aggregated into cells of 10 or more.
- Access to de-identified information does not require patient authorization.

The 18 HIPAA specified identifiers

The following identifiers apply to the patient, the patient's family, household and employer:

- name, location, dates, telephone numbers, fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan numbers, account numbers, license numbers, vehicle ID's, device ID's, URLs, IP addresses, biometric ID's (finger and voice prints), full face images, and any other unique identifying number or code.

Allowable Identifiers which may Facilitate Re-Identification

The following identifiers may provide a strong basis for re-identification, though they are not be one of the 18 HIPAA identifiers.

- age
- gender
- race/ethnicity
- allowable form of geolocation
- language

Access a Limited Data Set (LDS)

- A Limited Data Set includes a subset of HIPAA Identifiers: dates (admission, discharge, service, dates of birth and dates of death), city, state, zip codes and ages in years, months or days or hours. Excluded are names, street address, remainder of 18 HIPAA Identifiers.
- A limited data set is still PHI under HIPAA.
- Patient authorization is not required for release of or access to a LDS for research when the LDS is accompanied by a Data Use Agreement (“DUA”) which satisfies HIPAA requirements.
- Loss or suspected loss must be immediately reported to the Fred Hutch Help Desk at 206.667.5700.

Access to Identified/Full PHI

- Identified/Full PHI is data that includes individually identifiable information about an individual (i.e., patient).
- Use and disclosure of full PHI are subject to federal and state requirements.
- Identified PHI should not contain information such as social security numbers, bank account numbers, passwords, etc.
- Loss or suspected loss must be immediately reported to the Fred Hutch Help Desk at 206.667.5700.

PHI & Research

FRED HUTCH
CURES START HERE™

Research Use of Full PHI

- Washington State imposes more stringent requirements than federal HIPAA laws in certain important aspects when allowing access to identified information for research. Examples include:
  - Washington state law requires an “authorization” for access to individually identifiable health information following death.
  - Washington state requires a confidentiality pledge from researchers in order to obtain access to identified information when patient does not authorize access.
- Access to Protected Health Information must be controlled and regulated to satisfy all regulatory requirements.
- Use requires explicit authorization by individual to whom the PHI relates. Authorization must meet HIPAA and state law requirements.

Access to Full PHI for Research without Authorization

- When Researchers require access to identified PHI for research purposes and don't have the ability to obtain the express authorization from participants, researchers seek approval a Waiver of Authorization ("waiver"), allowing access to data without patient signature.
- Researchers seek waiver approval from the Institutional Review Board (IRB), an oversight body charged by law to protect research participants from many forms of harm.
- Waivers are typically sought for viewing PHI for reviews preparatory to research consistent with HIPAA and Washington State law (RCW 70.02.050).
- Plans to protect the identifiers during the research use and to destroy the identifiers when no longer needed should be considered carefully and followed.

Security Policy, Minimum Necessary and Accountings

Once allowed access to PHI, the researcher must adhere to three overarching federal requirements (“principles”):

- Adherence to the institutional/FH Information Security Policy and Standards.
- “Minimum Necessary Use” - the researcher must make efforts to request, disclose or use only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.
- “Accounting” - if PHI is accessed via an IRB approved waiver of HIPAA authorization, access must be documented for each individual (create an accounting of disclosures). Individuals have a right to receive an accounting of who has seen their PHI over the last 6 years.

Contacting Patients for Recruitment

Can consortium investigators contact individuals for recruitment?

- IRB approval required in all situations.

Research Use of Identified Data: Unauthorized Disclosure

Can a researcher use or share identified information for reasons outside the study protocol? No. The disclosure or use of identified data violates scope of the HIPAA Authorization or the IRB-approved waiver HIPAA Authorization. This is unauthorized use.

What happens if identifiable research data somehow becomes open-facing to the public via the internet? This represents an unauthorized and unsecured disclosure of PHI. Disclosure/use of unauthorized, unsecured PHI may require notification to the IRB and the HIPAA Covered Entity that is the source of the PHI. Call ISO Security/Fred Hutch Help Desk at 206.667.5700 or Fred Hutch Office of the General Counsel at 206-667-4320.

What happens if identifiable research data on a non-encrypted smartphone is lost? Because the phone is not encrypted (password protection is not sufficient), this is also an unauthorized, unsecured disclosure.

Reporting and Non-Retaliation

No individual who in good faith reports a known or suspected conduct, incident or practice that may violate 1) institutional compliance and/or ethical conduct policies and/or 2) related state and federal laws and regulations will be discharged, demoted, suspended, threatened, harassed, discriminated against or otherwise retaliated against for making such report. Workforce members who conduct retaliatory behavior may be disciplined.

Suspected non-compliance of identified data held or managed at FH should be reported to ISO Security Fred/Hutch Help Desk at 206.667.5700 or Fred Hutch Office of the General Counsel at 206-667-4320.

THANK YOU

FRED HUTCH
CURES START HERE™

fredhutch.org