Data Access Training

Data Stewardship Training for Collaborators

Access to Identifiable Cancer Data at Hutch Data Commonwealth

Revised August 2019
Welcome!

You are provided this training because you have been or will be granted access to identifiable patient information as part the collaboration with Fred Hutch (FH).

This training is to make sure individuals who access this data 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.

This training, along with others, such as Human Subjects Training, are safeguards for you, your employer and FH.
Purpose of this Training

Stewardship

What is Identified Human Data

Data used in Research

Security and Handling of Identified Human Data

Reporting Data Misuse and Remediation
Why Stewardship Matters
Why We Care About Stewardship

Strong stewardship maintains our legal, regulatory and ethical responsibilities as an institution.

Strong stewardship represents our commitment to current and future patients, who are the primary owners of this information. Without such stewardship, FH, its collaborators and affiliates break the trust and social contract with patients and research subjects whose information we use.

FH also has strong and fundamental relationships with care hospitals and doctors, such as at UW and SCCA. These care providers are the primary stewards and secondary owners of the information. Data stewardship is our commitment to them, as well. Maintaining the trust of these providers ensures FH has the information resources needed to continue its mission.
Why You Care About Stewardship

Because you collaborate with us and receive our data, your organization and you as a team member accept our ethical and legal responsibilities associated with medical research.

Identified data is regulated on a federal and state level and subject to FH institutional policies. Relevant privacy and security regulations and requirements, as well as federal and state enforcement rules, begin when the information is generated and flow down to you and your organization.

Accidental or intentional unauthorized exposure/use within your organization or between your organization and an outside entity may result in reputational harm to your organization and informational harm to the patients who own the data.
Fred Hutch electronically receives identified cancer patient data from UW and SCCA.

HDC shared data with internal, consortium and external researchers and partners.

FHCRC/Hutch Data Commonwealth (HDC) Operations makes data accessible for research.

UW Medicine and SCCA Identified Cancer data:
HER, Lab, other eSources, manual extraction.
What is Identified Human Data?
What is Identified Human Data?

Identifiable data in health care and health/medical research either:

1. directly identify an individual, such as through one of the 18 HIPAA* identifiers (next slide) and/or

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

* Health Information Portability and Accountability Act
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
De-Identified Human Data

De-Identified data bears very small risk that a patient can be re-identified. This is done by removal of the 18 HIPAA identifiers and/or coding and statistical methods to block re-identification.

Regardless of whether the data you see is identified or de-identified, you should not have Social Security Number, Driver License number or other financial account numbers associated with the shared data. If so, please report to your supervisor or FH immediately.
Using Identified Data Under Research
Using Identified Data Under Research

- Research which uses identified human data is considered Human Subjects research. As a result, use of identified data is subject not only to federal HIPAA laws, but also federal Human Subject Protection laws.

- Human Subject Protection law requires a researcher to submit a research plan (a protocol) to the FH Institutional Review Board (IRB) for approval. The IRB is a committee which reviews all protocols involving humans or human data to ensure research methods sufficiently protect human subjects from all forms of harm. IRB Committee maintains oversight of the research work for the life of the protocol.
Using Identified Data Under Research (Cont’d)

- Identified data may only be used with authorization. Generally, identified data can only be used for research after the patient provides authorization for his/her data. If the patient does not authorize use, the IRB can authorize use in the patient’s stead.
Once allowed access to identified data, all who work with the data must adhere to the following 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.
Collaboration Not Conducted Under Research

If you are receiving identified data as a collaborator for reasons other than research, you will be receiving this data under a data use agreement. Good data stewardship requires you to understand the data use agreement which allows the sharing of data within the collaboration.

Adherence to FH Information Security Policy and Standards.

Using identified data will not fall under Human Subjects Protection, but likely under full HIPAA requirements. Relevant privacy and security regulations and requirements, as well federal and state enforcement rules, flow down to you and your organization.
Security and Handling of Identified Human Data
Security and Handling of Identified Human Data

Fred Hutch Information Security Policy

- Identifiable data is considered Strictly Confidential Information under the FH Information Classification Standard, part of the FH Information Security Policy.

- This standard flows down to FH collaborators and is summarized in the next two slides.
FH Strictly Confidential Information Standard

Strictly Confidential Information requires special protection. Unauthorized access, disclosure, destruction, or alteration of Strictly Confidential information may constitute a violation of law or contractual or ethical obligations. Such violations or breaches could cause serious to catastrophic harm to FH or your institution, including severe financial loss, legal liability, public distrust, or harm to reputation. Unauthorized use of Strictly Confidential 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
Strictly Confidential Information:

- 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 (within 24 hours of awareness) to Fred Hutch.
Handling FH Strictly Confidential Information

Access to Strictly Confidential Information has the following responsibilities:

To not re-disclose any Strictly Confidential Information to any person or entity not authorized to receive such information.

To not remove Strictly Confidential Information from Fred Hutch/Collaborator managed environment unless authorized to do so.

To report to my superior or FH if I have reason to believe the confidentiality or security of my password or access to information has been compromised.
Patterns of Security Incidents and Data Breaches
(From Verizon, 2019 Data Breach and Investigations Report)

Healthcare stands out due to the majority of breaches being associated with internal actors. Denial of Service attacks are infrequent, but availability issues arise in the form of ransomware.

Miscellaneous Errors, Privilege Misuse and Web Applications represent 81% of incidents.

Threat actors by order: Internal (59%), External (42%), Partner (4%) and Multiple parties (3%) (breaches)
Reporting Misuse of Identified Human Information
Reporting Misuse of Identified Human Information

Regardless if you are an employee or non-employee affiliate.

Regardless if the data is shared for research or non-research purposes.

Intentional and unintentional misuse of the data - including unauthorized or unauthorized and unsecured use/disclosure - needs to be reported to FH within 24 hours of first awareness.

Contact your supervisor call HDC Security/Compliance at (mike and susan number) or Fred Hutch Office of the General Counsel at 206-667-1224
Notification of Misuse of Identified Human Information

Unauthorized, or unauthorized and unsecured use of identifiable human data by FH collaborators will likely result in notification to the care providers or hospitals which provide FH with the information.

Unsecured exposure of data owned by a large number of unique patient individuals may result in a HIPAA reportable event with civil penalties.

If the collaboration is under research use, notification to the FH Institutional Review Board (IRB) is also required.

The Institutional Review Board (IRB) has discretionary power to suspend or terminate work on a collaboration if that collaboration is considered a research project.
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 patient-signed authorization or the IRB approval. This is unauthorized use.

What happens if identifiable research data somehow become open-facing to the public, such as via the internet? This represents an unauthorized and unsecured disclosure. Notification to FH is required. Disclosure/use of unauthorized, unsecured identified data may also require notification to the IRB and the hospital or provider which is the source of the data.

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 and notification is required.
Summing It Up: Managing Shared Risk

**KEY POINTS:**

> Ethical
> Law
> Company Policy
> Protect Rights
> Duty of Care
> Best Practice
Summing It Up: Managing Shared Risk

Successful Collaboration

- Training
- Clear Lines of Authority
- Security and Access Management
- Clear Agreements and Ongoing Communication
Any questions about this training session can be directed to Susan Glick at sgglick@fredhutch.org.
THANK YOU