Privacy and Research

Compliance: 734-8808
http://www.ucdmc.ucdavis.edu/compliance/
Agenda

– De-identified data and limited sets
– Authorization of data collection for research preparation
– Permission to use personal health information (PHI) for research
– Break the Glass security function and research subject’s medical record access
– Minimize reputational and legal exposure associated with loss or misuse of identifiable private information
– Continuous Quality Improvement (CQI) for using chart review to identify potential research subjects
– Promote trust and increase participation in research

• Basic Principles
  – Privacy in Research
Basic Principles
Basic Privacy Requirements in Human Subjects in Research (Common Rule)

• If you conduct human subjects research – whether by intervention, interaction or collecting identifiable private information – the following rules apply:
  – You must assure that there are adequate provisions to protect the subject’s privacy and maintain confidentiality of data
  – You must disclose foreseeable risks (e.g., privacy risks) in the informed consent process and form (unless waived)
  – You must disclose the extent, if any, to which confidentiality of records will be maintained (unless waived)

• These requirements apply to all human subjects research, regardless of funding source, performed at UC or by UC researchers
Privacy Laws and Research

• Many laws and regulations support FIPS, for example:
  – Health Insurance Portability and Accountability Act (“HIPAA”)
    • Federal law that applies to health care providers who bill electronically, health plans, and health care clearinghouses – each of these is a “Covered Entity”
    • HIPAA protects the privacy and security of identifiable health information created, received, or maintained by a Covered Entity (“PHI”)
  – California Information Practices Act (“IPA”)
    • State law applies to California government agencies, including the UC
    • IPA protects the privacy and security of an individual’s health information created, received, or maintained by California agencies
  – These and other laws supplement the Common Rule
Defining the “Covered Entity”

UC is a big organization. Some parts are “covered” by HIPAA, some are not. The covered parts are called the “Single Health Care Component.”

<table>
<thead>
<tr>
<th>Single Health Care Component (SHCC)</th>
<th>Non-Covered Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospitals, clinics, and other health facilities that provide health care, and bill Medicare and other health insurers or health plans for that care</td>
<td>Researchers conducting studies that:</td>
</tr>
<tr>
<td></td>
<td>• Do not include a diagnostic or therapeutic intervention performed by the SHCC; and</td>
</tr>
<tr>
<td></td>
<td>• Neither acquire PHI from nor contribute PHI to the SHCC or its providers</td>
</tr>
<tr>
<td>Physicians, physician assistants, nurses, and other health care providers who deliver health care items or services to patients</td>
<td>Researchers collecting data as part of the subject’s voluntary participation in a study and not as a byproduct of a healthcare service event</td>
</tr>
<tr>
<td>Clinical operations of the health professions schools that perform covered functions</td>
<td>Hospital human resources department</td>
</tr>
<tr>
<td>Student health and counseling centers</td>
<td>Vendors that work on behalf of the covered component, but do not use or disclose PHI</td>
</tr>
<tr>
<td>Other entities that engage in covered functions with PHI</td>
<td>Other components that do not engage in covered functions with PHI (and are not otherwise designated as part of the covered component)</td>
</tr>
</tbody>
</table>
HIPAA Applies to Your Research if Any of the Following Is True:

- Any UCDHS medical records are used, e.g.:
  - To identify potential participants
  - To annotate biospecimens collected solely for research purposes
  - To measure outcomes of a research intervention
- The study will generate information for the UCDHS medical record, e.g.:
  - A laboratory test is performed in the UCDHS clinical laboratory purely for research purposes and is not billed to insurance, but the data are reported and maintained in EPIC
  - An office visit is performed only for research purposes and is not billed to insurance, but a record of the visit is maintained in EPIC
  - Research data are placed in the medical record to facilitate care of the patient
- The study involves treatment of any subjects
- Any protocol-required services (or treatment of study-related injuries) provided at UCDHS will be billed to Medicare, Medicaid, or other government or private health plans
Practical Guidance
What do researchers have to do?
Notice

• Rule
  – Every patient and research participant must be told, usually in writing, what information we collect and what we do with it
  – The content of the notice is governed by laws, regulations, and internal policies

• Researcher Responsibilities
  – HIPAA Notice of Privacy Practices – must be given to all research participants receiving health care at UC (i.e., any health care items or services billed to Medicare, private insurance companies or health plans)
    • Hospital and clinic registration staff usually take care of this
  – Informed Consent for Participation in Research – must be signed before enrollment by all individuals who participate in research, unless waived by the Institutional Review Board (“IRB”)

Informed Consent for Participation in Research – must be signed before enrollment by all individuals who participate in research, unless waived by the Institutional Review Board (“IRB”)
Permission

• Rule
  – An individual’s voluntary written permission is required prior to collection, use or disclosure of his or her identifiable private information unless an exception applies
  – The permission must include specific language and in some cases must be documented in a specified format

• Researcher Responsibilities
  – Discuss the study with all participants before enrollment, including what information will be collected and how it will be used
  – Have participants sign the IRB-approved informed consent form and give them a copy
  – If HIPAA applies to the project, have participants sign the standard HIPAA research authorization form (http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/resauth.html), as approved by the IRB, and give them a copy
  – Maintain copies of the signed consent and authorization forms in the research record
HIPAA Authorization Exceptions

• You can use HIPAA-regulated data without written authorization if you have documentation of:
  – A waiver of authorization granted by the IRB or Privacy Board
  – Use of decedents’ information for the research (apply at http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/resdeced.html)
  – Use is permitted “preparatory to research” (apply at http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/resprep.html)
  – A data use agreement signed by the Privacy Officer or designee allowing you to use a “limited data set” that excludes direct identifiers (see http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/limdata.html for guidance)

• De-identified data currently are not regulated by HIPAA (see http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/deident.html for detailed guidance)
Safeguards – Securing Private Information

• Rule
  • Protect against reasonably anticipated threats or hazards to security of identifiable private information created, used or maintained for research

• Researcher Responsibilities
  • Establish Administrative Safeguards
    • Make sure all research staff are trained on privacy obligations (check with the Privacy Office if you’re not sure)

• Establish Physical Safeguards
  • Retain sensitive information in locked buildings/offices/file cabinets
  • Secure any non-encrypted computers or devices under lock and key
  • Shred any documents with sensitive information when no longer needed
Safeguards (cont’d)

– Establish Technical Safeguards
  • If you maintain servers, protect them with appropriate firewalls, patches, and other technical safeguards
    – Research projects involving large sensitive data stores typically will require skilled and experienced IT staff support
  • Encrypt all desktops, laptops, flash drives, mobile devices, and similar electronic storage units if and as possible
    – This is not a direct mandate but where encryption is not utilized, some other safeguard is needed (e.g., the computer is not encrypted but it is always locked in an office that is accessible only by authorized staff with key cards)
  • Carefully store or transfer data that cannot be encrypted (e.g., digital cameras) ... don’t leave unencrypted devices in the car!
  • Use strong passwords and never share passwords
  • Log off of your computer when not in use and at the end of each day

– Report Unauthorized Access, Security Incidents and Breaches
  • If you become of aware that your research data have been compromised, or of any potential breach of identifiable private information, immediately notify abuse@ucdavis.edu or the Compliance Hotline at (877) ETHICS-2
Limitations and Restrictions on Use and Disclosure

• Rule
  – All disclosures of identifiable private information for research without authorization are subject to a “minimum necessary” rule designed to avoid unnecessary privacy intrusion
  – A disclosure includes any release of identifiable private information outside of UCDHS without authorization
  – A disclosure also includes use without authorization of protected health information maintained by the SHCC for research purposes, even if the information never leaves UCDHS

• Researcher Responsibilities
  – Disclose only the minimum amount of identifiable personal information necessary for your project
  – Exceptions:
    • Disclosures to UCDHS or other health care providers for treatment purposes
    • Disclosures of a limited data set under a data use agreement (more later)
    • Disclosures made at the patient’s request, with his or her written authorization
Limitations and Restrictions on Use and Disclosure \( (cont’d) \)

- **Rule**
  - Researchers do not have unfettered access to medical records or other SHCC records that contain HIPAA protected health information

- **Researcher Responsibilities**
  - Understand that your access to medical records as a health care provider does not entitle you to access the same records for research
  - Do not access medical records or other SHCC records that contain HIPAA protected health information for research purposes unless and until you have obtained HIPAA authorization or documented an authorization exception (see next slide for options to identify and recruit potential participants)
De-Identified Protected Health Information

- Once protected health information (PHI) has been de-identified, it is no longer PHI, and the restrictions and requirements of federal and state privacy laws no longer apply. However, if a re-identification code is added to the data, certain privacy and security rules apply to the code.

- There are two methods of de-identification: 1) use of statistical methods proven to render information not individually identifiable, and 2) deletion of 18 specified identifiers.

**Statistical Method**

Applying such principles and methods and determining that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documenting the methods and results of the analysis that justify such determination.
Deletion of 18 Specified Identifiers

- Name
- Address
- DOB
- Telephone #
- Fax #
- Email address
- URL address
- IP address
- Account #s
- License #s
- Medical Record #
- Health Plan Beneficiary #
- Device ID/Serial #
- Vehicle ID/Serial #
- Biometric ID (finger/voice)
- Full face photo or comparable image
- Any other unique identifying #, code or characteristic
Limited Data Sets (LDS)

- A limited data set is protected health information that excludes certain identifiers but permits the use and disclosure of more identifiers than in a de-identified data set.
- In particular, the limited data set allows the inclusion of all dates, 5 digit ZIP codes, and city as indirect identifiers.
- A limited data set may be used only for the purposes of research, public health, or health care operations.
- UC Davis Health System may use or disclose limited data set information only if it enters into a valid data use agreement.

**UCDHS does not have to account to the subject for disclosures using a limited data set.**
Identifying and Recruiting Subjects from Medical Record Information

- **Rule**
  - Researchers may use medical records to recruit patients to participate in studies only if they follow prescribed steps

- **Researcher Responsibilities and Options**
  - Get authorization (http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/resauth.html) from patients to put their information in a recruiting registry for future studies; or
  - Get a “partial” waiver of authorization from the IRB or Privacy Board to facilitate recruitment; or
  - Submit a “Review Preparatory to Research” application http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/resprep.html

- Prospective participants may be identified from medical records
- The information may be used to contact the participants, but
- The research team, when contacting participants, is considered a “business associate” and the contact information is regulated by HIPAA
Access and Correction

• Rule
  – Individuals whose identifiable private information we maintain are, with certain exceptions, generally entitled to access that information and to request correction of inaccurate information

• Researcher Responsibilities
  – Document any request for access and comply with the request unless:
    • You are concerned that disclosure of the information may harm the participant or others
    • The information requested includes results from laboratory tests that were not ordered by a physician or licensed practitioner and/or were not performed in a CLIA-certified clinical laboratory
    • There is some other reason to withhold access
  – If you do not intend to comply with a request for access, or need assistance in responding to the request, or are asked to make a correction with which you do not agree, contact the Privacy Office for assistance
Accounting for Disclosures

- **Rule**
  - Patients and research participants are entitled to an accounting of disclosures made without their authorization, unless an exception applies.
  - Use of UCDHS identifiable private information within UCDHS is not a disclosure, unless HIPAA applies to your project.
  - If HIPAA applies to your project, use of medical information for research without the patient’s authorization may trigger an accounting requirement (see next slide).
Accounting for Disclosures

• Researcher Responsibilities
  – Identify whether your project will trigger an accounting requirement
  – If so, report disclosures to the UCDHS Tracking of Disclosure Database: https://disclose.ucdmc.ucdavis.edu/disclose unless:
    • The patient or legally authorized representative signed a HIPAA authorization form for the study; or
    • You received only a limited data set, under a data use agreement
  – If a research participant requests an accounting of disclosures, refer him or her to the Health Information Management Department – all requests must be made in writing to the HIM Department
Break the Glass (BTG)

Break the Glass is a functionality used in EMR to monitor the access of certain patient records.

Employees must choose the appropriate reason from the drop down menu as to why they are accessing the record.

If no option is available, use the "other" option and provide a brief description.

Employee must re-enter their password.

• BTG options
  1. DEFAULT – Direct Medical Care
  2. Referral or appointment scheduling
  3. Lab or x-ray test interpretation
  4. Claim or billing activity
  5. Authorized CQI review
  6. Release of Information
  7. IRB-approved research (must enter IRB# and exp date below)
  8. EMR Team (explanation required)
  9. Other (explanation required)
BTG Print Screens
Common Scenarios
Common Scenarios

• Scenario (1)
  – Data are collected from a participant in connection with a routine office visit and recorded in the medical record
  – Intended Use: Research only
    • HIPAA Applies
    • Reasoning: HIPAA obligations apply to PHI created or received by or on behalf of the SHCC; purpose of creation or receipt is irrelevant.
Common Scenarios (cont’d)

- Scenario (1)
  - Data are collected from a participant in connection with a routine office visit and recorded in the medical record
  - Intended Use: Research only
    - HIPAA Applies
    - Reasoning: HIPAA obligations apply to PHI created or received by or on behalf of the SHCC; purpose of creation or receipt is irrelevant.
Common Scenarios (cont’d)

• Scenario (2)
  – Medical history collected from participant as part of voluntary participation in study
  – Data is not a byproduct of a clinical visit, or any other healthcare service event (any visit or service billed to Medicare, Medicaid, or another public or private health plan)
    • HIPAA Does Not Apply
    • Reasoning: Unit is outside of covered component; data not used for covered function.
Common Scenarios (cont’d)

• Scenario (3)
  – Data obtained from existing research records
  – Data did not originate from SHCC or other provider
  – Data not used for covered function (e.g., health care, payment)
    • HIPAA Does Not Apply
    • Reasoning: Researcher not performing covered function; data was never created/received by or on behalf of SHCC.