



Protecting Personally Identifiable Information (PII)

Privacy Act Training
for Project Sponsors

Health Information Management and Legal Considerations

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Establishes standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data.
- Mandates standardized formats for all patient health, administrative, and financial data; unique identifiers (ID numbers) for each healthcare entity, including individuals, employers, health plans and health care providers; and security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual.
- Prior to the implementation of the HIPAA privacy rule, healthcare providers were bound primarily by state-specific privacy laws

Health Information Management and Legal Considerations

- **Key terms:**
 - ***Confidentiality*** – The obligation of the healthcare provider is to maintain client/patient information in a way that will not allow disclosure beyond the healthcare provider.
 - It is the responsibility of **ALL** healthcare providers to keep client/patient-specific health information safe from dissemination/disclosure.

Health Information Management and Legal Considerations

- **Key Terms continued:**
 - ***Informed Consent*** – A legal doctrine that requires the healthcare provider to disclose information to a client/patient about the treatment to be done, its risks and benefits, and alternative treatment options so that the patient is well "informed" about the procedure and outcomes and can knowledgeably "consent" to the treatment being proposed.

Health Information Management and Legal Considerations

- Who may provide consent?
 - The competent adult patient
 - Parents or legal guardian of a MINOR child
 - Guardian (proxy) of incompetent or impaired adults

Health Information Management and Legal Considerations

- **When can a MINOR provide consent?**
 - *Only if they are:*
 - Legally EMANCIPATED
 - Married
 - In childbirth
 - In the armed forces

Some states allow minor consent for special medical circumstances like pregnancy (abortion or family planning), STD's, or substance abuse treatment.



Health Information Management and Legal Considerations

- Privacy – The right to be left alone and the right to control personal information and decisions regarding it.

Health Information Management and Legal Considerations

- What's the difference between Confidentiality and Privacy?
- Confidentiality is the **DUTY** of the **provider** to the client/patient.
- Privacy is the **RIGHT** of the **client/patient**.

Health Information Management and Legal Considerations

- **Protected Health Information:**
 - Anything spoken, written or in an electronic format
 - Relates to an individual's past, present and/or future physical/mental condition
 - Identifies an individual, or can be USED to identify an individual

Health Information Management and Legal Considerations

- **ESTATE of BEHRINGER vs. MEDICAL CENTER at PRINCETON**
 - Physician Behringer went into hospital for pneumonia, tested positive for HIV and was diagnosed with AIDS. By the time he was discharged his HIV/AIDS status had spread through the hospital grapevine, and as a result, most of his patients learned of it and left his practice. Dr. Behringer sued the medical center for breach of the duty to maintain confidentiality of his diagnosis. The courts found in Dr. Behringer's favor.



Protecting Personally Identifiable Information (PII)



Personally Identifiable Information (PII)

- Any information about an individual maintained by an agency that can be used to distinguish, trace, or identify an individual's identity, including personal information that is linked or linkable to an individual.

Sensitive Personally Identifiable Information(SPII)

- Social Security numbers, or comparable identification numbers, financial information associated with individuals, and medical information associated with individuals.

Note: Sensitive PII, a subset of PII, requires additional levels of security controls.

Personally Identifiable Information

What comprises PII?

PII includes: Name, email, home address, phone #

Sensitive PII includes:

If Stand-Alone:

- Social Security number
- Driver's License/ State ID#
- Passport number
- Alien Registration number
- Financial Account #
- Biometric identifiers

If Paired With Another identifier:

- Citizenship/immigration status
- Medical Information
- Ethnic or Religious affiliation
- Sexual orientation
- Account passwords
- Last 4 digits of SSN
- Date of Birth
- Criminal history
- Mother's Maiden name

Privacy Requirements

- Project Sponsors must maintain the confidentiality and privacy of client information.
- Agencies must keep all client information, including credit reports, confidential and secure.
- All staff who interact with clients/collect personal information must be trained – and demonstrate competence – on privacy issues and procedures.
- HUD and the approved agencies must safe guard data with client information.
- Loss of data must be reported to the designated MHC contact immediately.

Agency Privacy Policy

- In addition to the required disclosures, it is recommended that Project Sponsors disclose their privacy policy

A privacy policy is a legal document that states how a Project Sponsor collects, manages, and discloses both public and personal client data.

On the form, Project Sponsors typically list the entities to whom they disclose client information.

HUD's Privacy Protection Guidance for Third Parties

- HUD expects its third-party business partners who collect, use, maintain, or disseminate HUD information, to protect the privacy of that information in accordance with applicable law.
- See: PIH Notice 2014-10, HUD Privacy Protection Guidance for Third Parties
<http://portal.hud.gov/hudportal/documents/huddoc?id=pih2014-10.pdf>

HUD's Privacy Protection Guidance for Third Parties

Project Sponsors should take the following steps to help ensure compliance:

- Limit Collection of PII
- Manage Access to Sensitive PII
- Protect Electronic Transmissions of Sensitive PII via fax, email, etc.
- Protect Hard Copy Transmissions of Files Containing Sensitive PII
- Records Management – Retention and Disposition
- Incident Response



HUD's Privacy Protection Guidance for Third Parties

Limit Collection of PII

- Do not collect or maintain sensitive PII without proper authorization.
- Collect only the PII that is needed for the purposes for which it is collected.



HUD's Privacy Protection Guidance for Third Parties

Manage Access to Sensitive PII

- Only share or discuss sensitive PII with those persons who have a need to know for purposes of their work.
- Collect only the PII that is needed for the purposes for which it is collected.



HUD's Privacy Protection Guidance for Third Parties

Manage Access to Sensitive PII


- When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.
- Never leave messages containing sensitive PII on voicemail.
- Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests nearby who may overhear your conversation.



HUD's Privacy Protection Guidance for Third Parties

Manage Access to Sensitive PII


- Hold meetings in a secure place if sensitive PII will be discussed.
- Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.
- Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.



HUD's Privacy Protection Guidance for Third Parties

Protect Hard Copy and Electronic Files Containing Sensitive PII


- Clearly label all files containing sensitive PII—documents and removal media (example: ForOfficialUseOnly)
- Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.
- Protect all media(thumbdrives, CDs, etc.) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.



HUD's Privacy Protection Guidance for Third Parties

Protect Hard Copy and Electronic Files Containing Sensitive PII

- Keep accurate records of where PII is stored, used, and maintained
- Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.



HUD's Privacy Protection Guidance for Third Parties

Protect Hard Copy and Electronic Files Containing Sensitive PII

- Secure digital copies of files containing sensitive PII. Protection includes encryption, implementing enhanced authentication mechanisms such as two-factor authentication and limiting the number of people allowed access to the files.
- Store sensitive PII only on workstations located in areas that have restricted physical access.

HUD's Privacy Protection Guidance for Third Parties

Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

- When faxing sensitive PII, use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that the fax was received. Ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and all paper waste is disposed of properly, e.g., shredded. When possible, use a fax machine that uses a secure transmission line.



HUD's Privacy Protection Guidance for Third Parties

Protecting Electronic Transmissions of Sensitive PII via fax, email, etc

- Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.
- When faxing sensitive PII, use only individually controlled fax machines, not central receiving centers.



HUD's Privacy Protection Guidance for Third Parties

Protecting Electronic Transmissions of Sensitive PII via fax, email, etc

- Do not transmit sensitive PII via an unsecured information system (e.g., e-mail, Internet, or electronic bulletin board) without first encrypting the information.
- Do not place PII on shared drives, multi-access calendars, an Intranet, or the Internet.

HUD's Privacy Protection Guidance for Third Parties

Protecting Electronic Transmissions of Sensitive PII via fax, email, etc

- Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor.
- Sufficient justification, as well as evidence of information security, must be presented.

HUD's Privacy Protection Guidance for Third Parties

Protecting Electronic Transmissions of Sensitive PII via fax, email, etc

- Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque envelopes. Mark the envelope to the recipient's personal attention.
- When using the U.S. Postal Service to deliver information with sensitive PII, double-wrap the documents (e.g. use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement – ***To Be Opened by Addressee Only.***

HUD's Privacy Protection Guidance for Third Parties

Records Management: Retention and Disposal

- Follow records management laws, regulations, and policies applicable within your jurisdiction.
- Do not maintain records longer than required per records management schedules.
- Dispose of sensitive PII appropriately – use shredders for hard copies and permanently erase (not just delete) electronic records.

HUD's Privacy Protection Guidance for Third Parties

Incident Response

- Supervisors should ensure that all personnel are familiar with incident-response procedures.
- Promptly report all suspected compromisers of sensitive PII related to MS Home Corporation.

Consequences of Non-Compliance

- The Privacy Act imposes civil penalties when an employee:
 - Unlawfully refuses to amend a record.
 - Unlawfully refuses to grant access to records.
 - Fails to maintain accurate, relevant, timely and complete data.
 - Fails to comply with any Privacy Act provision or agency rule that results in an adverse effect.

Consequences of Non-Compliance

- The Privacy Act imposes criminal penalties: Misdemeanor and a fine of up to \$5,000 (for each offense).
 - For knowingly and willfully disclosing Privacy Act information to any person not entitled to receiving it.
 - For maintaining a System of Records without meeting the public notice requirements.
 - For knowingly and willfully requesting or obtaining records under false pretenses.

References & Resources

- The Privacy Act of 1974,
<http://usdoj.gov/opcl/privstat.htm>
- The E-Government Act of 2002,
http://www.whitehouse.gov/omb/memoranda_m03-22/
- Federal Information Security Management Act of 2002, Title 3 of e-Gov Act of 2002,
<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

Quiz

- Quiz