Indian Health Service

Nuts & Bolts of HIPAA Privacy & Privacy Act

HEATHER MCCLANE

IHS SENIOR OFFICIAL FOR PRIVACY/

BRYAN K. BURRELL

LEAD CONSULTANT, HIM

15 AUG 2024

Privacy at IHS

Carl Mitchell – Senior Agency Official for Privacy (SAOP)

Heather McClane – Senior Official for Privacy (SOP)

IHS Area Privacy Coordinators – (in the GAL)

Facility Privacy Liaisons

Health Insurance Portability & Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and give patients rights to their health information.

HIPAA establishes standards to safeguard the protected health information (PHI) that you hold if you're one of these covered entities or their business associate:

- Health plan
- Health care clearinghouse
- Health care provider that conducts certain health care transactions electronically

Health Plan

Although IHS is named in the HIPAA regulations specifically as a Health Plan.

IHS is also a Health care provider that conducts certain health care transactions electronically.

As both a Health Plan and Health care Provider, IHS must comply with:

The Privacy Rule

The Security Rule

Breach Notification Rule

The HIPAA Privacy Rule

The Privacy Rule protects patients' PHI while letting you securely exchange information to coordinate patients' care.

The Privacy Rule also gives patients the right to:

- Examine and get a copy of their medical records, including an electronic copy of their medical records
- Request corrections
- Restrict their health plan's access to information about treatments they paid for in cash Under the Privacy Rule, most health plans can't use or disclose genetic information for underwriting purposes. You're allowed to report child abuse or neglect to the authorities.

Protected Health Information

The Privacy Rule protects PHI that you hold or transmit in any form, including electronic, paper, or verbal.

PHI includes information about:

- Common identifiers, such as name, address, birth date, and SSN
- The patient's past, present, or future physical or mental health condition
- Health care you provide to the patient
- The past, present, or future payment for health care you provide to the patient

Requirements

The Privacy Rule requires IHS to:

- Notify patients about their privacy rights and how you use their information;
- Adopt privacy procedures and train employees to follow them;
- Assign an individual to make sure you're adopting and following privacy procedures;
- Secure patient records containing PHI so they aren't readily available to those who don't need to see them.

Sharing Information with Other Health Care Professionals

To coordinate patient's care with other providers, the Privacy Rule lets you:

- Share information with doctors, hospitals, and ambulances for treatment, payment, and health care operations, even without a signed consent form from the patient
- Share information about an incapacitated patient if you believe it's in the patient's best interest
- Use health information for research purposes
- Use email, phone, or fax machines to communicate with other health care professionals and with patients, as long as you use safeguards (e.g. Secure Data Transfer)

Incidental Disclosures

The HIPAA Privacy Rule requires you to have policies that protect and limit how you use and disclose PHI, but you aren't expected to guarantee the privacy of PHI against all risks.

Sometimes, you can't reasonably prevent limited disclosures, even when you're following HIPAA requirements.

For example, a hospital visitor may overhear a doctor's confidential conversation with a nurse or glimpse a patient's information on a sign-in sheet.

These incidental disclosures aren't a HIPAA violation as long as you're following the required reasonable safeguards.

The Office for Civil Rights (OCR) offers guidance about how this applies to health care practices, including incidental uses and disclosures FAQs.

De-Identification

De-Identification at IHS is a 4 step process:

Using the de-identification standards at 45 CFR 164.514 (b)(2):

One person makes required redactions

One person reviews redactions (makes any corrections)

IHS HQ Privacy Officer/Senior Official for Privacy verifies redactions

IHS Senior Agency Official for Privacy authorizes disclosures

Breach Notification

When you experience a PHI breach, the Breach Notification Rule requires you to notify affected patients, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The unpermitted use or disclosure of PHI is a breach unless there's a low probability the PHI has been compromised, based on a risk assessment of:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or got the disclosed PHI
- Whether an individual acquired or viewed the PHI
- The extent to which you reduced the PHI risk

Who Enforces HIPAA Rules?

The HHS Office of Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules. Violations may result in civil monetary penalties. In some cases, U.S. Department of Justice enforced criminal penalties may apply. Common violations include:

- Unpermitted PHI use and disclosure
- Use or disclosure of more than the minimum necessary PHI
- Lack of PHI safeguards
- Lack of administrative, technical, or physical ePHI safeguards
- Lack of patients' access to their PHI

Report Fraud, Waste, Abuse and Mismanagement

Whistleblower disclosures can save lives as well as billions of taxpayer dollars. They play a critical role in keeping our government honest, efficient and accountable. Recognizing that whistleblowers root out waste, fraud and abuse, and protect public health and safety, federal laws strongly encourage employees to disclose wrongdoing. Federal laws also protect federal employees from retaliation.

All employees, contractors and anyone who has contact with the Indian Health Service (IHS) can combat fraud, waste, abuse, and mismanagement. We encourage you to report these matters to the IHS Division of Personnel Security and Ethics (DPSE). OR the Department of Health Human Services Office of Inspector General (OIG) .

See the IHS page here: https://www.ihs.gov/ReportFraud/

Whistleblower Disclosures (within IHS)

Disclosures of information specifically prohibited by law (HIPAA or Privacy Act or 42 CFR Part 2) to be kept secret are protected only when made to an OIG, OSC, or certain individuals within Congress.

Additionally, federal law establishes that a federal employee has the right to communicate with and provide information to Congress.

To make a fraud, waste or abuse complaint you can make disclosures to supervisors or someone higher up in management within IHS;

You can report to privacy related matters to https://pirt.ihs.gov/privacy/

Whistleblower Disclosures (outside IHS)

Federal employees have many options on where to disclose wrongdoing, including but not limited to:

making disclosures to supervisors or someone higher up in management;

the agency's Inspector General (IG); OSC; or, Congress.

For whistleblower disclosures involving information protected from public release by law (e.g. patient privacy information), whistleblowers must use confidential channels such as an IG, OSC, or Congress in order to be protected from adverse personnel actions related to their disclosures.

Privacy Act

Privacy Act

Applies to federal agencies. Limits collection of personal information e.g. no secret government records, no secret use of government records, right to correct and see ones own records. Civil and criminal remedies.

All components of the Department are governed by the provisions of this part, including the Indian Health Service.

Protects **records about individuals retrieved by personal identifiers** such as a name, social security number, or other identifying number or symbol. An individual has rights under the Privacy Act to seek access to and request correction (if applicable) or an accounting of disclosures of any such records maintained about him or her.

Disclosures

Prohibits disclosure of such records without the prior, written consent of the individual(s) to whom the records pertain, unless one of the twelve disclosure exceptions enumerated in subsection (b) of the Act applies or as permitted by a Routine Use described in a System of Records Notice

Requires such records to be described in System of Records Notices (SORNs) published in the Federal Register and posted to the Internet.

Requests for Correction/Amendment

The patient must complete the IHS-917 form, "Request for Correction/Amendment of Protected Health Information."

Document the date you received the IHS-917 form and provide an acknowledgment of receipt of the IHS-917 form within 10 working days. (See 2-7.9B for a model letter on acknowledgment of receipt.)

If a decision on the request for correction or amendment can be made within 10 working days of the IHS' receipt of the request, the IHS will notify the patient of the receipt of the patient's correction or amendment request and its decision within that 10 day period.

In consultation with the appropriate staff member review the request for correction or amendment and inform the patient in writing within 60 days after receipt of the request, of approval or denial of the request for correction or amendment. The IHS-917 form will be filed at the site of the contested entry in the individual's medical record and maintained for the life of the record.

Permitted Disclosures

Consent to disclosure by a subject individual.

(1) Except as provided in paragraph (b) of this section authorizing disclosures of records without consent, no disclosure of a record will be made without the consent of the subject individual. In each case the consent, whether obtained from the subject individual at the request of the Department or whether provided to the Department by the subject individual on his own initiative, shall be in writing. (IHS-810)

Disclosures without consent (examples)

Disclosures without the consent of the subject individual. The disclosures listed in this paragraph may be made without the consent of the subject individual. Such disclosures are:

(1) To those officers and employees of the Department who have a need for the record in the performance of their duties.

(2) Required to be disclosed under the Freedom of Information Act.

(3) For a routine use which will be listed in any notice of a system of records.

Accounting

Accounting of disclosures.

(1) An accounting of all disclosures of a record will be made and maintained by the Department for 5 years or for the life of the record, whichever is longer.

except that, such an accounting will not be made:

For disclosures under the FOIA or to department officials who have a need for the record in the performance of their duties.


INDIAN HEALTH SERVICE
PHS · 1955 ·