

4. Health Insurance Portability and Accountability Act Privacy Rule

Contents

4.1	About the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule	4-2
4.1.1	IHS Notice of Privacy Practices.....	4-3
4.1.2	Request for Restrictions on Patient Information.....	4-3
4.1.3	Authorization for Use or Disclosure of Health Information	4-4
4.1.4	Request for Accounting of Disclosures	4-4
4.1.5	Hospital Directory	4-4
4.2	HIPAA Training.....	4-5
4.3	Impact of Privacy Regulations on the Business Office.....	4-5
4.3.1	Collection of Personal Information.....	4-6
4.3.2	Access to Records	4-7
4.3.3	Correction/Amendment of Records	4-8
4.4	Protected Health Information (PHI) Use and Disposal.....	4-9
4.4.1	Limiting Protected Health Information (PHI) to the Minimum Necessary	4-10
4.5	Maintaining Patient Confidentiality	4-10
4.5.1	Sending and Receiving Patient Information	4-11
4.5.2	Faxing Patient Information	4-11
4.5.3	Telephone Conversations	4-11
4.5.4	Workers' Compensation	4-12
4.6	HIPAA and Pharmacy Compliance.....	4-12
4.6.1	Medication Pick-up by Proxy	4-14

4.1 About the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 includes privacy regulations, which are designed to protect identifiable health care information of individuals during the transfer, storage, release, and destruction of that information.

All medical records and other identifiable health information used or disclosed in any form – whether electronically, on paper, or orally – are covered by the HIPAA Privacy Rule. Under this Rule patients have significant rights to understand and control how their health information is used and disclosed.

Patients have the right to:

- Inspect and receive a copy of their health record
- Request a restriction on their protected health information (PHI)
- Request a correction/amendment to their health record
- Request confidential communications about their health record/information
- Request a listing of certain disclosures IHS has made
- Revoke their written authorization to use or disclose their health information
- Obtain a paper copy of the IHS Notice of Privacy Practices upon request
- Obtain a paper copy of the IHS Health, Medical, and Billing Records System Notice #09-17-0001 upon request
- File a written complaint with the Service Unit Director/Chief Executive Officer or the Service Unit Privacy official or the Secretary of Health and Human Services, U.S. Department of Health and Human Services, Washington, DC 20201

For more information on HIPAA Policies and Procedures and HIPAA-compliant forms specified in the following sections, go to this website:

http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm?module=training_forms

4.1.1 IHS Notice of Privacy Practices

All patients, both new and established, shall be provided a copy of the current IHS Notice of Privacy Practices at their first visit to an IHS facility after April 13, 2003, as follows:

- Patient Registration staff will provide a copy of the current Notice to the patient.
- The patient will acknowledge receipt of the Notice by signing the “**Acknowledgement of Receipt of IHS Notice of Privacy Practices**” (Acknowledgement form).
- The Acknowledgement form will be filed in the patient’s medical record.

4.1.2 Request for Restrictions on Patient Information

Patients have the right to request restriction(s) on how their protected health information (PHI) can be used or disclosed to carry out treatment, payment, and health care operations, hospital directory; or disclosed to relatives, family members, close friends, health care givers, and any other person involved in the patient’s care or payment who is identified by the patient.

These are the procedures that shall be followed when requesting restrictions on patient information:

- The request must be writing, using **Form IHS 912-1 - Request for Restriction(s)**.
- The SUD/CEO or designee shall review the request before the patient is notified of the decision, except for acceptance of the request to restrict PHI from the hospital directory.
- If IHS agreed to a requested restriction, it may be terminated by IHS or the patient, using **Form IHS 912-2 - Request for Revocation of Restrictions(s)**.

4.1.3 Authorization for Use or Disclosure of Health Information

Prior to disclosing health information, **Form IHS 810 - Authorization for Use or Disclosure of Health Information**, must be completed and signed. A valid written request from the patient may also be honored.

Completion of the Authorization for Use or Disclosure of Health Information form (IHS-810) is not required for disclosures for which authorization is not required.

Disclosure of health information is a function of HIM staff; however, patient information is also contained in third-party billing records, and may be requested and released from Business Office staff.

Note: The requirement for an original signature is no longer mandatory but preferred. Copies of signatures may be honored, especially from other federal agencies, such as the Social Security Administration.

4.1.4 Request for Accounting of Disclosures

A patient has the right to request and receive an accounting of disclosures of protected health information (PHI) about the patient made by IHS and its contractors (business associates).

The request must be in writing, using **Form IHS 913 - Request for an Accounting of Disclosures**.

The following disclosures require accounting:

- Disclosures under the Routine Uses, 1 through 16 of the IHS Health, Medical, and Billing Records, System of Records, 09-17-0001
- Disclosures 3 through 12 of the Privacy Act, 5 U.S.C. 522(a)

4.1.5 Hospital Directory

An IHS facility may maintain a directory of patients and disclose limited protected health information (PHI) from that directory without the individual's written authorization, provided the individual was informed of the intended use or disclosure in advance, and had the opportunity to either agree to or prohibit the use of disclosure.

PHI that may be disclosed from a patient directory is limited to the patient's

- name
- location in the facility
- condition described in general terms (e.g., stable) that do not communicate specific information
- religious affiliation, which may be disclosed *only* to clergy, if the patient has not objected to such disclosure

4.2 HIPAA Training

It is everyone's responsibility to protect the patient's privacy. Therefore, IHS facilities must provide HIPAA privacy training to

- All employees, volunteers, and contractors
- New employees as soon as possible, but no later than 30 days after start date
- Designated staff, whenever HIPAA-related policies and procedures are revised

HIPAA training provided to staff shall be documented and maintained in writing or electronically for six (6) years.

For more information, go to the IHS HIPAA website:

<http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm>

For IHS HIPAA Policies and Procedures (P&P) and related forms, go to this website:

http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm?module=trainin_g_forms

4.3 Impact of Privacy Regulations on the Business Office

The affect of the HIPAA Privacy Rule on health records will be incorporated into Health Information Management (HIM). The HIM staff members are the experts in using and disclosing protected health information (PHI). However, the Business Office must be aware that Billing records are also PHI and have been added to the Privacy Act's System of Records.

As of April 13, 2004, HIPAA requires that each patient sign an acknowledgement that he or she received a copy of the Notice of Privacy Practices. This form is filed in the medical record.

In addition, facilities must account for any disclosure or use of any patient health information, to whom it was disclosed, the date of disclosure, and the purpose of the disclosure and/or a copy of the authorization/request for disclosure.

The following sections provide a summary of an individual's rights and IHS employee responsibilities under the Privacy Act:

4.3.1 Collection of Personal Information

The following paragraphs summarize an individual's rights when asked to provide personal information and the health care employee's responsibilities when requesting such information.

Individual Rights: Whenever an individual is requested to provide personal information to a Federal agency, he/she is entitled to know the

- legal authority for requesting the information,
- purpose for collecting this information,
- what related uses might be made of this information,
- whether their response is mandatory or voluntary, and
- what effect their refusal to provide the information would have.

Employee Responsibilities: You must collect *only* personal information that is relevant, accurate, complete, and necessary to accomplish an authorized agency function. Whenever you request personal information from an individual, you must inform him/her in writing of the

- legal authority,
- purpose for collecting this information,
- what related uses will be made of this information,
- whether a response is mandatory or voluntary, and
- what will be the effect if he/she refuses to respond.

The collection of personal information is usually provided on a form given to the person providing the information. You should always attempt to collect personal information directly from the individual rather than from other sources.

Whenever you ask for a Social Security Number you must tell the individual the purpose for requesting it.

4.3.2 Access to Records

The following paragraphs summarize an individual's rights to access his/her medical records and the health care employee's responsibilities when responding to a request for access to medical records.

Individual Rights:

- An individual can request to see his/her records in writing or in person. The individual should describe the information he/she wishes to see, because blanket requests for "all the information the agency has on me" cannot be honored.
- If the individual appears in person, identification will be required to verify that he/she is the person whose record is requested. If the patient does not have suitable identification, he/she will be asked to certify his/her identity in writing.
- The individual may have another person accompany him/her to review his/her records.
- The individual is entitled to receive a copy of his/her record or an acknowledgement of his/her request within ten (10) working days.
- An individual is not required to give a reason for the request.

Employee Responsibilities:

- When an individual requests to see his/her record, you must verify his/her identity or require written certification that he/she is the subject of the record requested.
- Always keep a signature on file, so that the signature on the written request can be checked against the one on file. If, by chance, the signature is forged, your legal protection is that you acted in "good faith".

Note: Telephone requests are not honored, because positive identification of the caller may be difficult to establish.

- When a request for a record is received, you should check to see whether a record exists on the person in the system of records that is subject to the Privacy Act. Depending on the procedure in your organization, the system manager or designee must either present the record or a copy of it, or acknowledge the request within ten (10) working days.

- You should not ask the person to give a reason or to justify a need to see his or her own record
- If a patient requests another person's presence when he/she wants to inspect or discuss his/her records, you must have the individual authorize the other person's presence in writing prior to the inspection or discussion of the records.

For the policy and procedure related to accessing records, go to this website:

<http://www.ihs.gov/AdminMngrResources/HIPAA/documents/AuthorizationforUseorDisclosurePP31JAN03A.pdf>

4.3.3 Correction/Amendment of Records

In general, only factual, verifiable information is subject to amendment under the Privacy Act. Other procedures, such as personnel grievance procedures, should be followed if the patient wishes to contest subjective opinion.

The following paragraphs summarize an individual's rights to request an amendment to his/her health records and the health care employee's responsibilities when responding to such a request.

Individual Rights:

- An individual can request to correct, delete, or add information in his/her health record in writing or in person. The individual must identify the record information to be corrected and give his/her reasons for the desired change.
- The individual should expect an acknowledgement of the request within ten (10) working days.
- If the individual appears in person, identification will be required to verify that he/she is the person whose record is requested. If the patient does not have suitable identification, he/she will be asked to certify his/her identity in writing.

Employee Responsibilities:

- When an individual requests an amendment to his/her health record, you must verify his/her identity or require written certification that he/she is the subject of that record.
- Depending on your organization's procedures, you or a designated official must acknowledge a request to amend a record within ten (10) working days and advise the person when he or she can expect a decision on the request.
- Normally, a review should be completed within thirty (30) days. Under the regulations, an appeal must be decided within 30 days, which may be extended an additional 30 days.

4.4 Protected Health Information (PHI) Use and Disposal

Protected health information (PHI) includes any medical or demographic data that specifically identifies a particular patient, or may be used with other data to identify the patient, regardless of the type of storage media. This includes but is not limited to anything with the patient's

- name
- chart number
- address
- phone number
- fax number
- cell-phone number
- pager number
- e-mail address
- social security number

Additionally, PHI includes data identifying relatives or data, which when combined with other data, can be used to identify the patient. The Privacy Act defines what is identifying information.

PHI data may be found on health summaries, lab slips, unused prescription labels, label reprints, NCR copies, unused summary labels, Drug Utilization Review logs, manual or electronic organizers, computer files, palm device files, compact disks, floppy disks, zip drive disks, e-mail messages, and notes to yourself with patient identifiers.

All unused PHI, including label reprints, unused labels, summary labels, health summary copies, report copies needing to be destroyed, should be shredded, sequestered, and incinerated, or otherwise made to be completely unreadable.

Labels that are not applied to anything tend to jam shredders. These can be cup-up with scissors, may be applied to other PHI or scratch paper and shredded, or sequestered and later incinerated.

If any PHI is sequestered, make sure it remains secure and out of the view of persons who are not authorized to view it. PHI obliterated by marking over key data with black felt markers may still be readable by using different lighting techniques or back lighting, and is not recommended.

Covered health care providers may use protected health information to create de-identified information. De-identified information must be void of any information that could be used to identify the individual subject of the information, such as the patient's name, address, exact birthdate, or any unusual identifiers (e.g., unusual occupation, high salary, or age).

For more information, see the *Indian Health Manual*, Part 5, Chapter 15, "Records Management Program" (Section 5-15.4), at this website:

<http://www.ihs.gov/PublicInfo/Publications/IHSManual/Part5/pt5chapt15/pt5c hpt15.htm>

4.4.1 Limiting Protected Health Information (PHI) to the Minimum Necessary

IHS must make reasonable efforts to limit the use and disclosure of and request for protected health information (PHI) to the **minimum necessary** to accomplish the intended purpose of the use, disclosure, or request, except to the subject patient or pursuant to a valid authorization.

4.5 Maintaining Patient Confidentiality

Patient confidentiality is a serious matter. Even if you are using a code, you are passing confidential information.

Asking a patient how they are doing with their medical problem in front of other people is a breach of patient confidentiality. Having a conversation about a person, saying "so-and-so" has cancer, is not acceptable. The bottom line is – do not discuss patients' conditions casually.

If you breach patient confidentiality, you can be fined, criminally charged, and even sent to prison. Furthermore, you risk the wrath of the angry patient whose privacy has been exploited and who is perfectly within his or her right to sue your health care facility.

The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. The following sections provide some helpful tips for maintaining patient confidentiality.

4.5.1 Sending and Receiving Patient Information

IHS will ensure that patient information or medical records sent from or received by IHS facilities are handled in a manner that protects against unauthorized disclosure of such records to third parties.

4.5.2 Faxing Patient Information

Because the use of Facsimile (FAX) machines poses certain risks of improper disclosure of confidential patient information, IHS facilities are encouraged to send and receive patient medical records by mail whenever practical.

Transmission of patient medical records by FAX should be limited to the minimum amount necessary to accomplish the intended purpose. For the policy and procedure related to faxing protected health information (PHI), go to this website:

<http://www.ihs.gov/AdminMngrResources/HIPAA/documents/FacsimilePP31JAN03.pdf>

4.5.3 Telephone Conversations

When there is a request for confidential patient information, it is better to have the patient make his or her request in writing than to address it over the phone.

Another precautionary idea is to ask the patient his or her name, address, telephone number, birth date, and Social Security number. If the patient stumbles or pauses when giving a birth date, that is a possible sign the person isn't who he/she says he/she is. A better way is to ask the patient for the above information and tell her you will call back with an answer. This way you can check the phone number against the one in your file. This is added protection.

In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

Make sure all staff is trained on how to handle such patient inquiries.

4.5.4 Workers' Compensation

It is not uncommon for an employer to call a facility to ask direct questions regarding a person who claimed they were injured on the job. Tell the caller you cannot give out patient information. If the caller claims to be the patient, it is very important that you ask the caller to put their questions in writing or ask for their name, address, telephone number, birth date, and Social Security number, or some other identifying information such as mother's maiden name.

4.6 HIPAA and Pharmacy Compliance

HIPAA requires that certain electronic transmissions be standardized. The new law requires using the National Council for Prescription Drug Programs (NCPDP) Telecommunication Standards Version 5.1. The Privacy Officer, techs and upper management of the facility or retail chain will make sure transaction standards are in place. Most pharmacists will not have to deal with this directly.

Pharmacies should keep three years of records, including

- payable claims
- a copy of the patient's prescription (hard copy readily retrievable)
- a copy of the Prior Authorization

A signature log needs to be kept that clearly informs the patient of what they are acknowledging. This acknowledgement cannot be used as a waiver or permission for anything else that appears on the log book (such as a waiver to consult with the pharmacist).

The HIPAA Privacy Rule provides covered health care providers with discretion to design an acknowledgment process that works best for their business. The signature log, along with other records, should be stored for seven years.

A local procedure for providing information to payers needs to be defined and written. This would include disclosures for the purpose of treatment, payment, or health care operations.

Signed acknowledgements that patients received a copy of the Notice of Privacy Practices must be retained for six years from the date they were signed or the last date a patient was treated, whichever is later.

In addition, providers must keep track of any disclosure or use of any information that is not related to treatment, payment, or health care operations or pursuant to an authorization for six years. The documentation of a disclosure must

- describe the PHI that was disclosed,
- to whom it was disclosed,
- the date of disclosure, and
- the purpose of the disclosure (and/or a copy of the authorization or request for disclosure).

On patient request, a pharmacy must provide a written accounting of these disclosures. It must also establish a policy for responding to patient requests for such documentation. Accountings must be provided to a patient at no charge for the first request within a 12-month period. Pharmacies may establish a reasonable fee to provide additional accountings to patients within a 12-month period.

Patients have the right to obtain a copy of their pharmacy records. On receipt of a patient request, the pharmacy has 30 days to provide the patient with a copy.

Patients can also request a change to their records. It is best to ask the patient to put the request in writing and include the reason for the change. The pharmacy must act within 60 days to determine whether the change is appropriate and then correct the records, if necessary.

For example, a patient denies receiving a prescription for haloperidol. Under the privacy rules, the pharmacy may be required to check their records, contact the physician, or other, to see if this is a real error before updating the patient's medical record.

Before deleting any health information from a patient's record, make sure the removal of the information is consistent with other laws or your facility's general practices.

A pharmacy should have counseling rooms that are out of ear-shot from other patients. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients.

The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. Reasonable precautions should be taken to minimize the chance of incidental disclosures to others who may be nearby.

Pharmacists can call the prescriber to clarify a patient's medication and can report to public health surveillance programs, suspected victims of abuse or neglect. One concept of HIPAA is the concept that patient privacy should be protected by minimizing the amount of private information that is given out about a patient and minimizing where the information is sent. This concept is often referred to as "minimum necessary" (IHS HIPAA P&P).

4.6.1 Medication Pick-up by Proxy

A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription.

For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual's care, and the HIPAA Privacy Rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the pharmacist with the names of such persons in advance.

As written, the HIPAA regulations give the professional considerable latitude in making the decision to give or not give medications to proxies. The key is that the professional, using his or her personal judgment, must decide if giving a proxy the patient's medications, is in the patient's best interest.

Consider the following guidelines when deciding whether to give a patient's medication to a proxy:

- The pharmacist should determine if the proxy is indeed involved in the patient's care. The pharmacist can find evidence of this by checking the chart to see if the proxy is the patient's next of kin, caregiver, or is referred to in the physician's or other health care professional's Patient Care Component notes. If there is no notation, the pharmacist should ask, "Did the patient ask you to pick up their medications?" and "What is your relationship to the patient?"
- If the pharmacist suspects that the person picking up the medications is not who they say they are, or that the proxy does not have permission from the patient, then the pharmacist should refuse to give that person the medications.

An example might be the "proxy" who attempts to pick up narcotics for one or more "relatives," and you know the patients have not come to the facility for some time. If the pharmacist is unsure, he or she can call the patient or can look for evidence that the person picking up the medications is involved in the patient's health care as noted above.

- If the pharmacist feels that it may not be in the patient's interest to give the medications to a proxy even with permission, then he or she should refuse to give the proxy the medications.

An example of this might be a Metronidazole prescription for the patient and the patient's contacts, where the spouse is one of multiple contacts. In such instances, the pharmacist should request the patient to pick-up medications or should find some confidential way of getting the medications to the patient.

- Under no circumstances should the pharmacist volunteer that medications are here for someone's relative.

As an example, "Did you know that your sister's medications are here? Would you like to take them to her?" is clearly outside of acceptable limits. The proxy must be asked by the patient to pick up the medications or be involved in the patient's health care. Parents, Caregivers, PHNs, and CHRs meet this definition within HIPAA.

- If the pharmacist refuses to give the medications to the proxy, then he or she should document the incident and the reason why in the patient's chart.