Washburn University Athletic Training Program

HIPAA Education Document
Health Insurance Portability and Accountability Act

HIPAA is the first-ever federal privacy standards to protect patients' medical records and other health information provided to health insurers, doctors, hospitals and other health care providers. These new standards, developed by the Department of Health and Human Services (HHS), provides patients with access to their medical records, and more control over how their personal health information is used and disclosed. They represent a uniform, federal law of privacy protection for consumers across the country.

HIPAA originated in 1996 and implemented on April 14, 2003. It was designed to help protect a patient's privacy or PHI (Protected Health Information). Regulations cover information that is communicated or transmitted electronically, written or verbally. HIPAA is a federal law designed to apply consistent patient confidentiality practices nationwide. Violations will result in fines and penalties. Simple negligence could result in a fine up to $50,000 and/or 1 year in prison. Disclosure under false pretences could result in a fine up to $100,000 and/or 5 years in prison. Intent to sell or use information could result in a fine up to $250,000 and/or 10 years in prison. Federal and State laws have existed for a long time regarding privacy. When federal law (HIPAA) and state law conflict, HIPAA prevails, except when the state law is more stringent. HIPAA makes everyone's practice consistent.

HIPAA is divided into 3 sets of regulations:
- Electronic Transactions and Code Sets
- Patients Privacy
- Electronic Security

Regulations were written by the Department of Health & Human Services, and were approved by Congress and the President. Care was taken in carefully wording the regulations:

Example: Word Comparison:

Pathagorean Theorem	24 words
The Ten Commandments	179 words
Lincoln's Gettysburg Address	286 words
Declaration of Independence	1,300 words
HIPAA Privacy Regulations	401,034 words

HIPAA provides patients certain rights regarding their PHI:
- Right to Inspect and Copy their Medical Record
- Right to Amend information in their Medical Record
- Right to an Accounting of Disclosures
- Right to Request Restrictions on the Release of their Health Information
- Right to Request Confidential/Alternate Communications
- Right to a paper copy of the Notice of Privacy Practices

Authorization

Authorization (Release Of Information) forms must be in writing, specifying exactly what information is being released. Psychotherapy Notes require a separate authorization for release, even when that release is for treatment purposes. A verbal statement that an authorization exists is not acceptable. An official personal representative can sign an authorization form for a specific patient (personal representatives include durable power of attorney for example)

Required elements of an authorization:

- A specific and meaningful description of the information to be released
- Name or other specific identification of the person(s) or class of persons authorized to make the disclosure
- Name or other specific identification of the person(s) to whom the facility may make the disclosure
- An expiration date or event that relates to the individual or the purpose of the use or disclosure
- A statement of the individual's right to revoke the authorization in writing
- A statement about the exceptions to the right to revoke and a description of how the individual may revoke the authorization
- A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient of the PHI and will no longer be protected by the privacy rule
- The signature of the individual authorized to initiate the authorization
- The date the authorization is signed
- The relationship of the individual signing the authorization, if not the patient

The patient may revoke a written authorization at any time. The revocation request must be in writing. The facility may refuse the request under the following circumstances:

- The facility has already taken action based upon the previously signed authorization
- If the authorization was obtained as a condition of obtaining insurance coverage, other laws provide the insurer with a right to contest the claim under this policy

Inspect and Copy Records

Patients or their personal representative can request to view or receive a copy of their medical records. This may not be allowed if the information is harmful to the patient's health (for example, psychiatric records). Hospitals, clinics, nursing homes and other covered entities generally should provide access to these records within 30 days and may charge patients for the costs of copying and mailing the records.

Amendments to Records

Requests to amend records must be in writing.
The hospital or physician may accept or deny (in whole or in part) the request to amend.
If an amendment is accepted, it must be made to all copies of the medical record. (This includes records sent to other physicians, insurance companies, workers comp, etc.) The patient will be provided notice that these actions have occurred and who was notified of the change.

If the amendment is denied, the patient will be notified of the reason.
The patient may appeal a denial. The facility will assign an associate or medical staff member not involved in the care of the patient to review amendment.

Accounting of Disclosures

Patients can request a list of parties to whom their PHI was disclosed within the past 6 years (going back to April 1, 2003). The request must be in writing. The facility must keep documentation of the accounting of PHI for a period of at least 6 years.
The facility is not required to provide an accounting for:

- Copies to patient's attending physician, insurance carriers
- Copies to the individual patient, parent of un-emancipated minor child
- Listing of patient's religious affiliation, disseminated to Clergy, per patient's prior agreement
- Copies to new physician or clinic, as a result of authorization form signed by the patient
- National security or intelligence purpose
- Correctional institutions or law enforcement officials as provided in 45 C.F.R. 164.512(k)(5)
- As part of a limited data set in accordance with 45 C.F.R. 164.514(e)

The information the patient will receive for each disclosure is:

- Date of the disclosure
- Name of the entity or person who received the PHI
- If known, the address of the entity or person
- A brief description of the PHI disclosed
- A brief statement of the purpose of the disclosure, in lieu of such a statement, a copy of the individual's written authorization

Restrictions of Use of PHI

Patients may request restrictions on how their PHI is used in treatment, payment, healthcare operations, and disclosures to family and friends. The facility may accept or deny the request. It may be denied if the restriction could get in the way of providing emergency care.

Confidential Communications

Patients can request that their doctors, health plans and other covered entities take reasonable steps to ensure that their communications with the patient are confidential.
Patients may request alternate means of communications, such as:
Alternate address
Alternate phone number
E-mail address
The facility may not require the patient to explain why they are requesting an alternate method of confidential communication of their PHI. If there are costs to accommodate a request the individual will be notified of the cost.

Notice of Privacy Practices

On the date of the first delivery of treatment after April 14, 2003, even if treatment is delivered electronically or via the telephone, a patient shall be presented with a Notice of Privacy Practices. The Notice of Privacy Practices describes how the patient's personal medical information may be used, and gives their rights under the new HIPAA privacy regulations. The notice will be mailed to the patient if the initial contact was not in person. A copy will also be offered to the patient at any time if they request one. A good faith effort will be made to obtain a written acknowledgment of receipt of the Notice of Privacy Practices. Documentation that a Notice of Privacy Practices has been offered to a patient for review must be placed in the patient's records.

Disclosure of PHI (Protected Health Information)

Confidential uses and disclosures of protected health information are allowed under HIPAA:

- When it cannot be reasonably prevented
- Disclosure occurs as a result of an otherwise permitted use or disclosure
- Safeguards must be in place to protect the confidentiality of patient health information
- Examples: A physician is at a nursing station talking quietly with a nurse about a patient's condition and the conversation is overheard by a visitor. In a semi-private room the physician is discussing the patient's condition with them and is overheard by the patient's roommate.

Patient Identification

Name, location, condition (general terms), religious preference can be released if:

- The patient is identified by their correct first and last name
- The patient has not "opted out" (a patient may request in writing that no patient identification information be released)

Release and disclosure of PHI without consent

Health care providers can release patient information without a signed authorization for the following reasons:

- When required by law
- Required for public health activities (such as mandated disease reporting, reporting to the FDA regarding and FDA regulated product or activity, the reporting of vital event, births, deaths, etc.)
- Reporting of abuse or neglect as required by law
- Law enforcement purposes
- Medical examiners and funeral directors
- Organ and tissue donation purposes
- Relating to approved research
- To comply with workers comp laws
- Emergency care
- Disaster relief

- Hospital directory (unless the patient opts-out)
- Inform clergy of patient status (unless the patient opts-out)
- Fundraising (unless the patient opts-out)
- Appointment reminders (minimum necessary information only will be used)

De-identified Information

Identifying elements of a patient information that are considered to be so specific as to serve as "identifiers" to others. If the health information does not identify the individual, and there is no reasonable basis to believe that the information can be used to identify the individual, then it is not individually identifiable health information. Removal of the following specified identifiers creates a presumption of de-identification, indicating that the information is no longer covered by the regulatory rules granting it the protection of protected health information (PHI).

Information may be considered "de-identified" if the following identifiers of the individual, their relatives, employers, or household members of the individual are not included:

- Names
- Selected geographic information including street address, city, county or zip code
- All elements of dates such as birth date, admission date, discharge date, date of death, all ages over age 89, and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical Record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial number, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code