

Uses and Disclosures

County of Butte HIPAA Training Module #2

Identifying Appropriate and Inappropriate Uses and Disclosures of Protected Health Information



Training Objectives:

Health care component staff members shall:

1. Understand when a disclosure is required or permitted without a “HIPAA-ized” authorization.
2. Use only County approved “HIPAA-ized” authorization forms when HIPAA requires the patient’s permission to disclose protected health information.



HIPAA Refresher

The Health Insurance Portability & Accountability Act of 1996 (HIPAA), Public Law 104-191, included “Administrative Simplification” provisions that required the federal Department of Health and Human Services to adopt national standards respecting electronic health care transactions for **billing** as well as to mandate minimum levels of **privacy** and **security**.

The **Privacy Rule** established, for the first time, a foundation of Federal protections for the privacy of protected health information. (Covering more than alcohol and drug health information addressed in 42 C.F.R. Part 2.)



“More Stringent” Rule

Keep in mind throughout this and all HIPAA training modules that:

- The Privacy Rule does not replace Federal, State or other law that grants individuals even greater privacy protections, and
- Covered entities are free to retain or adopt more protective policies or practices.



What is “PHI?”

Throughout this, and all County HIPAA training modules, we will use the term “PHI.” This refers to:

Protected

Health

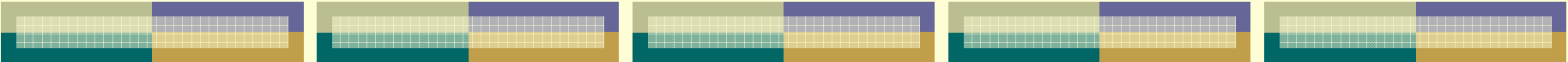
Information



Definition of PHI

PHI is any information, whether oral or recorded in any form or medium, that:

- A health care provider, health plan, public health authority, or health care clearinghouse creates or receives;
- Relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;
- Identifies the individual or there is a reasonable basis to believe that the information could be used to identify the individual, including demographic information (name, address, DOB, SSN, payment history, account number, etc.);
- Can be transmitted or maintained electronically, or in any other form or medium.



County Guidelines and Department Policies & Procedures

NOTE!

This training module outlines the County's HIPAA Implementation Guidelines. A copy of the Guidelines and other HIPAA materials can be found in the County's HIPAA Public Folder (in Outlook). You can also request a copy from your Department's Privacy Coordinator or the County Compliance Officer.

HIPAA-designated departments may develop policies and procedures based on these guidelines but which address concerns and situations particular to a department or program.

Also the forthcoming County HIPAA Security Policies & Procedures will further define technical safeguards.



Required HIPAA Disclosures

There are only two disclosures *required* under HIPAA:

Health care components are *required* to disclose protected health information:

1. to the patient when a request has been made, and
2. when required by the U.S. Department of Health and Human Services, Office of Civil Rights to investigate compliance with HIPAA's Privacy Regulations.

NOTE: Authorizations do not need to be obtained for these required disclosures.



Permitted Uses and Disclosures

Under HIPAA, authorizations are *not* required for certain types of disclosures to providers. However, HIPAA's permissible language leaves the door open for providers to still require an authorization before disclosing.

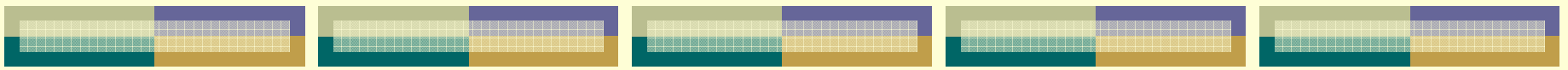
NOTE: Other State and/or federal privacy laws with more stringent privacy protections (such as laws protecting the confidentiality of alcohol and drug treatment information) may require a patient's consent even where HIPAA does not.



Permitted Uses and Disclosures

The following are the types of uses and disclosures permitted under HIPAA:

- Treatment , Payment or Health Care Operations (TPO)
 - Incidental Disclosures
- Other Permitted and Required Disclosures (such as to caregivers, as required by law, research, etc..which will be discussed in detail)
 - Authorized Disclosures



Treatment, Payment, Health Care Operations (TPO)

Under HIPAA, health care components are permitted to use or disclose protected health information for treatment, payment or health care operations.

Note: Even though HIPAA's Privacy Regulations do not require authorizations for these types of disclosures, providers may still require an authorization before disclosing. Additionally, there may be stricter State or federal privacy protections that must be address, such as laws protecting the confidentiality of alcohol and drug treatment information.



Treatment

Treatment generally means the provision, coordination, or management of health care and related services . . .

- among health care providers or by a health care provider with a third party such as a health plan,
- or the referral of a patient from one health care provider to another.



Examples of Disclosures for Treatment

- A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.
- A hospital may send a patient's health care instructions to a nursing home to which the patient is referred.
- A physician may send an individual's health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.



Remember!

HIPAA's Privacy Regulations create a floor, or a mandatory minimum level, for privacy protection.

Other State and/or federal laws may impose requirements that are more stringent under certain circumstances, such as for the sharing of alcohol and drug treatment information.

HIPAA does not supercede privacy protections that are more stringent than the Privacy Regulations.



Payment

Payment encompasses the various activities of health care providers:

- to obtain payment or be reimbursed for their services and of a health care plan to obtain premiums,
- to fulfill their coverage responsibilities and provide benefits under the plan, and
- to obtain or provide reimbursement for the provision of health care.



Examples of Disclosures for Payment

- Disclosing information necessary to determine eligibility or coverage under a plan and adjudicating claims.
- Disclosing information necessary to make risk adjustments.
 - Billing and collections activities.
 - Reviewing health care services for medical necessity, coverage, justification of charges, etc.



More Examples

- A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment services.
- A health care provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.



Health Care Operations

Health care operations are certain administrative, financial, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.



Examples of Disclosures for Operations

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines.
- Population-based activities relating to improving health or reducing health care costs.
- Case management and care coordination (internally and with other health care providers ... NOT with non-covered entities).
- Contacting health care providers and patients with information about treatment alternatives.



More Examples

- Reviewing the competence or qualifications of health care professionals.
 - Evaluating practitioner and provider performances.
- Conducting training programs in which students, trainees, or practitioners in areas of health care, learn under supervision to practice or improve their skills as health care providers.
 - Training of non-health care professionals, and
 - Accreditation, certification, licensing or credentialing activities.



Consent vs. Authorization

Keep in mind, HIPAA authorizations are NOT required for TPO disclosures. However, in some cases (such as when dealing with alcohol and drug treatment information) health care components may implement an extra layer of privacy protection by still requiring a *consent* by the client to release information relating only to *treatment, payment or health care operations*.

NOTE: Be sure to understand the distinction between a “consent” and an “authorization.”



Consent vs. Authorization

A “consent” document is *not necessarily* a valid permission to use or disclose protected health information for a purpose that requires an “authorization” under HIPAA’s Privacy Regulations, or where other requirements or conditions exist under the Regulations for the use or disclosure of protected health information.

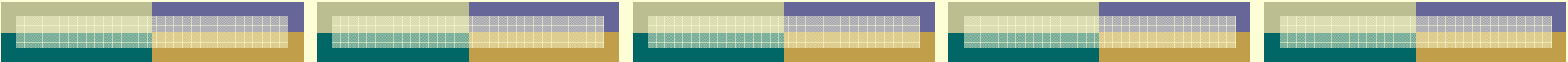
Questions about whether a consent is valid should be directed to a Supervisor, who would then consult with your Department’s Privacy Coordinator.



Incidental Disclosures

In addition to disclosures for TPO, the HIPAA Privacy Regulations also permit disclosures that are incident to a use or disclosure otherwise permitted or required by the Privacy Regulations so long as the information is the minimum necessary and other safeguards are in place to limit the disclosure.

For example: A sign-in sheet in a clinic that lists patients names would be an incidental disclosure to providing treatment to those individuals. However, the health care component must take care to limit the disclosure by asking only for a name, not the medical condition, and by keeping the sign-in sheet near to the receptionist.



Other Permitted and Required Disclosures

Other permitted disclosures may be made consistent with the HIPAA Privacy Regulations and the County's Privacy Policy & Procedures (and the corresponding Guidelines):

- Family and others involved in a patient's health care (see County HIPAA Guidelines #26)
- Disclosures required by law (see County HIPAA Guidelines #25)
- Disclosures for research purposes if authorization is properly waived (see County HIPAA Guidelines #29).



Disclosures to Family & Other Caregivers

HIPAA permits health care personnel to use or disclose protected health information to notify, or assist in the notification of (including identifying or locating):

- a family member,
- a personal representative of the client
- or another person responsible for the care of the patient.

NOTE: The authority and identity of such a person must be verified. Each Health Care Component must have specific procedures in place, and may also implement more stringent standards as State or federal law may require.



Disclosures Required by Law

Health care personnel may disclose protected health information without a patient's consent, authorization or the opportunity to agree or object as may be required by applicable state and federal laws.

Personnel should check with their Supervisor, the Department's Privacy Coordinator, and the County Compliance Officer (all of whom may consult with County Counsel as appropriate) to determine when a disclosure is required by law.



Examples of Disclosures Required by Law

- Mandatory reporting of suspected abuse or neglect of children.
- Mandatory reporting of suspected abuse, neglect, domestic violence or criminally injurious conduct against adults.
 - Pursuant to court orders.
 - Pursuant to subpoenas.
- Disclosures to law enforcement officials legitimate purposes (e.g. identify or locate a suspect, fugitive, material witness, or missing person)



More Examples

- Uses or disclosures to avert serious threats to health and safety.
- Uses and disclosures for special government functions (e.g. in compliance with the National Security Act).
- Uses and disclosures to Public Health or other recognized public health authority for a legitimate purpose.
- Uses and disclosures under worker's compensation laws.



IMPORTANT!

County Personnel shall consult with the County Compliance Officer and/or County Counsel before any disclosures required by law are made to confirm that the requirements for such disclosures are met.



Disclosures for Research

The basic rule is that use or disclosure of protected health information for research should always utilize an authorization if possible.

Only when it is not practical should one of the alternative methods provided in the HIPAA Privacy Regulations be used.

Note: The HIPAA Privacy Regulations govern only covered entities, not simply researchers. Researchers *within* a covered entity must, however, comply with HIPAA.



How to Approach Research

1. **Authorizations:** Has the researcher obtained authorizations from the individuals whose PHI is needed for the research?
2. **IRB/Privacy Board Waiver:** If the authorization is not feasible, does the researcher have documentation of an IRB or Privacy Board waiver of authorizations or a waiver of the content of the authorization?
3. **Limited Data Set Agreement:** Does a data use agreement that releases a limited data set meet the purpose of the research?
4. **De-Identified PHI:** Will the PHI that is de-identified meet the purpose of the research?



Waiver of Authorization

The following three (3) criteria must be satisfied for an Institutional Review Board (IRB) or Privacy Board (PB) to approve a waiver of authorization under the HIPAA Privacy Regulations . . .



Minimal Risk

1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of the individual, based on, at least, the presence of the following elements:
 - an adequate plan to protect the identifiers from improper use and disclosure,
 - an adequate plan to destroy the identifiers at the earliest opportunity (unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law),



Practicality

2. The research could not practically be conducted without the waiver or alteration;

AND

3. The research could not practically be conducted without access to and use of the PHI.



Disclosures Made Through Limited Data Sets

A limited data set is protected health information that does not directly identify the patient, but which contains certain potentially identifying information.

Health care personnel may use and disclose a limited data set without patient authorization **only** for the purpose of research, public health or health care operations **if** the health care component enters into a data use agreement with the intended recipient of the limited data set.

(see County HIPAA Guidelines #30 and forms/templates)



How Do We “Limit” Data?

To create a limited data set, the following direct identifier of the patient or of relatives, employers or household members of the patient must be removed:

- Names
- Postal address information, other than town, city, state and zip codes (unless the population is very low)
- Telephone numbers
- Fax numbers
- Electronic mail addresses



How Do We “Limit” Data? (con’t.)

- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
 - Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers.



How Do We “Limit” Data? (con’t.)

- Device identifiers and serial numbers
- Web Universal Resource Locators (URLS)
 - Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographs and comparable images.

NOTE: The “minimum necessary” rule applies.



Authorized Disclosures

In addition to permitted and required disclosures, a health care component may disclose other protected health information that has been expressly authorized by the client.

However, such an authorization *must* be provided through a County approved “HIPAA-ized” authorization form. Such forms are posted in the County’s HIPAA Public Folder and are also maintained by each health care component’s Privacy Coordinator.

Only use County approved HIPAA forms for this purpose.



Mitigation

What if a disclosure is made that does not comply with these guidelines?

A health care component must mitigate, to the extent practicable, any harmful effect that is known to the health care component of a use or disclosure of PHI in violation of the HIPAA Privacy Regulations and our County Privacy Policy & Procedures (and guidelines).

Advise your Supervisor, the Department's Privacy Coordinator and the County Compliance Officer of such events.



Privacy Incident Report

County health care and other designated departments must investigate the cause of an improper use or disclosure of PHI, and must notify the County Compliance Officer.

- Staff members shall report any incident of improper use or disclosure of PHI to their Supervisor.
- Supervisors, in coordination with their departments Privacy Coordinator, shall complete a Privacy Incident Report. (*See Privacy Form-14.*)
- The Privacy Coordinator shall provide a copy of the Privacy Incident Report to the County Compliance Officer, who will assist the department with their investigation and mitigation efforts.



Remember ...

- The HIPAA Privacy Regulations create a minimum level of protection. Other State and/or federal laws may have more stringent requirements.
 - Where HIPAA requires an authorization, only a County approved authorization form may be used.
 - If a Department chooses to obtain written consent even where HIPAA does *not* require an authorization (such as for TPO), such forms and procedures must be approved by the Department and the County.



And last but not least

If you have any questions regarding the HIPAA Privacy Regulations, the County's Privacy Policy & Procedures and corresponding guidelines and forms, or about privacy protections in general

Contact :

Your Supervisor,

Your Department's Privacy Coordinator

and/or

the County Compliance Officer.

The End

