Using & Disclosing Protected Health Information (PHI)

Jill Moore, JD, MPH, UNC School of Government
May 2018

Introduction

One of the most frequently asked questions about HIPAA is whether it permits the use or disclosure of protected health information (PHI) in a particular situation. Answering the question requires familiarity with the use and disclosure provisions of the HIPAA Privacy Rule—but there are multiple use and disclosure provisions. So, it is important to be able to figure out which provision applies to the particular use or disclosure in question.

The primary purpose of this document is to help readers learn how to find the right use or disclosure rule for different situations.

The document begins with some foundational information that is necessary to understanding the use and disclosure rules. It's important to know how HIPAA defines certain words, such as PHI, so the document begins with definitions of key terms. It then summarizes two HIPAA rules that must always be kept in mind when disclosing PHI: the Minimum Necessary Standard, and the Verification Standard.

To determine which use or disclosure provision applies to a particular question, it's useful to have an analytical framework. This document introduces a framework that focuses on three questions, which I call the 3 Ws, for what, who and why. It then summarizes the HIPAA use and disclosure rules.

Locating the appropriate HIPAA rule is an important first step in answering use or disclosure questions, but sometimes other confidentiality laws must be taken into account, in addition to HIPAA. Therefore, this document concludes with a brief summary of other laws that may affect a local health department's use or disclosure of PHI.

The document is organized into the following sections:

- **Definitions.** This section reviews HIPAA terminology that must be understood to apply the use and disclosure rules correctly.
- **HIPAA Standards Affecting Most Disclosures.** This section addresses the Minimum Necessary Standard and the Verification Standard.
- **Analyzing Use and Disclosure Questions**. This section provides an analytical framework to help you find the appropriate rule to answer a use or disclosure question.
- **Summary of the Use and Disclosure Rules**. This section briefly summarizes HIPAA's use and disclosure rules.
- **Other Laws that May Affect Use or Disclosure.** This section briefly describes several other laws that may affect use or disclosure of PHI

Definitions of Key Terms

This section describes five key terms that are important to understanding all of the use and disclosure rules. HIPAA defines many more terms, including some that are relevant to particular uses or disclosures, but these five can be considered a core HIPAA vocabulary because they appear in many different HIPAA provisions. Please note that these descriptions summarize the definitions; they do not repeat them verbatim. The complete definitions can be found in the HIPAA regulations.[1]

Protected health information (PHI): Individually identifiable information or records that a covered entity has in any form (paper, electronic, spoken), that relates to any one or more of the following:

- An individual's mental or physical health status or condition,
- Provision of health care to an individual, or
- Payment for the provision of health care to an individual.

Information is individually identifiable if it specifically identifies an individual, or if it could be used in conjunction with other available information to identify an individual.

There are three exceptions to this definition. Individually identifiable health information is not considered PHI if any of the following apply:

- The information is about a student and is covered by FERPA, the Family Educational Rights and Privacy Act. The confidentiality of this information is protected by FERPA rather than HIPAA.
- The information is about an employee and is maintained by the covered entity in its capacity as an employer. In North Carolina local health departments, the confidentiality of this information is protected by a state law rather than HIPAA.[2]
- The information pertains to a person who has been deceased for more than 50 years. This means that a deceased person's individually identifiable information *is* considered PHI that is protected by HIPAA for the first 50 years after death.

Individual: A person who is the subject of protected health information. In other words, the patient or client that the PHI is about.

Many of the use and disclosure rules refer to the individual. For example, if a particular disclosure requires written authorization, usually the individual is the person who must provide written authorization. The individual is also the person who ordinarily may exercise the right of access to the individual's PHI.

Personal representative: A person who is legally authorized to make health care decisions for an individual who is unable to make those decisions for him or herself, such as the parent of a minor child,[3] or a person who has health care power of attorney for an incapacitated adult. When an individual is

[1] 45 C.F.R. 160.103 (definitions of protected health information, individual, use, and disclosure); 164.502(g) (description of personal representative).
[2] For most local health department employees, the applicable confidentiality law is G.S. 153A-98.
[3] The parent should not be treated as the personal representative when a minor consents to health care under G.S. 90-21.5 (minor's consent law).

unable to make his or her own health care decisions, the individual's personal representative is the person to look to when a HIPAA use or disclosure rule requires some action by the individual. For example, if a particular disclosure requires a written authorization form, the personal representative should sign it on behalf of the individual.

Use: The sharing, employment, application, utilization, or analysis of PHI within the entity that maintains the PHI.

Disclosure: The release, transfer, provision of access to, or otherwise divulging PHI outside the entity holding the PHI.

The rule-of-thumb distinction between use and disclosure is that *use* refers to sharing or using PHI within the HIPAA-covered parts of an entity, and *disclosure* refers to releasing information outside the HIPAA-covered parts of the entity.

HIPAA Standards Affecting Disclosures

Minimum Necessary Standard

The Minimum Necessary Standard requires covered entities to assure that uses and disclosures of PHI are limited to the minimum that is needed to accomplish the purpose of the particular use or disclosure. When requesting PHI from another covered entity, a covered entity must limit its request to the PHI that is reasonably necessary to accomplish the purpose for which the request is made. 45 C.F.R. 164.502(b); 164.514(d).

The Minimum Necessary Standard does not apply to any of the following uses or disclosures:

- Disclosures to or requests by a health care provider for treatment purposes;
- Uses or disclosures made to the individual who is the subject of the PHI;
- Uses or disclosures made pursuant to a written authorization that complies with the HIPAA authorization rule;
- Uses or disclosures that are required by law;
- Disclosures made to the US Department of Health and Human Services for compliance or enforcement purposes; and
- Uses or disclosures that are required for compliance with the requirements of the privacy rule.

The standard is meant to be flexible to accommodate the different needs of different covered entities, so it does not prescribe the specific practices that a local health department may need to have. Instead, it sets out general methods for assuring uses, disclosures, and requests for PHI are limited to the minimum necessary.

To limit uses of PHI to the minimum necessary, a covered entity must:

- Identify the persons (or classes of persons) in its workforce who need access to PHI to carry out their duties;
- Identify the categories of PHI each person (or class of persons) needs access to, and any conditions appropriate to such access; and
- Make reasonable efforts to limit workforce members' access to PHI in accordance with the above determinations.

To limit disclosures of PHI to the minimum necessary, a covered entity must:

- Determine which disclosures of PHI it makes on a routine and recurring basis, and develop policies and procedures addressing those disclosures. The policies and procedures can be in the form of standard protocols that limit the PHI disclosed to the amount that is reasonably necessary to achieve the purpose of the disclosure. An example of a disclosure in this category would be disclosures of PHI to health insurers to obtain reimbursement for services provided by the LHD. This is a disclosure for a payment purpose.
- For all other disclosures, the covered entity must develop criteria designed to limit the PHI disclosed to that which is reasonably necessary to accomplish the purpose for which PHI is sought, and review requests for disclosure on an individual basis in accordance with the criteria.

An example of a disclosure in this category would be a disclosure of PHI to a law enforcement officer to assist in locating a missing person.

A covered entity may rely on a requested disclosure as the minimum necessary for the stated purpose in any of the following circumstances:

- When making disclosures to public officials that are permitted under section 164.512 of the HIPAA Privacy Rule, if the public official represents that the information requested is the minimum necessary for the stated purpose.[4]
- When the information is requested by another covered entity.
- When the information is requested by a professional who is either a member of its workforce or a business associate, if the request for disclosure is for the purpose of providing professional services to the covered entity, and the professional represents that the information requested is the minimum necessary for the stated purpose.
- When the disclosure is for research purposes, and the person requesting the disclosure has provided documentation or representations that comply with the requirements of 45 C.F.R. 164.512(i) (the section of the Privacy Rule that addresses disclosures for research).

To limit requests for PHI to the minimum necessary, a covered entity must:

- Determine which requests for PHI it makes on a routine and recurring basis, and implement policies and procedures regarding those requests. The policies and procedures can be in the form of standard protocols that limit the PHI requested to the amount that is reasonably necessary to achieve the purpose of the disclosure.
- For all other requests, the covered entity must develop criteria designed to limit the PHI that is requested to that reasonably necessary to accomplish the purpose for which PHI is sought, and review requests on an individual basis in accordance with the criteria.

Finally, the Minimum Necessary Standard addresses uses, disclosures, and requests for entire medical records. If the standard applies to a particular use, disclosure, or request for PHI, a covered entity may not use, disclose, or request the entire medical record. Note that this is the rule *only if* the minimum necessary standard applies. The minimum necessary standard *does not apply* to every use, disclosure, or request for an entire medical record. For example, it does not apply to a request by a health care provider for treatment purposes – the entire record may be requested or disclosed in that circumstance.

Even if the minimum necessary standard applies, the covered entity may use, disclose, or request the entire medical record if it specifically justifies that the entire record is the amount of PHI that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

[4] The summaries of HIPAA's use and disclosure rules that appear later in this document identify the disclosures that fall under section 164.512.

Verification Standard

The HIPAA Privacy Rule requires covered entities to verify the identity of a person to whom protected health information is to be disclosed, as well as the person's legal authority to receive the PHI. 45 C.F.R. § 164.514(h). The verification requirement does not apply to uses of PHI, but it applies to most disclosures, with just a few exceptions.

A covered entity is not required to verify a person's identity or authority in the following circumstances:

- When the disclosure is of PHI from a facility directory, such as a hospital's directory of patient names and room numbers, and is limited to what is authorized by the facility directory provisions in 45 CFR 164.510(a).
- When the disclosure is to a person who is involved in an individual's health care, such as a friend or family member, and the disclosure is made in accordance with the provisions of 45 CFR 164.510(b).
- When the disclosure is for the purpose of notifying a person responsible for an individual's care of the individual's location, condition, or death, and the notification is made in accordance with 45 CFR 164.510(b).
- When the disclosure is made in order to avert a serious threat to the health or safety of a person or the public and the covered entity complies with the provisions of 45 CFR 164.512(j) in making the disclosure.

The HIPAA Privacy Rule does not include specific requirements for how verification should be done. However, it does provide guidance for how to verify the identity and authority of one category of people who may request PHI – public officials. Examples of public officials who may request PHI include employees of the department of social services, law enforcement officers, or the employees of other public health agencies.

To verify a public official's identify:

- If the request is made in person, identity may be verified by the person presenting an agency identification badge, other official credentials, or other proof of government status.
- If the request is in writing, the request should be on the appropriate government letterhead.

A public official's legal authority may be verified by either of two things:

- A written statement[5] of the legal authority under which the information is requested; or
- A subpoena, warrant, order, or other legal process that has been issued by a grand jury or a judicial or administrative tribunal.

Please note that the documents described above are sufficient to verify a public official's identity and legal authority, but they ***do not authorize the covered entity to turn over protected health information***. Before disclosing PHI, the covered entity must still ensure that the specific disclosure the public official is requesting is allowed by the HIPAA Privacy Rule, and that any additional requirements that are imposed on the disclosure by HIPAA or another law are satisfied.

[5] An oral statement is sufficient if a written statement is impracticable.

Analyzing Use & Disclosure Questions to Find the Appropriate Rule

The HIPAA use and disclosure rules govern whether and how protected health information may be *used* (shared, employed, utilized, or analyzed) or *disclosed* (released, transferred, provided for access, or otherwise divulged). But HIPAA doesn't have *one* use & disclosure rule; it has many. How do you know which rule applies to a particular use or disclosure? The answer depends in large part on three questions, that I call the three Ws, for what, who, and why.

What: What specific information will be used or disclosed? Is it protected health information (PHI) that is covered by HIPAA? If so, is it subject to additional confidentiality requirements, such as the those protecting information about individuals with communicable diseases? If it isn't covered by HIPAA, is it subject to some other law, such as FERPA, the law that protects student records?

Who: Who will the information be shared with as a result of the use or disclosure? For example, different rules apply if the recipient is a health care provider, versus a law enforcement officer.

Why: Why is the information being used or disclosed? Or in other words, what is the purpose of the use or disclosure?

The *why* question is particularly important because it gets to purpose, and the use and disclosure provisions of the HIPAA Privacy Rule are largely purpose-driven. There are different rules addressing different purposes, so knowing the purpose of a particular use or disclosure is important to finding the right rule to apply. For example, if a use or disclosure of PHI is for the treatment of an individual, there's a specific rule that applies, and it is designed to allow information to flow fairly freely, in order to better support individual's health care. On the other hand, if the purpose of a disclosure is to provide medical records for a court proceeding, there's a different rule that applies, and it is considerably more restrictive, allowing the disclosure only after particular steps are taken to ensure patient confidentiality is protected.

The *who* question can also help you identify purpose. For example, if the recipient of the disclosure is a law enforcement officer, then it's likely the disclosure is for law enforcement purposes, which has its own section in the HIPAA use and disclosure rules.

The *what* question is mostly useful to determining which laws will answer your use or disclosure question—whether it will be HIPAA alone, HIPAA plus another law, or if the information is not PHI, some other law.

Summary of HIPAA's Use and Disclosure Rules

This section provides a very brief summary of the HIPAA use and disclosure rules. It does not address the nuances of each rule. Please use the citations that are provided to find the full text of the rule.

Required Disclosures (45 C.F.R. § 164.502(a))

There are only two categories of disclosures that are required by HIPAA.

Disclosures to the individual. A covered entity must disclose PHI to an individual who requests PHI as part of exercising either of the following individual rights:

- Right of access (45 C.F.R. 164.524) – An individual has a right to view and obtain a copy of the individual's PHI, and may use the right of access to direct disclosure of the individual's PHI to a third party.[6]
- Right to an accounting of disclosures (45 C.F.R. 164.528) – An individual has a right to receive an accounting of most disclosures of PHI made by a covered entity over the six year period preceding the individual's request.

Disclosures to the federal agency responsible for HIPAA compliance and enforcement actions – A covered entity must disclose PHI to the federal Office for Civil Rights (OCR), the HIPAA enforcement agency, when that office requires the information as part of a compliance or enforcement action.

These are the only disclosures that HIPAA requires, but be aware that there are other laws that sometimes require disclosures, especially state laws.

Disclosures for Treatment, Payment, or Health Care Operations (45 C.F.R. 164.506)

A covered entity may use or disclose PHI for purposes of treatment, payment, or health care operations (TPO). The terms treatment, payment, and health care operations have specific definitions in the HIPAA regulations. *Treatment* generally refers to health care services and activities to arrange health care services. It includes the provision, coordination, or management of health care related services by health care providers; including consultation and referrals. *Payment* refers to activities to obtain or provide reimbursement for health care, including billing, claims submission, collection activities, and more that are specified in the full definition. *Health care operations* refers generally to the activities of a covered entity that are related to its covered functions. This includes a wide range of activities, from quality assurance and performance evaluation, to audits and business planning. This category also includes case management and care coordination.

A covered entity may use or disclose PHI for its own TPO purposes, and sometimes may disclose PHI for another covered entity's TPO purposes as well. See the rule for details.

[6] The right of access is substantial and complicated. The U.S. Department of Health and Human Services' Office for Civil Rights (OCR), which enforces the HIPAA Privacy Rule, has provided important guidance on this right. *See* Individuals' Right Under HIPAA to Access Their Health Information, at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (accessed May 4, 2018).

The minimum necessary standard does not apply to uses or disclosures for treatment purposes, but it does apply to disclosures for payment purposes or for health care operations.

The verification standard applies to TPO disclosures. This means that if the covered entity discloses PHI for treatment purposes, it must verify the identity and authority of the recipient. However, remember that a covered entity is not required to ask for proof of identity or authority if it is already known to the covered entity. For example, if a LHD already knows that the recipient of the PHI is a health care provider who needs or has requested the information for treatment purposes, and also knows that this disclosure is allowed under HIPAA, there is no need for further action to verify identity and authority.

HIPAA does not require a covered entity to get an individual to sign a written authorization or any other form of release before using or disclosing PHI for treatment, payment, or health care operations purposes, so long as use or disclosure is in accordance with the specific rules for those disclosure types. (There is a very limited exception: HIPAA requires the individual's written authorization is required to use or disclose psychotherapy notes for TPO purposes.) However, consent or some other form of release may still be required if another law requires it for a particular program or a particular type of information, or if a covered entity chooses to require releases to be signed for TPO disclosures.

Disclosures that Require the Individual's Written Authorization (45 C.F.R. 164.508)

HIPAA requires the individual's written authorization for:

- Uses or disclosures of psychotherapy notes;[7]
- Uses or disclosures of PHI to market a health care product or service to the individual; or
- Any other use or disclosure that isn't otherwise permitted or required by the HIPAA Privacy Rule.

When a use or disclosure of PHI requires authorization, the authorization must be provided in writing on a HIPAA-compliant form. To be HIPAA-compliant, the form must include elements that are specified in the Privacy Rule. In brief, the form must include:

- A specific and meaningful description of the PHI that is to be used or disclosed.
- The name or other specific identification of the person requesting the use or disclosure.
- The name or other specific identification of the person or entity that will receive the PHI.
- A description of the purpose of the use or disclosure.
- An expiration date or event.

[7] The term "psychotherapy notes" does not encompass all mental health records or information. Rather, it refers only to a specific type of notes a mental health professional takes during a therapy session and keeps separate from the medical record. HIPAA defines "psychotherapy notes" as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of an individual's record." The definition specifically excludes "medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." 45 C.F.R. 164.501.

- A statement regarding the individual's right to revoke the authorization.
- A statement about whether the covered entity is permitted to condition treatment or benefits on the individual's agreement to sign an authorization.
- Notice that the authorization does not protect against redisclosure of PHI by the recipient of the information.
- The individual's signature. If a personal representative signs on behalf of an individual, the form should also include a brief description of what makes the person a personal representative.

The minimum necessary standard does not apply to disclosures made pursuant to an authorization. Instead, the authorization itself prescribes the amount of PHI that may be disclosed.

The verification standard does apply to disclosures made pursuant to an authorization. The identity and authority of the person requesting the disclosure must be verified, unless it is already known.

Disclosures that Require the Individual to Have Opportunity to Agree or Object (45 C.F.R. 164.510)

This HIPAA provision addresses disclosures that are permitted without written authorization, but ordinarily the individual must have an opportunity to agree or object to the disclosure. There are three types of disclosures in this category:

Disclosures for facility directories – A covered health care provider may maintain a directory that includes patients' names, their location in the facility, a statement about a patient's condition in general terms, such as "good" or "stable," and their religious affiliation. The directory information may be disclosed to people who inquire about the person by name, or to clergy members. A health care provider that maintains a directory must notify individuals that it has a directory, what PHI may be included, and to whom information may be disclosed. The individual must be given an opportunity to restrict or prohibit some or all directory uses or disclosures. This is a provision that is intended primarily for inpatient facilities. It is unlikely to apply to local health departments.

Disclosures to family members or others involved in the individual's care – A covered entity may disclose PHI to a family member, friend, or other person who is involved in an individual's health care. The entity must obtain the individual's express agreement for the disclosure, or give the individual an opportunity to object, or infer that the individual does not object, if that inference is reasonable under the particular circumstances.

Disclosures for emergency notification – A covered entity may disclose PHI to notify a family member or personal representative of an individual's location, general condition, or death. The disclosure may be made directly to the family member or personal representative, or to a disaster relief entity that then notifies the family member or personal representative. The individual ordinarily must be given an opportunity to object to this disclosure, but there is an exception if it is impracticable due to the individual's incapacity or an emergency circumstance.

The minimum necessary standard applies to these disclosures. A covered entity must limit these types of disclosures to the minimum amount of PHI that is necessary to accomplish the purpose of the disclosure.

All of these disclosures fall under an exception to the HIPAA verification standard. A covered entity that makes one of these disclosures is not required to verify the identity or authority of the person to whom the PHI is disclosed.

Disclosures for Public Interest or Public Benefit (45 C.F.R. 164.512)

This section of the HIPAA Privacy Rule is actually titled, "Uses or disclosures for which an authorization or opportunity to agree or object is not required." It addresses a number of types of uses and disclosures that HIPAA allows to be made without the individual's permission, in order to support other important goals and purposes. These are sometimes described as the public interest or public benefit disclosures.

This section of the Privacy Rule addresses uses and disclosures for a wide variety of purposes, including:

- Uses and disclosures required by law – 45 C.F.R. 164.512(a)
- Uses and disclosures for public health purposes – 45 C.F.R. 164.512(b)
- Disclosures about victims of abuse, neglect, or domestic violence – 45 C.F.R. 164.512(c)
- Uses and disclosures for health oversight activities – 45 C.F.R. 164.512(d)
- Disclosures for judicial and administrative proceedings – 45 C.F.R. 164.512(e)
- Disclosures for law enforcement purposes – 45 C.F.R. 164.512(f)
- Uses and disclosures about decedents – 45 C.F.R. 164.512(g)
- Uses and disclosures for cadaveric organ, eye, or tissue donation purposes – 45 C.F.R. 164.512(h)
- Uses and disclosures for research purposes – 45 C.F.R. 164.512(i)
- Uses and disclosures to avert a serious threat to health or safety – 45 C.F.R. 164.512(j)
- Uses and disclosures for specialized government functions – 45 C.F.R. 164.512(k)
- Disclosures for workers' compensation – 45 C.F.R. 164.512(l)

Each of these purposes is addressed extensively in the HIPAA Privacy Rule. Many include multiple categories of sub-purposes for which information may be used or disclosed, and many impose substantial conditions on use or disclosure. I have not attempted to summarize those details here. It is imperative to consult the rule and your agency's policies and procedures before making a disclosure under one of these provisions.

The minimum necessary standard applies to all of these categories except uses and disclosures that are required by law.

The verification standard applies to all of these categories except uses and disclosures to avert a serious threat to health or safety.

Other Laws that May Affect Use or Disclosure

HIPAA provides the baseline for determining whether a particular use or disclosure is allowed. Additional confidentiality laws may apply to particular programs, services, or types of information. As a general rule, whichever law is stricter—whether it's HIPAA or the other law—will control whether or to what extent a particular use or disclosure can be made. A LHD should determine which confidentiality laws apply to the LHD's programs or services and ensure that the LHD's use and disclosure policies take them into account.

Three categories of information that LHDs may have in their records, and that are affected by laws limiting disclosures, are individually identifiable communicable disease information, information about clients of family planning programs, and information about clients of behavioral health services.

Communicable disease: Information that identifies a person who has or may have a reportable communicable disease is subject to a state law that limits some disclosures that HIPAA allows. G.S. 130A-143.

Family planning programs: Information about a person who is a client of a Title X-funded family planning program is subject to a federal regulation that requires documented consent for most disclosures. In North Carolina, LHDs use a consent form for family planning[8] that specifies further the limits on disclosure of information, and must comply with the terms of the consent form. 42 C.F.R. 59.11.

Behavioral health programs: Information from these programs may be subject to state mental health confidentiality laws (G.S. Chapter 122C) or federal substance abuse program confidentiality regulations (42 C.F.R. Part 2). The confidentiality requirements of G.S. Chapter 122C apply to information created or maintained in connection with particular types of services—specifically, those that have the *primary* purpose of providing treatment or other care related to mental health, developmental disabilities, or substance abuse. The requirements do not apply to mental health information that may be acquired as part of a service that has a different primary purpose, such as primary care. Similarly, the confidentiality requirements of 42 C.F.R. Part 2 apply to particular types of programs—specifically, federally-assisted substance abuse programs. The requirements do not apply to substance abuse information that may be acquired as part of a service that is not a federally-assisted substance abuse program.

[8] DHHS Form 4112, Family Planning General Consent for Services, last reviewed 02/2018. Available from the North Carolina Department of Health and Human Services, Division of Public Health, Women's and Children's Health Section, Family Planning and Reproductive Health Unit.