HIPAA Privacy Rule and Sharing Information Related to Mental Health

Background

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides consumers with important privacy rights and protections with respect to their health information, including important controls over how their health information is used and disclosed by health plans and health care providers. Ensuring strong privacy protections is critical to maintaining individuals' trust in their health care providers and willingness to obtain needed health care services, and these protections are especially important where very sensitive information is concerned, such as mental health information. At the same time, the Privacy Rule recognizes circumstances arise where health information may need to be shared to ensure the patient receives the best treatment and for other important purposes, such as for the health and safety of the patient or others. The Rule is carefully balanced to allow uses and disclosures of information—including mental health information—for treatment and these other purposes with appropriate protections.

In this guidance, we address some of the more frequently asked questions about when it is appropriate under the Privacy Rule for a health care provider to share the protected health information of a patient who is being treated for a mental health condition. We clarify when HIPAA permits health care providers to:

-
  - Communicate with a patient's family members, friends, or others involved in the patient's care;
  - Communicate with family members when the patient is an adult;
  - Communicate with the parent of a patient who is a minor;
  - Consider the patient's capacity to agree or object to the sharing of their information;
  - Involve a patient's family members, friends, or others in dealing with patient failures to adhere to medication or other therapy;
  - Listen to family members about their loved ones receiving mental health treatment;
  - Communicate with family members, law enforcement, or others when the patient presents a serious and imminent threat of harm to self or others; and

- Communicate to law enforcement about the release of a patient brought in for an emergency psychiatric hold.

In addition, the guidance provides relevant reminders about related issues, such as the heightened protections afforded to psychotherapy notes by the Privacy Rule, a parent's right to access the protected health information of a minor child as the child's personal representative, the potential applicability of Federal alcohol and drug abuse confidentiality regulations or state laws that may provide more stringent protections for the information than HIPAA, and the intersection of HIPAA and FERPA in a school setting.

Questions and Answers about HIPAA and Mental Health

Does HIPAA allow a health care provider to communicate with a patient's family, friends, or other persons who are involved in the patient's care?

Yes. In recognition of the integral role that family and friends play in a patient's health care, the HIPAA Privacy Rule allows these routine – and often critical – communications between health care providers and these persons. Where a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient's family members, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. See 45 CFR 164.510(b). The provider may ask the patient's permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. A common example of the latter would be situations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the provider when a disclosure is made.

Where a patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others involved in the patient's care or payment for care, as long as the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. Note that, when someone other than a friend or family member is involved, the health care provider

must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.

In all cases, disclosures to family members, friends, or other persons involved in the patient's care or payment for care are to be limited to only the protected health information directly relevant to the person's involvement in the patient's care or payment for care.

OCR's website contains additional information about disclosures to family members and friends in fact sheets developed for consumers and providers.

Does HIPAA provide extra protections for mental health information compared with other health information?

Generally, the Privacy Rule applies uniformly to all protected health information, without regard to the type of information. One exception to this general rule is for psychotherapy notes, which receive special protections. The Privacy Rule defines psychotherapy notes as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record. Psychotherapy notes do not include any information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests; nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. Psychotherapy notes also do not include any information that is maintained in a patient's medical record. See 45 CFR 164.501.

Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes. Therefore, with few exceptions, the Privacy Rule requires a covered entity to obtain a patient's authorization prior to a disclosure of psychotherapy notes for any reason, including a disclosure for treatment purposes to a health care provider other than the originator of the notes. See 45 CFR 164.508(a)(2). A notable exception

exists for disclosures required by other law, such as for mandatory reporting of abuse, and mandatory "duty to warn" situations regarding threats of serious and imminent harm made by the patient (State laws vary as to whether such a warning is mandatory or permissible).

Is a health care provider permitted to discuss an adult patient's mental health information with the patient's parents or other family members?

In situations where the patient is given the opportunity and does not object, HIPAA allows the provider to share or discuss the patient's mental health information with family members or other persons involved in the patient's care or payment for care. For example, if the patient does not object:

- A psychiatrist may discuss the drugs a patient needs to take with the patient's sister who is present with the patient at a mental health care appointment.
- A therapist may give information to a patient's spouse about warning signs that may signal a developing emergency.

BUT:

- A nurse may not discuss a patient's mental health condition with the patient's brother after the patient has stated she does not want her family to know about her condition.

In all cases, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care. See 45 CFR 164.510(b). Finally, it is important to remember that other applicable law (e.g., State confidentiality statutes) or professional ethics may impose stricter limitations on sharing personal health information, particularly where the information relates to a patient's mental health.

When does mental illness or another mental condition constitute incapacity under the Privacy Rule? For example, what if a patient who is experiencing temporary psychosis or is intoxicated does

not have the capacity to agree or object to a health care provider sharing information with a family member, but the provider believes the disclosure is in the patient's best interests?

Section 164.510(b)(3) of the HIPAA Privacy Rule permits a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient's information to the patient's family, friends, or other persons involved in the patient's care or payment for care, is in the best interests of the patient.[1]Where a provider determines that such a disclosure is in the patient's best interests, the provider would be permitted to disclose only the PHI that is directly relevant to the person's involvement in the patient's care or payment for care.

This permission clearly applies where a patient is unconscious. However, there may be additional situations in which a health care provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to the sharing of personal health information at a particular time and that sharing the information is in the best interests of the patient at that time. These may include circumstances in which a patient is suffering from temporary psychosis or is under the influence of drugs or alcohol. If, for example, the provider believes the patient cannot meaningfully agree or object to the sharing of the patient's information with family, friends, or other persons involved in their care due to her current mental state, the provider is allowed to discuss the patient's condition or treatment with a family member, if the provider believes it would be in the patient's best interests. In making this determination about the patient's best interests, the provider should take into account the patient's prior expressed preferences regarding disclosures of their information, if any, as well as the circumstances of the current situation. Once the patient regains the capacity to make these choices for herself, the provider should offer the patient the opportunity to agree or object to any future sharing of her information.

If a health care provider knows that a patient with a serious mental illness has stopped taking a prescribed medication, can the provider tell the patient's family members?

So long as the patient does not object, HIPAA allows the provider to share or discuss a patient's mental health information with the patient's family members. See 45 CFR 164.510(b). If the provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to sharing the information at that time, and that sharing the information would be in the patient's best interests, the provider may tell the patient's family member. In either case, the health care provider may share or discuss only the information that the family member involved needs to know about the patient's care or payment for care.

Otherwise, if the patient has capacity and objects to the provider sharing information with the patient's family member, the provider may only share the information if doing so is consistent with applicable law and standards of ethical conduct, and the provider has a good faith belief that the patient poses a threat to the health or safety of the patient or others, and the family member is reasonably able to prevent or lessen that threat. See 45 CFR 164.512(j). For example, if a doctor knows from experience that, when a patient's medication is not at a therapeutic level, the patient is at high risk of committing suicide, the doctor may believe in good faith that disclosure is necessary to prevent or lessen the threat of harm to the health or safety of the patient who has stopped taking the prescribed medication, and may share information with the patient's family or other caregivers who can avert the threat. However, absent a good faith belief that the disclosure is necessary to prevent a serious and imminent threat to the health or safety of the patient or others, the doctor must respect the wishes of the patient with respect to the disclosure.

Can a minor child's doctor talk to the child's parent about the patient's mental health status and needs?

With respect to general treatment situations, a parent, guardian, or other person acting in loco parentis usually is the personal representative of the minor child, and a health care provider is permitted to share patient information with a patient's personal representative under the Privacy Rule. However, section 164.502(g) of the Privacy Rule contains several important exceptions to this general rule. A parent is not treated as a minor child's personal representative when: (1) State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, the minor consents to the health

care service, and the minor child has not requested the parent be treated as a personal representative; (2) someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent; or (3) a parent agrees to a confidential relationship between the minor and a health care provider with respect to the health care service.[2] For example, if State law provides an adolescent the right to obtain mental health treatment without parental consent, and the adolescent consents to such treatment, the parent would not be the personal representative of the adolescent with respect to that mental health treatment information.

Regardless, however, of whether the parent is otherwise considered a personal representative, the Privacy Rule defers to State or other applicable laws that expressly address the ability of the parent to obtain health information about the minor child. In doing so, the Privacy Rule permits a covered entity to disclose to a parent, or provide the parent with access to, a minor child's protected health information when and to the extent it is permitted or required by State or other laws (including relevant case law). Likewise, the Privacy Rule prohibits a covered entity from disclosing a minor child's protected health information to a parent when and to the extent it is prohibited under State or other laws (including relevant case law). See 45 CFR 164.502(g)(3)(ii).

In cases in which State or other applicable law is silent concerning disclosing a minor's protected health information to a parent, and the parent is not the personal representative of the minor child based on one of the exceptional circumstances described above, a covered entity has discretion to provide or deny a parent access to the minor's health information, if doing so is consistent with State or other applicable law, and the decision is made by a licensed health care professional in the exercise of professional judgment. For more information about personal representatives under the Privacy Rule, see OCR's guidance for consumers and providers.

In situations where a minor patient is being treated for a mental health disorder and a substance abuse disorder, additional laws may be applicable. The Federal confidentiality statute and regulations that apply to federally-funded drug and alcohol abuse treatment programs contain provisions that are more stringent than HIPAA. See 42 USC § 290dd–2; 42 CFR 2.11, et. seq.

At what age of a child is the parent no longer the personal representative of the child for HIPAA purposes?

HIPAA defers to state law to determine the age of majority and the rights of parents to act for a child in making health care decisions, and thus, the ability of the parent to act as the personal representative of the child for HIPAA purposes. See 45 CFR 164.502(g).

Does a parent have a right to receive a copy of psychotherapy notes about a child's mental health treatment?

No. The Privacy Rule distinguishes between mental health information in a mental health professional's private notes and that contained in the medical record. It does not provide a right of access to psychotherapy notes, which the Privacy Rule defines as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record. See 45 CFR 164.501. Psychotherapy notes are primarily for personal use by the treating professional and generally are not disclosed for other purposes. Thus, the Privacy Rule includes an exception to an individual's (or personal representative's) right of access for psychotherapy notes. See 45 CFR 164.524(a)(1)(i).

However, parents generally are the personal representatives of their minor child and, as such, are able to receive a copy of their child's mental health information contained in the medical record, including information about diagnosis, symptoms, treatment plans, etc. Further, although the Privacy Rule does not provide a right for a patient or personal representative to access psychotherapy notes regarding the patient, HIPAA generally gives providers discretion to disclose the individual's own protected health information (including psychotherapy notes) directly to the individual or the individual's personal representative. As any such disclosure is purely permissive under the Privacy Rule, mental health providers should consult applicable State law for any prohibitions or conditions before making such disclosures.

What options do family members of an adult patient with mental illness have if they are concerned about the patient's mental health

and the patient refuses to agree to let a health care provider share information with the family?

The HIPAA Privacy Rule permits a health care provider to disclose information to the family members of an adult patient who has capacity and indicates that he or she does not want the disclosure made, only to the extent that the provider perceives a serious and imminent threat to the health or safety of the patient or others and the family members are in a position to lessen the threat. Otherwise, under HIPAA, the provider must respect the wishes of the adult patient who objects to the disclosure. However, HIPAA in no way prevents health care providers from listening to family members or other caregivers who may have concerns about the health and well-being of the patient, so the health care provider can factor that information into the patient's care.

In the event that the patient later requests access to the health record, any information disclosed to the provider by another person who is not a health care provider that was given under a promise of confidentiality (such as that shared by a concerned family member), may be withheld from the patient if the disclosure would be reasonably likely to reveal the source of the information. 45 CFR 164.524(a)(2)(v). This exception to the patient's right of access to protected health information gives family members the ability to disclose relevant safety information with health care providers without fear of disrupting the family's relationship with the patient.

Does HIPAA permit a doctor to contact a patient's family or law enforcement if the doctor believes that the patient might hurt herself or someone else?

Yes. The Privacy Rule permits a health care provider to disclose necessary information about a patient to law enforcement, family members of the patient, or other persons, when the provider believes the patient presents a serious and imminent threat to self or others. The scope of this permission is described in a letter to the nation's health care providers issued on January 15, 2013, and below.

Specifically, when a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, the Privacy Rule allows the provider, consistent with applicable law and standards of

ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat. These provisions may be found in the Privacy Rule at 45 CFR § 164.512(j).

Under these provisions, a health care provider may disclose patient information, including information from mental health records, if necessary, to law enforcement, family members of the patient, or any other persons who may reasonably be able to prevent or lessen the risk of harm. For example, if a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, HIPAA permits the mental health professional to alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat.

In addition to professional ethical standards, most States have laws and/or court decisions which address, and in many instances require, disclosure of patient information to prevent or lessen the risk of harm. Providers should consult the laws applicable to their profession in the States where they practice, as well as 42 USC 290dd-2 and 42 CFR Part 2 under Federal law (governing the disclosure of alcohol and drug abuse treatment records) to understand their duties and authority in situations where they have information indicating a threat to public safety. Note that, where a provider is not subject to such State laws or other ethical standards, the HIPAA permission still would allow disclosures for these purposes to the extent the other conditions of the permission are met.

If a law enforcement officer brings a patient to a hospital or other mental health facility to be placed on a temporary psychiatric hold, and requests to be notified if or when the patient is released, can the facility make that notification?

The Privacy Rule permits a HIPAA covered entity, such as a hospital, to disclose certain protected health information, including the date and time of admission and discharge, in response to a law enforcement official's request, for the purpose of locating or identifying a suspect, fugitive, material witness, or missing person. See 45 CFR § 164.512(f)(2). Under this provision, a covered entity may disclose the following information about an individual: name and address; date and place of birth; social security number; blood type and rh factor; type of

injury; date and time of treatment (includes date and time of admission and discharge) or death; and a description of distinguishing physical characteristics (such as height and weight). However, a covered entity may not disclose any protected health information under this provision related to DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue. The law enforcement official's request may be made orally or in writing.

Other Privacy Rule provisions also may be relevant depending on the circumstances, such as where a law enforcement official is seeking information about a person who may not rise to the level of a suspect, fugitive, material witness, or missing person, or needs protected health information not permitted under the above provision. For example, the Privacy Rule's law enforcement provisions also permit a covered entity to respond to an administrative request from a law enforcement official, such as an investigative demand for a patient's protected health information, provided the administrative request includes or is accompanied by a written statement specifying that the information requested is relevant, specific and limited in scope, and that de-identified information would not suffice in that situation. The Rule also permits covered entities to respond to court orders and court-ordered warrants, and subpoenas and summonses issued by judicial officers. See 45 CFR § 164.512(f)(1). Further, to the extent that State law may require providers to make certain disclosures, the Privacy Rule would permit such disclosures of protected health information as "required-by-law" disclosures. See 45 CFR § 164.512(a).

Finally, the Privacy Rule permits a covered health care provider, such as a hospital, to disclose a patient's protected health information, consistent with applicable legal and ethical standards, to avert a serious and imminent threat to the health or safety of the patient or others. Such disclosures may be to law enforcement authorities or any other persons, such as family members, who are able to prevent or lessen the threat. See 45 CFR § 164.512(j).

If a doctor believes that a patient might hurt himself or herself or someone else, is it the duty of the provider to notify the family or law enforcement authorities?

A health care provider's "duty to warn" generally is derived from and defined by standards of ethical conduct and State laws and court

decisions such as Tarasoff v. Regents of the University of California. HIPAA permits a covered health care provider to notify a patient's family members of a serious and imminent threat to the health or safety of the patient or others if those family members are in a position to lessen or avert the threat. Thus, to the extent that a provider determines that there is a serious and imminent threat of a patient physically harming self or others, HIPAA would permit the provider to warn the appropriate person(s) of the threat, consistent with his or her professional ethical obligations and State law requirements. See 45 CFR 164.512(j). In addition, even where danger is not imminent, HIPAA permits a covered provider to communicate with a patient's family members, or others involved in the patient's care, to be on watch or ensure compliance with medication regimens, as long as the patient has been provided an opportunity to agree or object to the disclosure and no objection has been made. See 45 CFR 164.510(b)(2).

Does HIPAA prevent a school administrator, or a school doctor or nurse, from sharing concerns about a student's mental health with the student's parents or law enforcement authorities?

Student health information held by a school generally is subject to the Family Educational Rights and Privacy Act (FERPA), not HIPAA. HHS and the Department of Education have developed guidance clarifying the application of HIPAA and FERPA.

In the limited circumstances where the HIPAA Privacy Rule, and not FERPA, may apply to health information in the school setting, the Rule allows disclosures to parents of a minor patient or to law enforcement in various situations. For example, parents generally are presumed to be the personal representatives of their unemancipated minor child for HIPAA privacy purposes, such that covered entities may disclose the minor's protected health information to a parent. See 45 CFR § 164.502 (g)(3). In addition, disclosures to prevent or lessen serious and imminent threats to the health or safety of the patient or others are permitted for notification to those who are able to lessen the threat, including law enforcement, parents or others, as relevant. See 45 CFR § 164.512(j).

Notes

[1] The Privacy Rule permits, but does not require, providers to disclose information in these situations. Providers who are subject to more stringent privacy standards under other laws,

such as certain state confidentiality laws or 42 CFR Part 2, would need to consider whether there is a similar disclosure permission under those laws that would apply in the circumstances.

[2] A parent also may not be a personal representative if there are safety concerns. A provider may decide not to treat the parent as the minor's personal representative if the provider believes that the minor has been or may be subject to violence, abuse, or neglect by the parent or the minor may be endangered by treating the parent as the personal representative; and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the parent as the personal representative. See 45 CFR 164.502(g)(5).

Public Health

Background

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose protected health information without authorization for specified public health purposes. In addition, if a covered entity engages a business associate to assist in a specified public health activity, the business associate's written agreement with the covered entity should identify these activities, and the business associate may make the disclosure for public health reasons in accordance with its written agreement.

How the Rule Works

General Public Health Activities. The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. See 45 CFR 164.512(b)(1)(i). Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority. See 45 CFR 164.512(b)(1)(i). Covered entities who are also a public health authority may use, as well as disclose, protected health information for these public health purposes. See 45 CFR 164.512(b)(2).

A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is

responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA). Generally, covered entities are required reasonably to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, covered entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law. See 45 CFR 164.502(b).

For disclosures to a public health authority, covered entities may reasonably rely on a minimum necessary determination made by the public health authority in requesting the protected health information. See 45 CFR 164.514(d)(3)(iii)(A). For routine and recurring public health disclosures, covered entities may develop standard protocols, as part of their minimum necessary policies and procedures, that address the types and amount of protected health information that may be disclosed for such purposes. See 45 CFR 164.514(d)(3)(i).

Other Public Health Activities. The Privacy Rule recognizes the important role that persons or entities other than public health authorities play in certain essential public health activities. Accordingly, the Rule permits covered entities to disclose protected health information, without authorization, to such persons or entities for the public health activities discussed below.

- **Child abuse or neglect.** Covered entities may disclose protected health information to report known or suspected child abuse or neglect, if the report is made to a public health authority or other appropriate government authority that is authorized by law to receive such reports. For instance, the social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case, the Privacy Rule would permit a covered entity to report such cases to that authority without obtaining individual authorization. Likewise, a covered entity could report such cases to the police department when the police department is authorized by law to receive such reports. See 45 CFR 164.512(b)(1)(ii). See also 45 CFR 512(c) for information regarding disclosures about adult victims of abuse, neglect, or domestic violence.
- **Quality, safety or effectiveness of a product or activity regulated by the FDA.** Covered entities may disclose protected health information to a person subject to FDA jurisdiction, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples of purposes or activities for which such disclosures may be made include, but are not limited to:
  - Collecting or reporting adverse events (including similar reports regarding food and dietary supplements), product defects or problems (including problems regarding use or labeling), or biological product deviations;
  - Tracking FDA-regulated products;
  - Enabling product recalls, repairs, replacement or lookback (which includes locating and notifying individuals who received recalled or withdrawn products or products that are the subject of lookback); and
  - Conducting post-marketing surveillance. See 45 CFR 164.512(b)(1)(iii). The "person" subject to the jurisdiction of the FDA does not have to be a specific

individual. Rather, it can be an individual or an entity, such as a partnership, corporation, or association. Covered entities may identify the party or parties responsible for an FDA-regulated product from the product label, from written material that accompanies the product (know as labeling), or from sources of labeling, such as the Physician's Desk Reference.

- **Persons at risk of contracting or spreading a disease.** A covered entity may disclose protected health information to a person who is at risk of contracting or spreading a disease or condition if other law authorizes the covered entity to notify such individuals as necessary to carry out public health interventions or investigations. For example, a covered health care provider may disclose protected health information as needed to notify a person that (s)he has been exposed to a communicable disease if the covered entity is legally authorized to do so to prevent or control the spread of the disease. See 45 CFR 164.512(b)(1)(iv).
- **Workplace medical surveillance.** A covered health care provider who provides a health care service to an individual at the request of the individual's employer, or provides the service in the capacity of a member of the employer's workforce, may disclose the individual's protected health information to the employer for the purposes of workplace medical surveillance or the evaluation of work-related illness and injuries to the extent the employer needs that information to comply with OSHA, the Mine Safety and Health Administration (MSHA), or the requirements of State laws having a similar purpose. The information disclosed must be limited to the provider's findings regarding such medical surveillance or work-related illness or injury. The covered health care provider must provide the individual with written notice that the information will be disclosed to his or her employer (or the notice may be posted at the worksite if that is where the service is provided). See 45 CFR 164.512(b)(1)(v).

OCR HIPAA Privacy
December 3, 2002 Revised April 3, 2003

Research

Background

The HIPAA Privacy Rule establishes the conditions under which protected health information may be used or disclosed by covered entities for research purposes. Research is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." See 45 CFR 164.501. A covered entity may always use or disclose for research purposes health information which has been de-identified (in accordance with 45 CFR 164.502(d), and 164.514(a)-(c) of the Rule) without regard to the provisions below.

The Privacy Rule also defines the means by which individuals will be informed of uses and disclosures of their medical information for research purposes, and their rights to access information about them held by covered entities. Where research is concerned, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research. Currently, most research involving human subjects operates under the Common Rule (45 CFR Part 46, Subpart A) and/or the Food and Drug Administration's

(FDA) human subject protection regulations (21 CFR Parts 50 and 56), which have some provisions that are similar to, but separate from, the Privacy Rule's provisions for research. These human subject protection regulations, which apply to most Federally-funded and to some privately funded research, include protections to help ensure the privacy of subjects and the confidentiality of information. The Privacy Rule builds upon these existing Federal protections. More importantly, the Privacy Rule creates equal standards of privacy protection for research governed by the existing Federal human subject regulations and research that is not.

How the Rule Works

In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose protected health information for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule. Research Use/Disclosure Without Authorization. To use or disclose protected health information without authorization by the research participant, a covered entity must obtain one of the following:

- **Documented Institutional Review Board (IRB) or Privacy Board Approval.** Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an IRB or a Privacy Board. See 45 CFR 164.512(i)(1)(i). This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants' authorization were required. A covered entity may use or disclose protected health information for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board, provided it has obtained documentation of all of the following:
  - Identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
  - A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Rule;
  - A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;
  - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
  - The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

The following three criteria must be satisfied for an IRB or Privacy Board to approve a waiver of authorization under the Privacy Rule:

1. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, 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 consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
   - adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for

authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the protected health information.

- **Preparatory to Research**. Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose. See 45 CFR 164.512(i)(1)(ii). This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.
- **Research on Protected Health Information of Decedents**. Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii).
- **Limited Data Sets with a Data Use Agreement.** A data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher for research, public health, or health care operations. See 45 CFR 164.514(e). A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual. The data use agreement must:
  - Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;
  - Limit who can use or receive the data; and
  - Require the recipient to agree to the following:
    - Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;
    - Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
    - Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
    - Not to identify the information or contact the individual.
- **Research Use/Disclosure With Individual Authorization**. The Privacy Rule also permits covered entities to use or disclose protected health information for research purposes when a research participant authorizes the use or disclosure of information about him or herself. Today, for example, a research participant's authorization will typically be sought for most clinical trials and some records research. In this case, documentation of IRB or Privacy Board approval of a waiver of authorization is not required for the use or disclosure of protected health information. To use or disclose protected health information with authorization by the research participant, the covered entity must obtain an authorization that satisfies the requirements of 45 CFR 164.508. The Privacy Rule has a general set of authorization requirements that apply to all uses

and disclosures, including those for research purposes. However, several special provisions apply to research authorizations:

- Unlike other authorizations, an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the "end of the research study".
- An authorization for the use or disclosure of protected health information for a research study may be combined with a consent to participate in the research, or with any other legal permission related to the research study.
- An authorization for the use or disclosure of protected health information for a research study may be combined with an authorization for a different research activity, provided that, if research-related treatment is conditioned on the provision of one of the authorizations, such as in the context of a clinical trial, then the compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the unconditioned research activity.
- An authorization may be obtained from an individual for uses and disclosures of protected health information for future research purposes, so long as the authorization adequately describes the future research such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for the future research purposes.

- **Accounting for Research Disclosures.** In general, the Privacy Rule gives individuals the right to receive an accounting of certain disclosures of protected health information made by a covered entity. See 45 CFR 164.528. This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose. See 45 CFR 164.528(b)(3). Among the types of disclosures that are exempt from this accounting requirement are:
  - Research disclosures made pursuant to an individual's authorization;
  - Disclosures of the limited data set to researchers with a data use agreement under 45 CFR 164.514(e).

In addition, for disclosures of protected health information for research purposes without the individual's authorization pursuant to 45 CFR164.512(i), and that involve at least 50 records, the Privacy Rule allows for a simplified accounting of such disclosures by covered entities. Under this simplified accounting provision, covered entities may provide individuals with a list of all protocols for which the patient's protected health information may have been disclosed under 45 CFR 164.512(i), as well as the researcher's name and contact information. Other requirements related to this simplified accounting provision are found in 45 CFR 164.528(b)(4).

Transition Provisions. Under the Privacy Rule, a covered entity may use and disclose protected health information that was created or received for research, either before or after the applicable compliance date, if the covered entity obtained any one of the following prior to the compliance date

- An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
- The informed consent of the individual to participate in the research;

- A waiver of authorization approved by either an IRB or a privacy board (in accordance with 45 CFR 164.512(i)(1)(i)); or
- A waiver of informed consent by an IRB in accordance with the Common Rule or an exception under FDA's human subject protection regulations at 21 CFR 50.24. However, if a waiver of informed consent was obtained prior to the compliance date, but informed consent is subsequently sought after the compliance date, the covered entity must obtain the individual's authorization as required at 45 CFR 164.508. For example, if there was a temporary waiver of informed consent for emergency research under the FDA's human subject protection regulations, and informed consent was later sought after the compliance date, individual authorization would be required before the covered entity could use or disclose protected health information for the research after the waiver of informed consent was no longer valid. The Privacy Rule allows covered entities to rely on such express legal permission, informed consent, or waiver of authorization of informed consent, which they create or receive before the applicable compliance date, to use and disclose protected health information for specific research studies, as well as for future unspecified research that may be included in such permission.

OCR HIPAA Privacy
December 3, 2002 Revised June 5, 2013

Emergency Situations: Preparedness, Planning, and Response

The Privacy Rule protects individually identifiable health information from uses and disclosures that unnecessarily compromise the privacy of an individual. The Rule is carefully designed to protect the privacy of health information, while allowing important health care communications to occur.

These pages address the release of protected health information for planning or response activities in emergency situations. In addition, please view the Civil Rights Emergency Preparedness page to learn how nondiscrimination laws apply during an emergency.

Planning

Access an interactive decision tool designed to assist emergency preparedness and recovery planners in determining how to gain access to and use health information about persons with disabilities or others consistent with the Privacy Rule.

The tool guides the user through a series of questions to find out how the Privacy Rule would apply in specific situations. By helping users focus on key Privacy Rule issues, the tool helps users appropriately obtain health information for their public safety activities.

The tool is designed for covered entities as well as emergency preparedness and recovery planners at the local, state and federal levels.

- Emergency Preparedness Planning and the Privacy Rule:

- Press Release: HHS Announces New HIPAA Privacy Decision Tool for Emergency Preparedness Planning
- HIPAA Privacy Rule: Disclosures for Emergency Preparedness - A Decision Tool

Response

In this section, access guidance about sharing patient information under the Privacy Rule in emergency situations, such as to assist patients in receiving the care they need, as well as to assist in disaster relief, public health, and law enforcement efforts.

- November 2014 Bulletin: HIPAA Privacy in Emergency Situations [PDF – 30KB]
- September 2013 HIPAA Guide for Law Enforcement [PDF – 177KB]
- September 2005 Hurricane Katrina Bulletins
  - Disclosing PHI in Emergency Situations [PDF - 30KB]
  - Compliance Guidance and Enforcement Statement [PDF - 148KB]

Waivers

If the President declares an emergency or disaster *and* the Secretary of HHS declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the Privacy Rule. The Privacy Rule remains in effect. The waivers are limited and apply only for limited periods of time.

- Frequently Asked Question: HIPAA waiver during a national or public health emergency

Health Information Technology

Health information technology (health IT) involves the exchange of health information in an electronic environment. Widespread use of health IT within the health care industry will improve the quality of health care, prevent medical errors, reduce health care costs, increase administrative efficiencies, decrease paperwork, and expand access to affordable health care. It is imperative that the privacy and security of electronic health information be ensured as this information is maintained and transmitted electronically.

The materials below are the HIPAA privacy components of the *Privacy and Security Toolkit* developed in conjunction with the Office of the National Coordinator. The *Privacy and Security Toolkit* implements the principles in *The*

Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework). These guidance documents discuss how the Privacy Rule can facilitate the electronic exchange of health information.

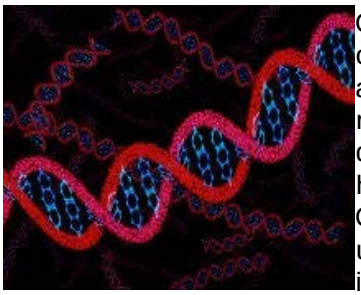
- Privacy and Security Framework: Introduction
  - Privacy and Security Framework: Correction Principle and FAQs
  - Privacy and Security Framework: Openness and Transparency Principle and FAQs
  - Privacy and Security Framework: Individual Choice Principle and FAQs
  - Privacy and Security Framework: Collection, Use, and Disclosure Limitation Principle and FAQs
  - Privacy and Security Framework: Safeguards Principle and FAQs
  - Privacy and Security Framework: Accountability Principle and FAQs
- The HIPAA Privacy Rule's Right of Access and Health Information Technology
- Personal Health Records (PHRs) and the HIPAA Privacy Rule

Learn more about the Privacy and Security Framework and view other documents in the Privacy and Security Toolkit, as well as other health information technology resources.

Genetic Information

The Genetic Information Nondiscrimination Act (GINA) was signed into law on May 21, 2008. GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.

In the proposed rule issued on October 1, 2009 OCR proposes to modify the Privacy Rule to clarify that genetic information is health information and to prohibit the use and disclosure of genetic information by covered health plans for underwriting purposes, which include eligibility determinations, premium computations, applications of any pre-existing condition exclusions, and any other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. OCR is publishing this proposed rule with a 60 day period for public comments.



OCR developed this proposed rule after coordinating with the Department of Labor (DOL), the Centers for Medicare and Medicaid Services (CMS), and the Department of the Treasury (Treasury), which have responsibility for issuing regulations under GINA Title I to prohibit discrimination based on genetic information by group health plans and health insurance issuers, and with the Equal Employment Opportunity Commission (EEOC), which has responsibility for issuing regulations under GINA Title II to prohibit discrimination based on genetic information by employers. Additionally, HHS sought guidance from the National Institutes of Health on the definitions and on other issues.

View the OCR Final Rule.

View the OCR Proposed Rule.

View the DOL/CMS/Treasury Interim Final Rule.

View the Press Release.

View the EEOC Final Rule.

HIPAA and Same-sex Marriage: Understanding Spouse, Family Member, and Marriage in the Privacy Rule

The HIPAA Privacy Rule contains several provisions that recognize the integral role that family members, such as spouses, often play in a patient's health care. For example, the Privacy Rule allows covered entities to share information about the patient's care with family members in various circumstances. In addition, the Privacy Rule provides protections against the use of genetic information about an individual, which includes certain information about family members of the individual, for underwriting purposes. This guidance addresses the effect of the 2013 Supreme Court decision regarding the Defense of Marriage Act (DOMA) on these provisions.

In *United States v. Windsor*, the Supreme Court held section 3 of DOMA to be unconstitutional. Section 3 of DOMA had provided that federal law would recognize only opposite-sex marriages. In light of the *Windsor* ruling, covered entities (and business associates, as applicable) must consider the following regarding lawfully married same-sex spouses and same-sex marriage.

At 45 CFR 160.103, the Privacy Rule includes the terms *spouse* and *marriage* in the definition of *family member*. Consistent with the *Windsor* decision, the term *spouse* includes individuals who are in a legally valid same-sex marriage sanctioned by a state, territory, or foreign jurisdiction (as long as, as to marriages performed in a foreign jurisdiction, a U.S. jurisdiction would also recognize the marriage). The term *marriage* includes both same-sex and opposite-sex marriages, and *family member* includes dependents of those marriages. All of these terms apply to individuals who are legally married, whether or not they live or receive services in a jurisdiction that recognizes their marriage.

- The definition of a *family member* is relevant to the application of §164.510(b) *Standard: Uses and disclosures for involvement in the individual's care and notification purposes*. Under certain circumstances, covered entities are permitted to share an individual's protected health information with a family member of the individual. Legally married same-sex spouses, regardless of where they live, are family members for the purposes of applying this provision.
- The definition of a *family member* is also relevant to the application of §164.502(a)(5)(i), *Use and disclosure of genetic information for underwriting purposes*. This provision prohibits health plans, other than issuers of long-term care policies, from using or disclosing genetic information for underwriting purposes. For example, such plans may not use information regarding the genetic tests of a family member of the individual, or the manifestation of a disease or disorder in a family member of the individual, in making underwriting decisions about the individual. This includes the genetic tests of a same-sex spouse of the individual, or the manifestation of a disease or disorder in the same-sex spouse of the individual.

This guidance was developed to assist covered entities in understanding how the *Windsor* decision may affect certain of their Privacy Rule obligations. In the coming months, OCR intends to issue additional clarifications through guidance or to initiate rulemaking to address same-sex spouses as personal representatives under the Privacy Rule.