

HIPAA: Disclosures to Family and Friends



Kim C. Stanger
(7-18)

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

Overview

- **Overview**
- **Situations in which HIPAA allows disclosures**
 - Personal representatives
 - Family and others involved in care
 - Treatment, payment or healthcare operations
 - Disclosures required by law
 - Requests and authorizations
- **Makin the disclosure**
- **Patient portal problems**
- **Reporting breaches**

Written Materials

- OCR, *Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524*
- OCR, *When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved In Your Care*
- OCR, *How HIPAA Allows Doctors to Respond to the Opioid Crisis*
- Client Alert, *HIPAA and Disclosure to Family Members or Others Involved in the Patient's Care*
- Client Alert, *HIPAA: Releases of Information v. Authorization*
- Client Alert, *HIPAA and Records of Deceased Persons*
- Client Alert, *HIPAA: Should You Ask Patients for Consent to Disclose Information?*

Health Insurance Portability and Accountability Act (“HIPAA”)

- 45 CFR 164
 - .500: Privacy Rule
 - .300: Security Rule
 - .400: Breach Notification Rule
- HITECH Act
 - Modified HIPAA
 - Implemented by HIPAA Omnibus Rule



Remember Other Laws



Privacy Protection

**More
restrictive law**

HIPAA

**Less restrictive
law**

- HIPAA preempts less restrictive laws.
- Comply with more restrictive law, e.g.,
 - Federally assisted drug and alcohol treatment program (42 CFR part 2)
 - State drug and alcohol programs
 - Others?
 - AIDS/HIV?
 - Mental health?



HIPAA Enforcement



Criminal Penalties

- Applies if employees or other individuals obtain or disclose protected health info from covered entity without authorization.

| Conduct | Penalty |
|--|---|
| Knowingly obtain info in violation of the law | <ul style="list-style-type: none">• \$50,000 fine• 1 year in prison |
| Committed under false pretenses | <ul style="list-style-type: none">• 100,000 fine• 5 years in prison |
| Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm | <ul style="list-style-type: none">• \$250,000 fine• 10 years in prison |

(42 USC 1320d-6(a))

HIPAA Civil Penalties

(as modified by recent inflation adjustment)

| Conduct | Penalty |
|--|---|
| Did not know and should not have known of violation | <ul style="list-style-type: none">• \$112 to \$55,910 per violation• Up to \$1,667,299 per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty |
| Violation due to reasonable cause | <ul style="list-style-type: none">• \$1,118 to \$55,910 per violation• Up to \$1,667,299 per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty |
| Willful neglect, but correct w/in 30 days | <ul style="list-style-type: none">• \$11,182 to \$55,910 per violation• Up to \$1,667,299 per type per year• Penalty is mandatory |
| Willful neglect, but do not correct w/in 30 days | <ul style="list-style-type: none">• At least \$55,910 per violation• Up to \$1,667,299 per type per year• Penalty is mandatory |

(45 CFR 160.404; see also 74 FR 56127)

Enforcement

- **State attorney general can bring lawsuit.**
 - **\$25,000 fine per violation + fees and costs**
- **In future, individuals may recover percentage of penalties.**
- **Must sanction employees who violate HIPAA.**
- **Must self-report breaches of unsecured protected health info**
 - **To affected individuals.**
 - **To HHS.**
 - **To media if breach involves > 500 persons.**
- **Possible lawsuits by affected individuals or others.**

Disclosures to Family and Friends

- Personal representatives.
- Family or others involved in health, care, or payment for care if patient does not object.
- Deceased persons.
- Facility directory.
- Treatment.
- Payment.
- Certain health care operations.
- Avert substantial harm.
- Required by law.
- Patient request to disclose or authorization.



Personal Representatives

- May/must disclose to “personal representatives.”
 - Treat personal representative as if they were the individual.
- “Personal representative” =
 - *For adult patient or emancipated minor*: person has authority to act on behalf of the patient.
 - *For unemancipated minor*: person has authority to make decisions for the minor’s health care, unless:
 - Minor may consent to their own healthcare;
 - Law doesn’t require consent of another person;
 - Parent or authorized surrogate agrees to confidentiality between patient and minor.
 - Provider may disclose or withhold info from parent or surrogate to the extent allowed by state law.

(45 CFR 164.502(g))

Personal Representatives

“HIPAA recognizes patient’s personal representatives according to state law.

- **“Generally, HIPAA provides a patient’s personal representative the right to request and obtain any information about the patient that the patient could obtain, including a complete medical record. Personal representatives are persons who have health care decision making authority for the patient under state law. This authority may be established through the parental relationship between the parent or guardian of an un-emancipated minor, or through a written directive, health care power of attorney, appointment of a guardian, a determination of incompetency, or other recognition consistent with state laws to act on behalf of the individual in making health care related decisions.”**

(OCR, How HIPAA Allows Doctors to Respond to the Opioid Crisis)

Personal Representatives

- **Not required to treat personal rep as patient (i.e., do not disclose PHI to personal rep) if:**
 - **Minor has authority to consent to care.**
 - **Minor obtains care at the direction of a court or person appointed by the court.**
 - **Parent agrees that provider may have a confidential relationship.**
 - **Provider determines that treating personal representative as the patient is not in the best interest of patient, e.g., abuse.**

(45 CFR 164.502(g))

Personal Representatives

- **May deny access if:**
 - PHI is outside the designated record set.
 - Psychotherapy notes.
 - PHI obtained under a promise of confidentiality and disclosure would identify source of info.
 - PHI compiled in anticipation of a civil, criminal, or administrative action or proceeding.
 - PHI concerning inmate if it would endanger patient or others.
 - Research.
 - Licensed provider has determined that access is reasonably likely to endanger the patient or others.
 - Subject to review by third party.

(45 CFR 164.524(a))

Family or Other Persons Involved in Care

- May use or disclose PHI to family or others involved in patient's care or payment for care:
 - *If patient present*, may disclose if:
 - Patient agrees to disclosure or has chance to object and does not object, or
 - Reasonable to infer agreement from circumstances.
 - *If patient unable to agree*, may disclose if:
 - Patient has not objected; and
 - You determine it is in the best interest of patient.
 - Limit disclosure to scope of person's involvement.
- Applies to disclosures after the patient is deceased.

(45 CFR 164.510)

Family or Other Persons Involved in Care

“Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?”

“Answer: Yes.... *If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions*, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient’s payment options with her adult daughter.
- A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.”

(OCR FAQ)

Family or Other Persons Involved in Care

“HIPAA respects individual autonomy by placing certain limitations on sharing health information with family members, friends, and others without the patient’s agreement.

- ***“For patients with decision-making capacity:*** A health care provider must give a patient the opportunity to agree or object to sharing health information with family, friends, and others involved in the individual’s care or payment for care. The provider is not permitted to share health information about patients who currently have the capacity to make their own health care decisions, and object to sharing the information (generally or with respect to specific people), unless there is a serious and imminent threat of harm to health as described above.”

(OCR, How HIPAA Allows Doctors to Respond to the Opioid Crisis)

➤ **Is notice in the Notice of Privacy Practices sufficient?**

Family or Other Persons Involved in Care

“Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?”

“Answer ...: *Even when the patient is not present or it is impracticable because of emergency circumstances or the patient’s incapacity for the covered entity to ask the patient ...*, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. Thus, for example:

- A surgeon may, if consistent with such professional judgment, inform a patient’s spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient’s progress and prognosis.
- A doctor may, if consistent with such professional judgment, discuss an incapacitated patient’s condition with a family member over the phone.”

(OCR FAQ)

Family or Other Persons Involved in Care

“HIPAA allows health care professionals to disclose some health information without a patient’s permission under certain circumstances, including:

- **“Sharing health information with family and close friends who are involved in care of the patient if the provider determines that doing so is in the best interests of an incapacitated or unconscious patient and the information shared is directly related to the family or friend’s involvement in the patient’s health care or payment of care. For example, a provider may use professional judgment to talk to the parents of someone incapacitated by an opioid overdose about the overdose and related medical information, but generally could not share medical information unrelated to the overdose without permission.”**

(OCR, How HIPAA Allows Doctors to Respond to the Opioid Crisis)

Family or Other Persons Involved in Care

“Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?”

“Answer: ...In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient’s best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.”

(OCR FAQ)

Family or Other Persons Involved in Care

“May a hospital or other covered entity notify a patient's family member or other person that the patient is at their facility?”

“Answer: Yes. The HIPAA Privacy Rule ... permits covered entities to notify ... family members, personal representatives, or other persons responsible for the care of the patient, of the patient's location, general condition, or death. Where the patient is present, or is otherwise available prior to the disclosure, and has capacity to make health care decisions, the covered entity may notify family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also use or disclose this information to notify the family and these other persons if it can reasonably infer from the circumstances, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- **A doctor may call a patient's wife to tell her that her husband was in a car accident and is being treated in the emergency room for minor injuries.**
- **A doctor may contact a pregnant patient's husband to let him know that his wife arrived at the hospital in labor and is about to give birth.**
- **A nurse may contact the patient's friend to let him know that his roommate broke his leg falling down the stairs, has had surgery, and is in recovery.”**

(OCR FAQ)

Asking Patient to List Persons to Whom Info May Be Disclosed

Benefits

- Documents consent to disclose to listed persons per 45 CFR 164.510.

Risks

- Does your staff check the list?
- What about people who are not on list?
- Does it create presumption that you will not disclose info to others even if HIPAA would otherwise allow?

➤ If list such persons, ensure you expressly reserve right to make disclosures otherwise allowed by HIPAA.

Treatment

- May disclose PHI for treatment purposes.
 - Your own treatment purposes.
 - Another provider’s treatment purposes.unless you have agreed otherwise with patient.
- “Treatment” = the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

(45 CFR 164.501, .506, and .522)

- Does not apply to psychotherapy notes.

Leaving Messages with Others

“May physician 's offices ... leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or ... reminders to patients' homes?”

“Answer: Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual’s privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.”

(OCR FAQ)

Leaving Messages with Others

May physician's offices ... leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or ... reminders to patients' homes?

Answer (cont.): A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

(OCR FAQ)

Leaving Messages with Others

“May physician's offices ... leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or ... reminders to patients' homes?”

“Answer (cont.): In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, ... a request to receive mailings from the covered entity in a closed envelope rather than by postcard [is] a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also ... reasonable requests, absent extenuating circumstances.”

(OCR FAQ)

Treatment of Others

“Under the HIPAA Privacy Rule, may a health care provider disclose protected health information about an individual to another provider, when such information is requested for the treatment of a family member of the individual?”

“Yes. The HIPAA Privacy Rule permits a covered health care provider to use or disclose protected health information for treatment purposes. While in most cases, the treatment will be provided to the individual, the HIPAA Privacy Rule does allow the information to be used or disclosed for the treatment of others. Thus, the Rule does permit a doctor to disclose protected health information about a patient to another health care provider for the purpose of treating another patient (e.g., to assist the other health care provider with treating a family member of the doctor’s patient)....”

(OCR FAQ)

Payment

- May disclose PHI for payment purposes.
 - Your own payment purposes.
 - Another covered entity’s or provider’s payment purposes.

unless you have agreed otherwise with patient.
- “Payment” = to obtain reimbursement for the provision of health care, including billing, collecting, obtaining payment, determining coverage, preauthorization, justification of charges, limited disclosures to consumer reporting agencies, etc.

(45 CFR 164.501, .506, and .522)

- Does not apply to psychotherapy notes.

Payment

“Does the HIPAA Privacy Rule permit a covered entity or its collection agency to communicate with parties other than the patient (e.g., spouses or guardians) regarding payment of a bill?”

“Answer: Yes. The Privacy Rule permits a covered entity ... to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. Therefore, a covered entity ... may contact persons other than the individual as necessary to obtain payment for health care services.... However, the Privacy Rule requires a covered entity, or its business associate, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of protected health information.”

(OCR FAQ)

Health Care Operations

- May disclose PHI for certain health care operations.
 - Your own health care operations.
 - Another covered entity’s health care operations if:
 - Each entity has relationship with patient and disclosure pertains to such relationship, and
 - Disclosure is for purpose listed in (1) or (2) of definition of “health care operations”.

Unless you have agreed otherwise with patient.

(45 CFR 164.501, .506)

➤ **Does not apply to psychotherapy notes.**

Health Care Operations

- **“Health care operations” =**
 - (1) **Conducting quality assessment and improvement activities; population-based activities relating to improving health or reducing health care costs, case management and care coordination, contacting providers and patients with info about treatment alternatives; and related functions that do not include treatment;**
 - (2) **Reviewing competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs for students, accreditation, certification, licensing, or credentialing activities; ...**
 - (4) **Conducting or arranging for medical review, legal services, and auditing functions;**
 - (5) **Business planning and development; and**
 - (6) **Business management and general administrative activities of the entity, including, but not limited to customer service; resolution of internal grievances; sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity.”**

(45 CFR 164.501)

Treatment, Payment or Operations

- If agree with patient to limit use or disclosure for treatment, payment, or healthcare operations, you must abide by that agreement except in an emergency.

(45 CFR 164.506 and 164.522)

- *Don't agree to limit disclosures for treatment, payment or operations.*
 - *Exception: disclosure to insurers.*
- *Beware asking patient for list of persons to whom disclosure may be made.*

Required by Law

- May use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(45 CFR 164.512(a))

- For example, law may require provider to disclose:
 - Threat of harm to target or other.
 - Treatment for certain types of care.
 - Others?

➤ **Limit disclosure to scope permitted by law.**

Avert Serious Threat

- May use or disclose PHI if the covered entity, in good faith, believes the use or disclosure:
 - is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
 - is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; and
- **Must be consistent with applicable law and standards of ethical conduct.**
- A covered entity is presumed to have acted in good faith if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(45 CFR 164.512(j))

Avert Serious Threat

“HIPAA allows health care professionals to disclose some health information without a patient’s permission under certain circumstances, including:

...

- **“Informing persons in a position to prevent or lessen a serious and imminent threat to a patient’s health or safety. For example, a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if the doctor informs family, friends, or caregivers of the opioid abuse after determining, based on the facts and circumstances, that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge.”**

(OCR, How HIPAA Allows Doctors to Respond to the Opioid Crisis)

Facility Directory

- **May disclose limited PHI for facility directory if:**
 - Gave patient notice and patient does not object, and
 - Requestor asks for the person by name.
- **If patient unable to agree or object, may use or disclose limited PHI for directory if:**
 - Consistent with person's prior decisions, and
 - Determine that it is in patient's best interests
- **Disclosure limited to:**
 - Name
 - Location in facility
 - General condition
 - Religion, if disclosure to minister

(45 CFR 164.510)

Patient Authorizes Disclosure

- Written requests
- Authorizations



Patient Request to Provide Information

- **Must provide PHI in designated record set to third party if:**
 - Written request by patient;
 - Clearly identifies the designated recipient and where to send the PHI; and
 - Signed by patient.

(45 CFR 164.524(c)(3)(ii))

- **Part of individual's right of access.**
 - Must respond within 30 days.
 - May only charge reasonable cost-based fee.

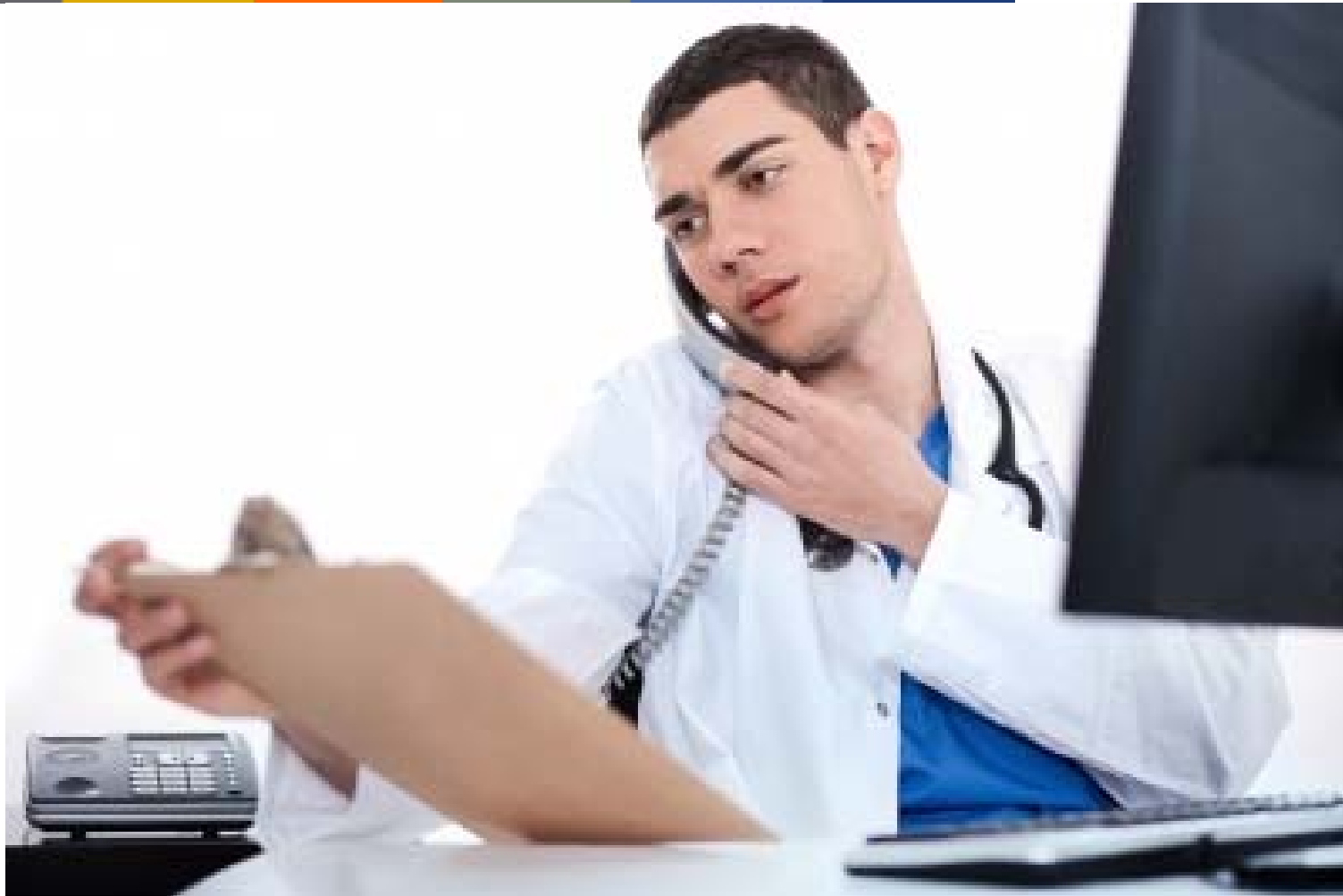
(OCR Guidance on Patient's Right to Access Information)

Authorization

- **Must obtain a valid written authorization to use or disclose protected PHI:**
 - Psychotherapy notes.
 - Marketing
 - Sale of PHI
 - Research
 - For all other uses or disclosures unless a regulatory exception applies.
- Authorization may not be combined with other documents.
- Authorization must contain required elements and statements.

(45 CFR 164.508)

Making the Disclosure



Minimum Necessary Standard

- May not use or disclose more PHI than is reasonably necessary for intended purpose.
- Minimum necessary standard does not apply to disclosures to:
 - Patient or personal representative.
 - Provider for treatment.
 - Per individual's authorization.
 - As required by law.

(45 CFR 164.502 and .514)

Verification

- **Prior to making permitted disclosure, covered entity must verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information if the identity or any such authority of such person is not known to the covered entity.**

(45 CFR 164.514(h))

- **For example, may ask for:**
 - Patient's date of birth, SSN, last date of treatment, etc.
 - Person's identification.
 - Document confirming person is a guardian, agent with power of attorney, executor of estate, etc.
 - Any other reasonable method to confirm person is who they claim.

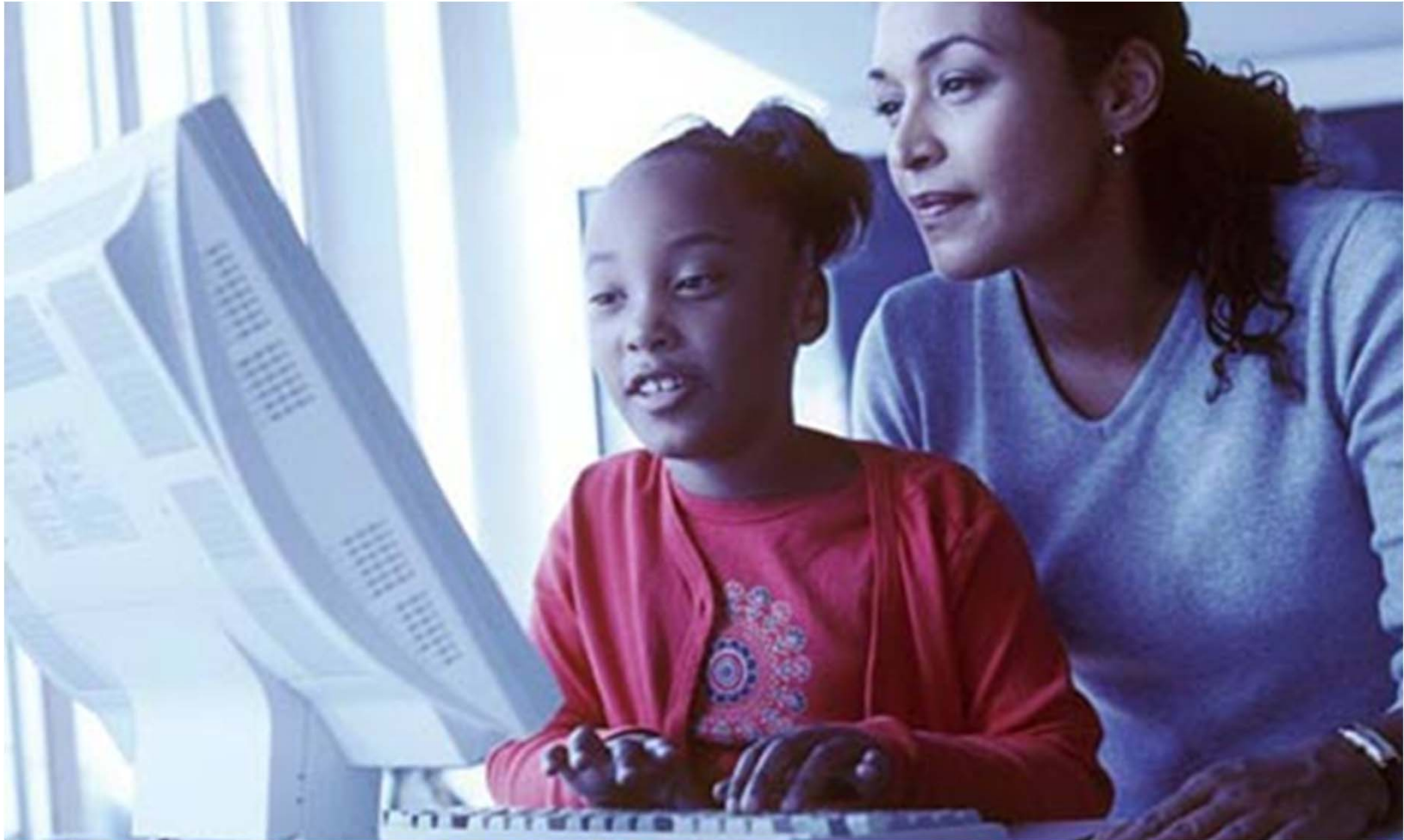
Verification

“If a patient’s family member, friend, or other person involved in the patient’s care or payment for care calls a health care provider to ask about the patient’s condition, does HIPAA require the health care provider to obtain proof of who the person is before speaking with them?”

“Answer: No. If the caller states that he or she is a family member or friend of the patient, or is involved in the patient’s care or payment for care, then HIPAA doesn’t require proof of identity in this case. However, a health care provider may establish his or her own rules for verifying who is on the phone. In addition, 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.”

(OCR FAQ)

Patient Portals



Limit Access to Some Records

- Portal Access < Patient's Right of Access
 - Under HIPAA, may limit access to PHI if:
 - Not part of designated record set
 - Psychotherapy notes
 - Obtained under a promise of confidentiality
 - Access may cause substantial harm to patient or other person.
- (45 CFR 164.524(a))
- May limit access to additional records in portal.
 - Create a process to flag or limit access to certain records.



Limit Access to Some Records

- **Check other laws for additional limits.**
 - **State laws**
 - **HIV/STDs**
 - **Mental health**
 - **Substance abuse**
 - **Genetic tests**
 - **Federally funded drug and alcohol programs have additional limits (see 42 CFR part 2)**
 - **Others?**

Access by Personal Reps

- Personal rep generally has a right to access info.
- May (should) deny personal rep access if:
 - Minor reaches age of majority.
 - Patient may consent to their own care under state law, e.g., minor seeks care for:
 - Sexually transmitted disease
 - Drug or alcohol treatment
 - Mental health
 - Reproductive health
 - Parent or guardian agrees to confidentiality.
 - Provider determines that allowing personal rep to access may endanger patient or not in patient's interest.

Check state law

(45 CFR 164.502(g))

Access by Personal Reps

- **Build in limits to portal access by personal reps, e.g.:**
 - Patient age 0-12: parents may access all records
 - Patient age 12-17: hold back or restrict parental access to certain sensitive records, e.g.,
 - Women's health
 - Psychiatry
 - Substance abuse
 - Others for which patient may consent on their own
 - Age 18 and over: terminate parental right to access unless:
 - Patient did not object and relevant to parent's involvement.
 - Patient authorization or consent.
- **Check state law!**

Access by Third Parties

- Warn patient against allowing third parties to use password.
- As practical matter, patient may allow anyone to access.
 - Provider may disclose to family members and others involved in care if patient does not object. (45 CFR 164.510)
- Provider may not knowingly allow third parties to access unless HIPAA exception applies, e.g.,
 - HIPAA-compliant authorization. (45 CFR 164.508)
 - Patient directs that PHI sent to third party. (45 CFR 164.524)
 - Family members and others involved in care so long as patient has not objected. (45 CFR 164.510)
 - Personal representative. (45 CFR 164.502)
 - Other?

Access by Third Parties

- **Options:**
 - Allow third party to use patient's user name and password.
 - Perhaps problems with Security Rule requiring unique user ID.
 - Give third party their own user name and password if patient agrees.
 - HIPAA authorization. (45 CFR 164.508)
 - Patient request to disclose. (45 CFR 164.524)
 - Set up separate account with different parameters, e.g., allow proxy to view but not change any fields.

Breach Reporting (45 CFR 164.400)



Breach Notification

- If there is “breach” of “unsecured PHI”,
 - Covered entity must notify:
 - Each individual whose unsecured PHI has been or reasonably believed to have been accessed, acquired, used, or disclosed.
 - HHS.
 - Local media, if breach involves > 500 persons in a state.
 - Business associate must notify covered entity.

(45 CFR 164.400 et seq.)

“Breach” of Unsecured PHI

- Acquisition, access, use or disclosure of PHI in violation of privacy rules is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the info has been compromised based on a risk assessment of the following factors:
 - nature and extent of PHI involved;
 - unauthorized person who used or received the PHI;
 - whether PHI was actually acquired or viewed; and
 - extent to which the risk to the PHI has been mitigated,unless an exception applies.

(45 CFR 164.402)

Additional Resources



http://www.hhs.gov/hipaa/

The screenshot shows the HHS.gov website for HIPAA for Professionals. A blue arrow points from the URL above to the search bar. Another blue arrow points from the search bar to the 'HIPAA for Professionals' button in the main navigation. A third blue arrow points from the left side of the page to the 'HIPAA for Professionals' sub-menu item.

HHS.gov Health Information Privacy U.S. Department of Health & Human Services

I'm looking for...  [HHS A-Z Index](#)

[HIPAA for Individuals](#) [Filing a Complaint](#) [HIPAA for Professionals](#) [Newsroom](#)

[HHS Home](#) > [HIPAA](#) > [HIPAA for Professionals](#)

Text Resize [A](#) [A](#) [A](#) Print  Share [f](#) [t](#) [+](#)

HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final [Privacy Rule](#) in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final [Security Rule](#) in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
- The [Enforcement Rule](#) provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a [final Omnibus rule](#) that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the [Breach Notification Rule](#).

HIPAA for Professionals

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +

Special Topics +

Patient Safety +

Covered Entities & Business Associates

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules


<https://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html>

bers and Frie x


Secure | <https://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html>

HHS.gov U.S. Department of Health & Human Services


Health Information Privacy

I'm looking for... 

[HHS A-Z Index](#)

 **HIPAA for Individuals**

 **Filing a Complaint**

 **HIPAA for Professionals**

 **Newsroom**

[HHS](#) > [HIPAA Home](#) > [For Individuals](#) > Family Members & Friends

HIPAA for Individuals 

- Mental Health & Substance Use Disorders
- Your Rights Under HIPAA
 - Your Medical Records
 - Employers and Health Information in the Workplace

Text Resize **A A A**

Print 

Share



Family Members and Friends



https://www.hhs.gov/sites/default/files/provider_ffg.pdf

vider_ffg.pdf



A HEALTH CARE PROVIDER'S GUIDE TO THE HIPAA PRIVACY RULE:



Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care

U.S. Department of Health and Human Services • Office for Civil Rights

This guide explains when a health care provider is allowed to share a patient's health information with the patient's family members, friends, or others identified by the patient as involved in the patient's care under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HIPAA is a Federal law that sets national standards for how health plans, health care clearinghouses, and most health care providers are to protect the privacy of a patient's health information.¹

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for

<https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf>

oid-crisis.pdf

Secure | <https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf>



How HIPAA¹ Allows Doctors to Respond to the Opioid Crisis



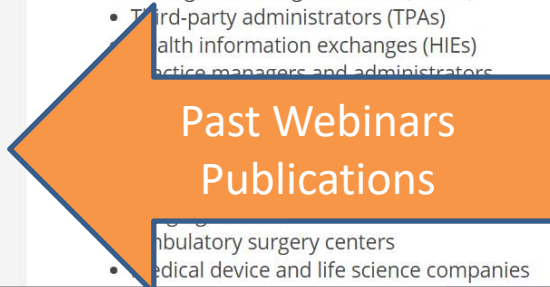
HIPAA regulations allow health professionals to share health information with a patient's loved ones in emergency or dangerous situations – but misunderstandings to the contrary persist and create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose. This document explains how health care providers have broad ability to share health information with patients' family members during certain crisis situations without violating HIPAA privacy regulations.²

HIPAA allows health care professionals to disclose some health information without a patient's permission under certain circumstances, including:

- Sharing health information with family and close friends who are involved in care of the patient if the provider determines that doing so is in the best interests of an **incapacitated or unconscious** patient and the information shared is directly related to the family or friend's involvement in the patient's health care or payment of care.³ For example, a provider may use professional judgment to talk to the parents of someone incapacitated by an opioid overdose about the overdose and related medical information, but generally could not share medical

<https://www.hollandhart.com/healthcare#overview>

The screenshot shows the top of the Holland & Hart website. The header includes the slogan "EXCELLENCE IN LEGAL SERVICES" and the firm's logo, which features a stylized mountain peak and the text "HOLLAND & HART" along with "70 YEARS EST. 1947". A navigation menu is visible on the left. The main content area is titled "OVERVIEW" and includes sections for "PRACTICES/INDUSTRIES", "NEWS & INSIGHTS", and "CONTACTS". Under "CONTACTS", there are two profile cards for Kim Stanger and Blaine Benard. Below the contact section is a "HEALTH LAW BLOG" section with a RSS icon and the text "Access to previous webinar recordings, publications, and more." The bottom of the screenshot shows a Windows taskbar with various application icons and a system tray on the right displaying the time as 7:34 AM on 2/8/2017.



Upcoming Webinars

- **7/26: Association Health Plans Final Rule**
- **8/9: HIPAA and 42 CFR part 2**
- **8/23: Healthcare Mergers and Acquisitions**





Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com