HIPAA: Checking Your Privacy Rule Compliance



Kim C. Stanger (2/17)

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.

Holland & Hart Webinar Series

Our 2017 HIPAA Compliance Webinars:

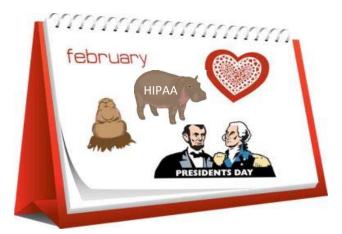
12/22/16 Risk Assessments

2/7/17 Security Rule

2/9/17 Privacy Rule

2/16/17 Business Associates

2/23/17 Responding to Breaches



Webinars and materials are available at http://www.hhhealthlawblog.com/webinar-recordings-and-presentations.



Overview

- Penalties
- Application: who, what, and whom
- Use and disclosure rules
- Authorizations
- Patient rights
- Administrative requirements
- "To Do" List
- ➤ Will be moving fast
- > Won't cover all slides in detail



Preliminaries

- Written materials
 - Copy of .ppt slides
 - Checklists
 - HIPAA compliance
 - Required privacy policies and forms
 - Notice of privacy practices
 - Authorization
 - Practice helps
 - Disclosures to law enforcement
 - Disclosures per subpoenas, orders and warrants
 - Communicating via e-mails and texts
- Written materials are available per the webinar instructions or contact me at <u>kcstanger@hollandhart.com</u>.
- Submit questions per Web-Ex "chat" function or contact me at kcstanger@hollandhart.com.



Health Insurance Portability and

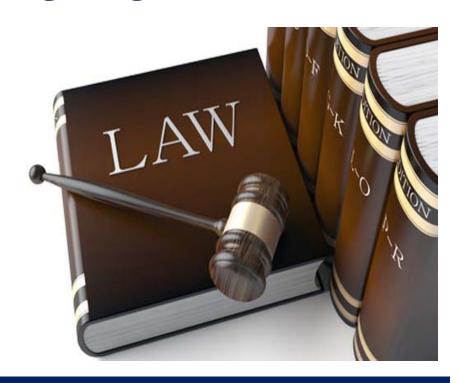
Accountability Act ("HIPAA")

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

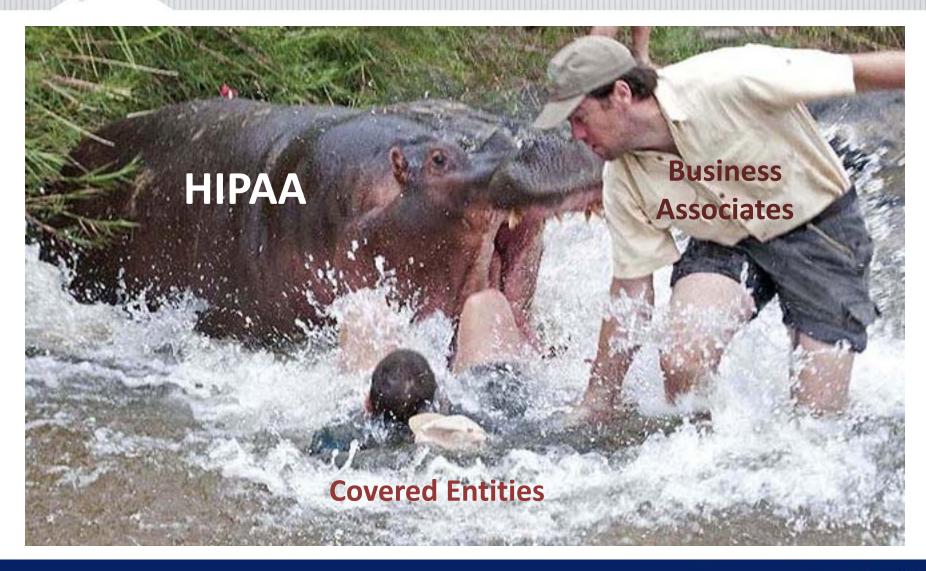


Remember Other Privacy Laws!

- Must comply with other law if it is more strict than HIPAA, i.e.,
 - Provides greater protection to patient info, or
 - Gives patients greater rights regarding their info.
- For example:
 - Medical Practices Act
 - Licensing regulations
 - Accreditation standards
 - Ethics standards
 - Common law duty
 - 42 CFR part 2



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	\$50,000 fine1 year in prison
Committed under false pretenses	100,000 fine5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	 \$250,000 fine 10 years in prison

Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	 \$100 to \$50,000 per violation Up to \$1.5 million per type per year No penalty if correct w/in 30 days OCR may waive or reduce penalty
Violation due to reasonable cause	 \$1000 to \$50,000 per violation Up to \$1.5 million 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	 \$10,000 to \$50,000 per violation Up to \$1.5 million per type per year Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	 At least \$50,000 per violation Up to \$1.5 million per type per year Penalty is mandatory

HIPAA Fines/Settlements Over Last Year

Conduct	Penalty
Loss or theft of unencrypted devices with info of 7,000+ patients	\$3,200,000
Theft of unencrypted USB with info of 2,209 individuals	\$2,200,000
Failure to timely report breach	\$475,000
Malware exposed info of 1,670 persons	\$650,000
Patient info accessible through internet searches	\$2,140,500
Loss of unencrypted backup tapes by BA; failure to review and update BAA	\$400,000
Breaches involving 4,000,000 persons	\$5,500,000
Theft of unencrypted laptop exposing info of 10,000 patients	\$2,750,000
Orthopedic group gave x-rays of 17,300 patients to vendor without BAA	\$750,000
Hospital laptop containing 13,000 patients' info stolen from car	\$3,900,000
BA's laptop containing 9,400 patients' info stolen; no BAA	\$1,550,000
PT clinic posted patient names, photos and testimonials on website	\$25,000
Employee left patient records behind when moved; investigation showed	\$239,800

HIPAA: Avoiding Civil Penalties

You can likely avoid HIPAA civil penalties if you:

- Have required policies and safeguards in place.
- Execute business associate agreements.
- Train personnel and document training.
- Respond immediately to mitigate and correct any violation.
- Timely report breaches if required.

No "willful neglect" = No penalties if correct violation within 30 days.

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.
- OCR is conducting Phase 2 audits.
- Must self-report breaches of unsecured protected health info.
 - To affected individuals.
 - To HHS.
 - To media if breach involves > 500 persons.
- In future, individuals may recover percentage of penalties.
- Possible lawsuits by affected individuals or others.
 - State privacy laws or tort claims
 - Consumer protection statutes
 - FTCA
 - FCRA

Who and What Does it Cover?



Entities Subject to HIPAA

Covered entities

Is your

health plan

compliant?

- Health care providers who engage in certain electronic transactions.
 - Consider hybrid entities.

Health plans, including employee group health plans if:

- 50 or more participants; or
- Administered by third party (e.g., TPA or insurer).
- Health care clearinghouses.
- Business associates of covered entities
 - Entities with whom you share PHI to perform services on your behalf.



Protected Health Information

- Protected health info ("PHI") =
 - Individually identifiable health info, i.e., info that could be used to identify individual.
 - Concerns physical or mental health, health care, or payment.
 - Created or received by covered entity in its capacity as a healthcare provider.
 - Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.
- Not de-identified info.



Not Covered by HIPAA

- Info after person has been dead for 50 years.
- Info maintained in capacity other than as provider.
 - e.g., as employer
 - Beware using patient info for employment purposes.
- "De-identified" info, i.e, remove certain identifiable info.
 - Dates (birth, admission, discharge, death)
 - Telephone, fax, and e-mail
 - Social Security Number
 - Medical Record Number
 - Account numbers
 - Biometric identifiers
 - Full face photos and comparable images
 - Other unique identifying number, characteristic, or code



Prohibited Actions

Unauthorized disclosure <u>outside</u> covered entity.

Unauthorized use <u>within</u> covered entity.

Unauthorized access from within or outside covered

entity.



Use and Disclosure Rules (45 CFR 164.502-.514)



Use and Disclosure Rules

- Cannot use or disclose PHI unless—
 - For purposes of treatment, payment, or healthcare operations.
 - For disclosures to family members and others involved patients care or payment for care if:
 - Patient has not objected,
 - Disclosure appropriate under circumstances, and
 - Limit disclosure to person's involvement.
 - For certain safety or government purposes as listed in 45 CFR 164.512.
 - Have a valid written authorization signed by patient that complies with 45 CFR 164.508.



Treatment, Payment or Operations

- May use/disclose PHI without patient's authorization for your own:
 - Treatment;
 - Payment; or
 - Health care operations.
- May disclose PHI to another covered entity for other entity's:
 - Treatment;
 - Payment; or
 - Certain healthcare operations if both have relationship with patient.
- Exception: psychotherapy notes.
- Requires specific authorization for use by or disclosures to others.
 (45 CFR 164.506. 164.508 and 164.522)

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; see discuss below.
- Beware asking patient for list of persons to whom disclosure may be made.
 - Creates inference that disclosures will not be made to others.
 - If list persons, ensure patient understands that we may disclose to others per HIPAA.



Persons Involved in Care

- May use or disclose PHI to family or others involved in patient's care or payment for care if:
 - 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)

Facility Directory

- May disclose limited PHI for facility directory <u>if</u>:
 - 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

(45 CFR 164.510)

Other Law Requires Disclosure

- May use or disclose PHI to the extent <u>required</u> by law.
 - Must strictly comply with law.
 - Must limit to requirements of the law.
 - Does not apply if law only <u>allows</u> disclosure.
- Examples:
 - Reporting abuse.
 - Reporting certain types of injuries.
 - Reporting certain types of diseases.
 - Reporting deaths in hospitals.
 - Mental health providers reporting threats to others.
 - Others?

(45 CFR 164.512(a))

Serious and Imminent Harm

- May use or disclose PHI to if believe in good faith that use or disclosure is:
 - Necessary to prevent or lessen a serious imminent threat to the health or safety of a person or the public; and
 - To a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(45 CFR 164.512(j))

Public Health Activities

- May use or disclose PHI for certain public health activities.
 - To report child abuse or neglect.
 - To report adult abuse or neglect, if certain conditions are satisfied.
 - To public health authority authorized to receive info to prevent disease or injury.
 - To a person at risk of contracting or spreading disease if covered entity is authorized by law to contact person.
 - To report school immunizations subject to conditions.
 - For certain workplace surveillance required by regulations.
 - For certain FDA-related actions.

(45 CFR 164.512(b)-(c))



Health Oversight Activities

- May disclose PHI to health oversight agency for oversight activities authorized by law.
 - Includes audits; investigations; inspections; or civil, criminal, or administrative proceedings.
 - Relates to
 - Oversight of health care system.
 - Eligibility for benefits under govt programs.
 - Compliance with govt programs.
 - Compliance with civil rights laws.

(45 CFR 164.512(d))



Judicial and Administrative Proceedings

- May disclose PHI if—
 - Order signed by judge or administrative tribunal.
 - Subpoena, discovery request, or legal process not accompanied by court order if either:
 - Reasonable steps taken to ensure patient has been given notice and a chance to object, e.g.,
 - -Satisfactory written assurances
 - Notify patient yourself.
 - Reasonable steps have been taken to obtain a protective order.

(45 CFR 164.512(e))



Law Enforcement: Legal Process

- May disclose PHI per
 - Court order, warrant, subpoena or summons issued by a judicial officer.
 - Grand jury subpoena.
 - Administrative request, subpoena, summons or demand authorized by law if:
 - PHI relevant and material to legitimate law enforcement inquiry;
 - Request is reasonably specific and limited to purpose; and
 - De-identified info could not be used.

(45 CFR 164.512(f)(1))



Law Enforcement: Locate Person

- Upon request from law enforcement, may disclose limited PHI to help identify or locate suspect, fugitive, witness, or missing person.
 - Name and address
 - Date and place of birth
 - SSN
 - Blood type and rh factor
 - Type of injury
 - Date and time of treatment and death
 - Description of distinguishing characteristics (height, weight, race, hair color, facial hair, scars, tatoo, etc.)
- NOT PHI re DNA, dental records, or sample or analysis of body fluids or tissues.

(45 CFR 164.512(f)(2))

Law Enforcement: Victims

- Upon request from law enforcement, may disclose limited PHI about person suspected to be victim of crime (other than abuse) if:
 - Person agrees to disclosure, or
 - Unable to obtain person's agreement because of incapacity or emergency, and
 - Info needed to determine violation of law by someone other than the person and will not be used against person;
 - Information needed immediately for law enforcement activity; and
 - Disclosure in best interests of individual.

(45 CFR 164.512(f)(3))



Law Enforcement: Report Crime

- If workforce member is the victim of a criminal act and disclosed PHI to law enforcement official, provided that:
 - The PHI is about perpetrator, and
 - The PHI is limited to info specified in the regulations.

(45 CFR 164.502(j)(2))

 If provider thinks that crime has occurred on the premises, provider may disclose PHI that provider believes in good faith constitutes evidence of crime.

(45 CFR 164.502(f)(4))

- If providing emergency care away from health care facility, may disclose PHI if necessary to alert law enforcement to:
 - Commission and nature of crime;
 - Location of crime or of victims; and/or
 - Identity, description, and location of perpetrator.

(45 CFR 164.502(f)(4))



Law Enforcement: Custody

- May disclose PHI about inmate or other person in custody to law enforcement if official represents that info necessary for:
 - Provision of health care to person.
 - Health and safety of individual, other inmates.
 - Health and safety of officers or employees at correctional facility.

(45 CFR 164.512(

Workers Comp

 May disclose PHI as authorized and to the extent necessary to comply with workers comp laws.

(45 CFR 164.512(I))

Check state laws to determine scope of permissible disclosures.

Other Exceptions

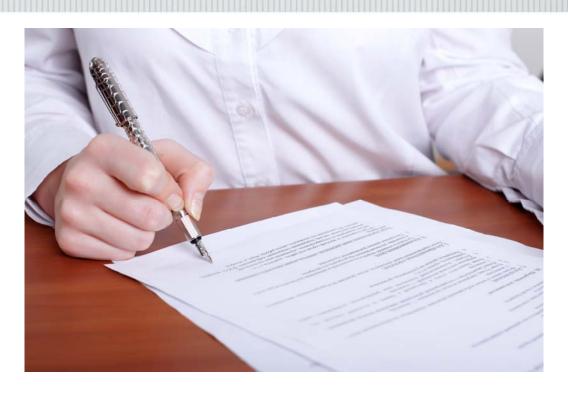
- To coroners
- To funeral directors
- For organ donation
- For certain research purposes
- For military personnel
- For national security and intelligence purposes

(45 CFR 164.512(g)-(k))



Patient Authorizes Disclosure

- Written requests
- Authorizations



Patient Request to Provide Info

- Must provide PHI in designated record 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))

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)



Authorization

- Required Elements
 - Written in plain language.
 - Describe PHI to be disclosed.
 - Identify entity authorized to make disclosure.
 - Identify entity to whom disclosure made.
 - Describe purpose of disclosure.
 - "At request of individual" if patient initiates.
 - Include expiration date or event.
 - Dated and signed by patient or representative.
 - State authority of personal representative.



Authorization

- Required Statements
 - Right to revoke the authorization in writing at anytime and either:
 - Describe exceptions and how to revoke, or
 - Refer to Notice of Privacy Practices where such info may be found.
 - Cannot condition treatment or payment on authorization.
 - PHI may be re-disclosed and, if so, may not be protected.

Psychotherapy Notes

- Must have authorization to use or disclose psych notes except for provider's use of own notes for treatment purposes.
 - "Psych notes" are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
 - "Psych notes" excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
- Psych authorization cannot be combined with any other authorization.

(45 CFR 164.508)



- Generally need authorization if communication is about a product or service that encourages recipient to purchase or use product or service <u>except</u>:
 - To describe product or service provided by the covered entity,
 - For treatment of patient, or
 - For case management, care coordination, or to direct or recommend alternative treatment, therapies, providers, or setting,

<u>unless</u> covered entity receives financial remuneration from third party for making the communication.

(45 CFR 164.501 and .508(a)(3))



- If covered entity receives financial remuneration from third party in exchange for making communication about the third party's items or services, then the following <u>are</u> "marketing" and covered entity must obtain patient's authorization to use or disclose PHI to market:
 - provide refill reminders or communicate about drug currently being prescribed unless remuneration is related to cost of making the communication.
 - for treatment purposes, including case management, care coordination, or recommendations for treatment alternatives, providers, etc.
- Authorization must disclose that covered entity is receiving remuneration.



- Even though covered entity receives financial remuneration, authorization is <u>not</u> required if:
 - communication is for treatment, healthcare operations or other marketing occurs in face-to-face communication with patient, or
 - consists of promotional gift of nominal value provided by the covered entity.
- Authorization would be required for such communications via telephone or e-mail since they are not "face-to-face".

Marketing Communication Authorization

needed

- Face to Face
- Promotional gift of nominal value

- Treatment
- Healthcare operations
- Describe covered entity's own products or services

Financial remuneration received for communication

Sale of PHI

- Cannot sell PHI unless obtain patient's prior written authorization and the authorization discloses whether covered entity will receive remuneration in exchange for PHI.
- "Sale of PHI" = disclosure of PHI by covered entity or business associate if they receive (directly or indirectly) any remuneration (financial or otherwise) from or on behalf of the recipient of the PHI in exchange for the PHI.

(45 CFR 164.508(a)(4))

Sale of PHI

- Does not apply to disclosures:
 - for treatment or payment purposes.
 - as part of sale of covered entity.
 - to business associate and payment is for business associate's duties.
 - for purposes allowed by HIPAA and payment is reasonable costbased fee to transmit PHI.
 - Recovery of fees allowed by law.
- Per commentary, does not apply to:
 - payments to provide services or grants.
 - payments to participate in health information exchange.



Fundraising

- Generally need authorization to use or disclose PHI for fundraising <u>unless</u> you:
 - Disclose limited PHI to institutionally-related foundation or business associate,
 - Name, address, contact info, age, gender and birth date.
 - Dates of healthcare provided by covered entity.
 - Department of service.
 - Treating physicians.
 - Outcome information.
 - Health insurance status.
 - Include statement in notice of privacy practices,
 - With each fundraising communication, provide clear and conspicuous opportunity to opt out of fundraising, which method may not cause undue burden or more than nominal cost.

(45 CFR 164.514(f))



Research

- Need authorization for most research purposes.
 - No expiration date on authorization.
 - May condition authorization on research-related treatment.
- Do not need authorization if:
 - Obtain approval of Institutional Review Board, or
 - Privacy Committee.
- See OCR, HIPAA and Research, available at <u>www.hhs.gov/ocr/privacy/hipaa/understanding/special/r</u> <u>esearch/</u>

(164.512(i) and elsewhere)



To summarize use and disclosure rules

- Cannot use or disclose PHI unless—
 - For purposes of treatment, payment, or healthcare operations.
 - For disclosures to family members and others involved in patients care or payment for care if
 - Patient has not objected,
 - Disclosure appropriate under circumstances, and
 - Limit disclosure to person's involvement.
 - For certain safety or government purposes as listed in 45 CFR 164.512.
 - Have a valid written authorization or request signed by patient that complies with 45 CFR 164.508 or 164.524.



Parents and Personal Representatives



Personal Representatives

- Under HIPAA, you must treat the personal representative as if they were the patient.
- Personal representatives generally have right to exercise patient rights, e.g.,
 - Request restrictions on use or disclosure of PHI.
 - Access PHI.
 - Amend PHI.
 - Obtain accounting of disclosures of PHI.
- Personal rep = persons with authority under state law to:
 - Make healthcare decisions for patient.
 - Make decisions for deceased patient's estate.

(45 CFR 164.502(g))



Personal Representatives

- Not required to treat personal representative as patient (i.e., do not disclose PHI to them) 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.

Summary: Family Members and Personal Representatives

- Potential bases for disclosure
 - Personal rep has right to access PHI.
 - Disclosure for treatment, payment or health care operations.
 - Disclosure to family members or others involved in care or payment if:
 - Patient did not object,
 - In patient's best interests, and
 - Limit disclosure to scope of person's involvement.
 - Other exception, e.g., to avert serious threat.
- See OCR, Communicating with a Patient's Family, Friends or Others, available at www.hhs.gov/ocr/privacy/hipaa.



Business Associates





Business Associates

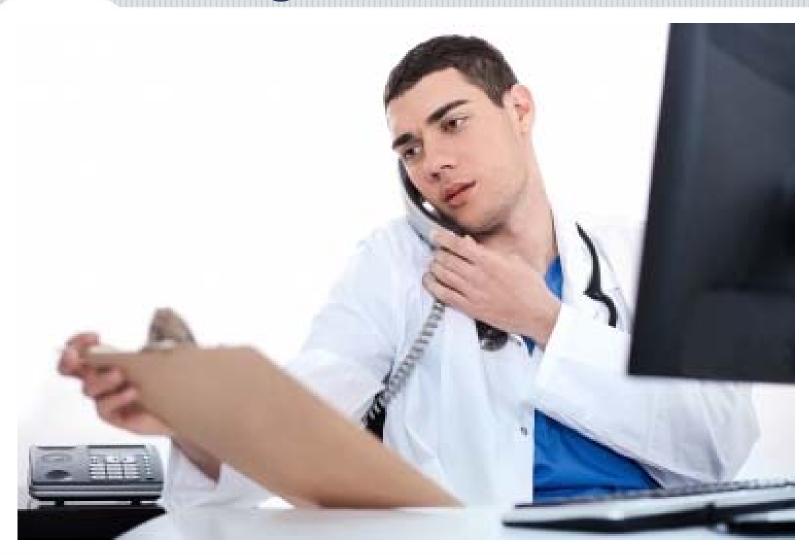
- May disclose PHI to business associate <u>if</u> you have valid business associate agreement.
 - Requires business associate to comply with certain HIPAA requirements.
 - Must contain required elements.
- Business associate = someone you want to create, maintain, transmit, or access PHI for you.

(45 CFR 164.502(e) and .504(e))

We will discuss this next week.



Making the Disclosure



Disclosure Optional

- Privacy rules usually <u>allow</u> you to make disclosures, but do not <u>require</u> it.
 - May decline to make disclosure even though privacy laws would let you make disclosure.
- Exceptions: must disclose—
 - To patient or authorized personal representative.
 - Per court order or warrant.
 - As required by other laws.

(45 CFR 164.502)

Verification

- Before disclosing PHI:
 - Verify the identity and authority of person requesting info if he/she is not known.
 - E.g., check the badge or papers of officers; birthdates or SSN for family; etc.
 - Obtain any documents, representations, or statements required to make disclosure.
 - E.g., written satisfactory assurances accompanying a subpoena, or representations from police that they need info for immediate identification purposes.

(45 CFR 164.514(f))



Minimum Necessary Standard

- Cannot use or disclose more PHI than is reasonably necessary for intended purpose.
- Minimum necessary standard does not apply to disclosures to:
 - Patient.
 - Provider for treatment.
 - Per individual's authorization.
 - As required by law.
- May rely on judgment of:
 - Another covered entity.
 - Professional within the covered entity.
 - Business associate for professional services.
 - Public official for permitted disclosure.

(45 CFR 164.502 and .514)



Minimum Necessary Standard

- Must adopt policies addressing—
 - Internal uses of PHI:
 - Identify persons who need access.
 - Draft policies to limit access accordingly.
 - External disclosures of PHI:
 - Routine disclosure: establish policies.
 - Non-routine disclosures: case-by-case review.
 - Requests for PHI:
 - Routine requests: establish policies.
 - Non-routine requests: case-by-case review.

Patient Rights



Individual Rights

- Right to receive notice of privacy practices.
- Right to request additional restrictions on use or disclosure for treatment, payment or operations.
- Right to receive information by alternative means or at alternative location.
- Right to access protected health information.
- Right to request amendment of protected health information.
- Right to limited accounting of disclosures.



Notice of Privacy Practices

- Notice summarizes HIPAA rules and explains how you will use the patient's information.
 - Must contain certain provisions.
- Direct treatment providers:
 - Give copy to patients by first date of treatment.
 - Post notice in "prominent locations"
 - Post notice on website.
 - Make good faith attempt to obtain acknowledgment of receipt.

(45 CFR 164.520)



ure https://www.hhs.gov/hipaa/for-professionals/privacy/quidance/model-notices-privacy-practices/

HHS.gov

Health Information Privacy

I'm looking for...



HHS A-Z Index









U.S. Department of Health & Human Services

HHS > HIPAA Home > For Professionals > Privacy > Guidance > Model Notices of Privacy Practices

Text Resize A A A

Print 🚍

Share







HIPAA for Professionals

Privacy Summary of the Privacy Rule Guidance Combined Text of All Rules

Model Notices of Privacy Practices

The HIPAA Privacy Rule requires health plans and covered health care providers to develop and distribute a notice that provides a clear, user friendly explanation of individuals rights with respect to their personal health information and the privacy practices of health plans and health care providers. This page provides options for meeting the requirement to create notices of privacy practices (NPP).

HHS developed the model NPPs you see on this site to help improve patient experience and understanding. These models use plain language and approachable designs.

The options below are senarated into two sets, for health plans and health care providers





















Request Restrictions on Use or Disclosure

- Individual has right to request additional restrictions on use or disclosure for treatment, payment and operations.
- Covered entity may generally decline restrictions.
 - DON'T AGREE!
- If covered entity agrees to additional restrictions, it must abide by them unless:
 - Emergency, or
 - Disclosure required by regulations.
- Covered entity may terminate the agreement for additional restrictions prospectively.

(45 CFR 164.522)



Restrictions on Disclosure to Insurers

- Must agree to request of a patient to restrict disclosure of PHI to a health plan if:
 - PHI pertains to health care item or service for which the patient, or another person on the patient's behalf, paid the covered entity in full; and
 - Disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law.
- Don't ask the patient!

(45 CFR 164.522)



Request Alternative Communications

- Must accommodate reasonable request to receive
 PHI by alternative means or at alternative locations.
 - May require written request.
 - May not require explanation.
 - May require info as to how payment will be handled.

(45 CFR 164.522(b))



Communicating by E-mail or Text

- HIPAA Privacy Rule allows patient to request communications by alternative means or at alternative locations.
 - Including unencrypted e-mail.

(45 CFR 164.522(b))

 Omnibus Rule commentary states that covered entity or business associate may communicate with patient via unsecured e-mail so long as they warn patient of risks and patient elects to communicate via unsecured e-mail to text.

(78 FR 5634)



Right to Access Info

- Individual has right to inspect and obtain copy of PHI in "designated record set, i.e., documents used to make decisions concerning healthcare or payment.
 - Includes documents created by others.
- Exceptions: no right to access to:
 - Info outside designated record set, e.g., peer review, etc.
 - Psychotherapy notes.
 - Info in anticipation of legal action.
 - Info provided under promise of confidentiality.
 - Info if provider determines that access would cause substantial harm to patient or another, subject to review by independent provider.

(45 CFR 164.524)

Right to Access Info

- May require request in writing.
- Covered entity must accept or deny request within 30 days unless obtain 30-day extension.
- If covered entity accepts the request:
 - Must provide records in form requested if readily producible.
 - May provide summary if individual agrees.
 - Must either mail records or produce records at convenient time and location.
- May charge reasonable cost-based fee, i.e., cost of actual labor and materials in making copies, not administrative or retrieval fee.



www.hhs.gov/hipaa/for-professionals /privacy/guidance/access/index.html



+

Combined Text of All Rules

Compliance & Enforcement

Covered Entities & Business

Training & Resources

Breach Notification

Special Topics

Patient Safety

Associates

Security

Access

Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. With the increasing use of and continued advances in health information technology, individuals have ever expanding and innovative opportunities to access their health information electronically, more quickly and easily, in real time and on demand. Putting individuals "in the driver's seat" with respect to their health also is a key component of health reform and the movement to a more patient-centered health care system.

The regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protect the privacy and security of individuals' identifiable health information and establish an array of individual rights with respect to health information, have always recognized the importance of providing individuals with the ability to access and obtain a copy of their health information. With limited exceptions, the HIPAA Privacy Rule (the Privacy Rule) provides individuals with a legal, enforceable right to see and receive copies upon request of the information in their medical and other health records maintained by their health care providers and health plans.

General Right

Right to Access Info

- If PHI is maintained in electronic form and patient requests electronic version:
 - Covered entity must provide the info in form and format requested by patient if it is readily producible.
 - If info is not readily producible in requested form, covered entity must provide it in a form as agreed by the covered entity and patient.
 - If covered entity requests that info be sent to another person, covered entity must comply so long as request is in writing, signed by patient, and identifies recipient.

Right to Access Info

- If covered entity denies the request:
 - Must give access to other info to the extent able.
 - Must provide written explanation, including:
 - Basis for denial.
 - Right to submit denial to independent review (if applicable).
 - Right to complain to covered entity, including the name, title and phone number to whom complaints are directed.
 - If the covered entity does not maintain the info, it must tell the patient where the info is located.



- Individual has right to request amendment.
- Covered entity may deny request if:
 - Record not part of designated record set.
 - Entity did not create the record unless creator is no longer available.
 - Record not subject to access.
 - Record is accurate and complete.
- Covered entity may:
 - Require request to be in writing.
 - Require explanation for request.
- Must act on request within 60 days.
 - May obtain a 30-day extension if explain basis for extension in writing.

(45 CFR 164.526)



- If covered entity accepts amendment:
 - Attach or link requested amendment to relevant records.
 - Notify individual of amendment.
 - Seek permission to notify others about the amendment,
 e.g.,
 - Persons identified by individual.
 - Persons who may rely on prior record to detriment of the individual, e.g., other doctors or business associates.

- If covered entity denies amendment,
 - Denial must be in writing and explain
 - Basis of denial.
 - Right to attach copy of request or statement of disagreement to record.
 - Explain complaint procedures.
 - May attach rebuttal statement.
 - Attach or link request or statement to the record.
 - Provide the request or statement with any future disclosure.



- Covered entity that receives notice of an amendment must amend its own records accordingly.
- Covered entity must document the names and titles of persons responsible for receiving and processing requests for amendments.

- Individual has a right to request accounting of all disclosures made for prior 6 years.
- Exceptions: do not need to account for disclosures
 - To the individual.
 - For treatment, payment, and health care operations.
 - Cases where disclosure is proper if given a chance to agree or object.
 - Pursuant to an authorization.
 - For certain law enforcement or health oversight purposes.
 - That occurred 6 years before.

(45 CFR 164.528)



- Net effect: must account for:
 - Improper disclosures
 - Disclosures made per 164.512, e.g., disclosures
 - Required by law.
 - For public health activities.
 - For health oversight activities.
 - For certain law enforcement purposes.
 - For workers compensation.
 - Etc.

- Accounting must include:
 - Date of disclosure.
 - Name of entity receiving disclosure.
 - Description of info disclosed.
 - Describe purpose of disclosure.
- Must keep track of this information so that you can provide accounting.
- Must account for disclosures made by business associates.
- Must account for disclosure even if you are not required to report it under breach notification rules.



- Covered entity must act on request within 60 days.
 - May obtain 30-day extension if explain basis for request in writing.
- Must provide first accounting within 12-month period free of charge.
- May charge reasonable cost-based fee for subsequent requests.
- If there are multiple, repeated disclosures, entity may summarize disclosures.

 HITECH Act requires HHS to issue regulations allowing individuals to obtain an accounting of disclosures made for purposes of treatment, payment and healthcare operations if the disclosure is through an electronic health record.

(HITECH Act 13405)

 HHS issued a proposed rule that would entitle individuals to obtain a broad report concerning those who accessed their PHI or to whom their PHI was disclosed.

(76 FR 31426 (5/31/11))

Subject to future rulemaking.

(78 FR 5568)

* Watch for new rule.



Administrative Requirements



Designate Officials

- Must designate HIPAA officers in writing:
 - Privacy officer: privacy policies
 - Security officer: security rules
 - Contact person: questions and complaints
 - Document appointment
- May be same person.

(45 CFR 164.530(a))

Implement Policies

- Implement written policies to ensure compliance with rules.
 - Modify to match changes in law
 - Coordinate notice of privacy practices
- Consider using valid forms.
 - Authorization
 - Notice of privacy practices
 - Business associate agreement
 - Request to access info
 - Request to amend info

Train Workforce

- Train workforce, i.e., those over whom you have control, e.g., employees, volunteers, students, temps.
 - New members: within reasonable time.
 - Changes in law or policy: within reasonable time.
- Document training.

(45 CFR 164.530(b))

Reasonable Safeguards

- Implement administrative, physical and technical safeguards to limit improper intentional or inadvertent disclosures.
 - No liability for "incidental disclosures" if implemented reasonable safeguards.
 - Problem: what is "reasonable"?
 - Protections are "scalable" and should not interfere with health care
 - See OCR Guidance at <u>www.hhs.gov/ocr/hipaa/privacy</u>

(45 CFR 164.530(c))

Reasonable Safeguards per OCR Guidance

NOT required to:

- Remodel.
- Eliminate sign-in sheets.
- Isolate x-ray boards.
- Remove bedside charts.
- Buy a computer.

MAY be required to:

- Keep records, monitors, faxes from view of unauthorized persons.
- Minimize eavesdropping.
- Supervise or lock areas where records stored.
- Use passwords.
- Avoid patient names in public.

Respond to Complaints and Violations

- Provide process for handling and documenting patient complaints.
- Impose and document sanctions against workforce members who violate policies.
- Mitigate wrongful use or disclosures.
- Do not retaliate.
- Do not require waiver of HIPAA rights.
- Document response.

(45 CFR 164.530(d)-(g))

Maintain Documentation

- Maintain required documentation required by HIPAA, e.g.,
 - Privacy notices and acknowledgments.
 - Policies.
 - Personnel designations.
 - Patient requests and denials.
 - Accountings.
 - Employee training.
 - Complaints.
 - Sanctions.
 - Communications that are required to be in writing.
 - Activities that are required to be documented.

(45 CFR 164.530(j))

Maintain Documentation

- Documentation may generally be retained in electronic or written form.
- Maintain documentation for 6 years from the later of:
 - When the document was created; or
 - When the document was last in effect.

Action Items



HIPAA Action Items

- 1. Assign and document HIPAA responsibility.
 - Privacy officer
 - Security officer
- 2. Ensure the officers understand the rules.
- 3. Review security rule compliance.
 - Conduct and document security risk assessment.
 - Beware electronic devices.
- 4. Ensure you have required policies.
 - Privacy rule.
 - Security rule.
 - Breach notification rule.

HIPAA Action Items

- 5. Develop and use compliant forms.
 - Authorization, privacy notice, patient requests, etc.
- 6. Execute BAAs with business associates.
 - Ensure they are independent contractors.
 - Follow up if there are problems with business associate.
- 7. Train members of workforce and document training.
 - Upon hiring.
 - Periodically thereafter.
- 8. Use appropriate safeguards.
 - Confidentiality agreements with workforce members.
 - Reasonable administrative, technical and physical safeguards

HIPAA Action Items

- 9. Respond immediately to any potential breach.
 - Immediately take appropriate steps to mitigate.
 - Retrieve PHI.
 - Obtain assurances of no further use or disclosure.
 - Warn persons who received info of penalties of violations.
 - Investigate facts to determine if there was a reportable breach.
 - Sanction workforce member as appropriate.
 - Implement corrective action, additional training, etc.
 - Document foregoing.
- 10. Timely report breaches as required.
 - To patient or personal representative.
 - To HHS
 - Internal accounting of disclosure log

Additional Resources





http://www.hhs.gov/hipaa

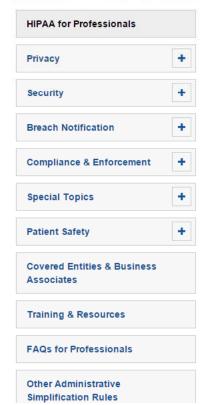
v/hipaa/for-professionals/index.html

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

I'm looking for...



HHS Home > HIPAA > HIPAA for Professionals



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.

Text Resize A A A

Print =

HHS A-Z Index

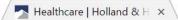
Share &

- HHS published a final <u>Privacy Rule</u> 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 <u>Security Rule</u> 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 <u>Enforcement Rule</u> provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a <u>final Omnibus rule</u> 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 <u>Breach Notification Rule</u>.

HIPAA Resources

- OCR website: www.hhs.gov/ocr/hipaa
 - Regulations
 - Summary of regulations
 - Frequently asked questions
 - Guidance regarding key aspects of privacy and security rules
 - Sample business associate agreement
 - Portal for breach notification to HHS
 - Enforcement updates
- OCR listserve
 - Notice of HIPAA changes

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









■ Secure https://www.hollandhart.com/healthcare#overview



HOLLAND&HART





OVERVIEW >

PRACTICES/INDUSTRIES **NEWS & INSIGHTS**

CONTACTS



Kim Stanger Partner Boise



Blaine Benard Partner Salt Lake City



The Healthcare this sector now stand ready to I

Issues such as rising innovations in healt minds of many of ou opportunities that a

Clients We Serve

- Hospitals
- Individual med
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs) Health information exchanges (HIEs) Practice managers and administrators

d facilities

Past Webinars Publications

ns (IPAs)

imaging centers Ambulatory surgery centers Medical device and life science companies





























and

in t 35 2

Upcoming Holland & Hart

Webinars

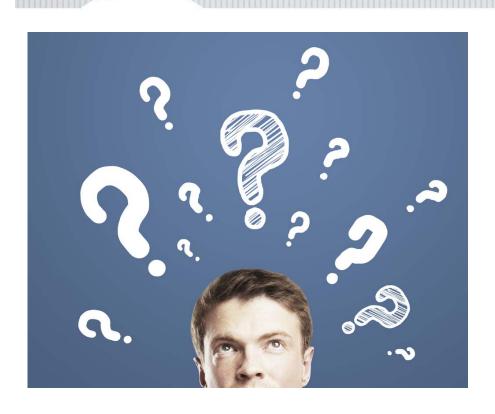
2/16 HIPAA and Business Associates

2/23 Responding to HIPAA Breaches



 To receive notices or client alerts, contact me at <u>kcstanger@hollandhart.com</u>.

Questions?



Kim C. Stanger (208) 383-3913

kcstanger@hollandhart.com