Medical Records: Definitions and Disclosures

Kim C. Stanger

IdHIMA

(4-19)

HOLLAND&HART LLP

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 LLP

Written Materials

- OCR, *Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524*
- Articles on www.hhhealthlawblog.com
  - *Producing Patient Records: "Designated Record Set" and the "Legal Health Record"*
  - *Producing Records of Other Providers*
  - *Releases of Information v. Authorization*
  - *Disclosures to Family Members or Others Involved in Patient's Care*
  - *Responding to Subpoenas, Orders and Administrative Demands*
  - *Disclosures to Law Enforcement*
  - *Records of Deceased Persons*
  - *Disclosures to the Media*
  - *HIPAA, E-mails, and Texts to Patients or Others*
  - *Disclosing Exam Results to Employers*
  - *Charging Patients for Copies of Their Records*

“Medical Record”

HOLLAND&HART LLP

"Medical Record"

- Depends on context
  - Facility policies and practices
  - Regulatory standards
  - "Business record" under Idaho Rules of Evidence
  - "Designated record set" under HIPAA
  - Records requested per:
    - Patient request to access
    - Authorization
    - Subpoena or court order

Policies and Practices

- May generally define the "medical record" as you want.
- Consider purposes of the record:
  - Effective care to patient
  - Communicate info to other providers
  - Basis for evaluating care
  - Provide support for payment
  - Protect legal interests of patient or provider
  - Planning, research, education
- Consider whether to include
  - E-mails and texts
  - Correspondence and communications with patient
  - Incident reports and other quality assurance activities
  - Other?

- What info is needed?
- How info documented?
- How/where info maintained?

HOLLAND&HART LLP

Regulatory Standards

Hospital records shall contain sufficient information to justify the diagnosis, warrant the treatment and end results and contain the following info:

- Admission date
- Identification data and consent forms
- History, including chief complaint, present illness, inventory of systems, past history, family history, social history and record of results of physical examination and provisional diagnosis
- Diagnostic, therapeutic and standing orders
- Records of observations, including progress notes and consultations
- Reports of special examinations including labs, x-rays, EKGs, etc.
- Conclusions that include the final diagnosis; condition on discharge; discharge summary; and autopsy
- Informed consent forms.
- Anatomical donation request record (for those patients who are at or near the time of death)

(IDAPA 16.03.14.360(12))

"Business Records"

"Business records — When competent evidence. A record of an act, condition or event, shall, insofar as relevant, be competent evidence if the custodian or other qualified witness testifies to the identity and the mode of its preparation, and if it was made in the regular course of business, at or near the time of the act, condition or event, and if, in the opinion of the court, the sources of information, method and time of preparation were such as to justify its admission."
(IC 9-414)

HOLLAND&HART LLP

"Business Records"

"*Records of a Regularly Conducted Activity.* A record of an act, event, condition, opinion, or diagnosis if:

(A) the record was made at or near the time by – or from information transmitted by – someone with knowledge;

(B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;

(C) making the record was a regular practice of that activity;

(D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12); and

(E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness."

(Idaho Rule of Evidence 803(6))

"Business Records"

"*Medical or Dental Tests and Test Results for Diagnostic or Treatment Purposes.* A written, graphic, numerical, symbolic or pictorial representation of the results of a medical or dental test performed for purposes of diagnosis or treatment for which foundation has been established pursuant to Rule 904, unless the opponent shows that the sources of information or other circumstances indicate a lack of trustworthiness. This exception shall not apply to:

(a) psychological tests;

(b) reports generated pursuant to I.R.C.P. 35(a);

(c) medical or dental tests performed in anticipation of or for purposes of litigation; or

(d) public records specifically excluded from the Rule 803(8) exception to the hearsay rule."

(Idaho Rule of Evidence 803(23))

"Designated Record Set"

- For records in a "designated record set", patient generally has a right to:
  - Access or obtain a copy of the records.
  - Have records sent to a third party.
  - Request an amendment to the records.
  - Obtain an accounting of disclosures.
- Must provide records in format requested by patient if reasonable to do so.
- May charge reasonable cost-based fee.

(45 CFR 164.524-.528)

HOLLAND&HART LLP

"Designated Record Set"

- "A group of records maintained by or for a covered entity that is
  - (i) The medical records and billing records about individuals maintained by or for a covered health care provider; [or]
  - (ii) Used, in whole or in part, by or for the covered entity to make decisions about individuals."

(45 CFR § 164.501)

"Designated Record Set"

Includes "medical records, billing and payment records, insurance information, clinical laboratory test reports, X-rays, wellness and disease management program information, and notes (such as clinical case notes or "SOAP" notes … but not including psychotherapy notes …), among other information generated from treating the individual or paying for the individual's care or otherwise used to make decisions about individuals…." (See OCR FAQ, available at https://www.hhs.gov/hipaa/for-professionals/faq/2042/what-personal-health-information-do-individuals/index.html).

HOLLAND&HART LLP

"Designated Record Set"

Presumably includes records created by other providers.

> **"A provider might have a patient's medical record that contains older portions of a medical record that were created by another previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?**
>
> "**Answer:** Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment."

(Available at http://www.hhs.gov/ocr/privacy/hipaa/faq/minimum_necessary/214.html).

"Designated Record Set"

"The Privacy Rule generally requires HIPAA covered entities … to provide individuals, upon request, with access to the [PHI] in one or more "designated record sets" maintained by or for the covered entity. This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice.

"Individuals have a right to access this PHI for as long as the information is maintained by a covered entity … regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (e.g., whether the covered entity, another provider, the patient, etc.)."

(OCR, Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524, available at https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/ access/index.html).

Authorization v. Patient Request to Transfer

Authorization

- Initiated by third party
- Must contain required elements, e.g., describe info to be disclosed. (see 45 CFR 164.508)
- ➢ When in doubt as to content, clarify with patient or personal representative.
- Disclosure is permitted, but not required.
- May charge reasonable fee.

Patient Request to Transfer

- Initiated by patient
- Must specify info to be disclosed
- Must provide info per request (see 45 CFR 164.524)
- ➢ When in doubt as to content, clarify with patient or personal representative.
- May charge reasonable cost-based fee.

HOLLAND&HART LLP

Order, Warrant or Subpoena

- Order: signed by judge, magistrate or administrative officer.
- Warrant: signed by judge or magistrate.
- Subpoena: may be signed by—
  - Judge or magistrate
  - Administrative officer
  - District clerk
  - Attorney

- Issue is how govt defines the record, not how you define it.
- Scope of production depends on the order, warrant or subpoena.
- If fail to produce documents within scope, may be subject to penalties, e.g., contempt, obstruction of justice, etc.
- Limit disclosure to scope.
- When in doubt, clarify with entity issuing the order, warrant or subpoena.

Common Disclosure Issues

HOLLAND&HART LLP

Common Disclosure Issues

- Treatment and payment
- Healthcare operations
- Friends and family
- Patient request
- Authorization
- Disclosures required by law
- Orders, warrants and subpoenas
- Law enforcement

Apply Most Restrictive Law

- 42 CFR part 2
  - Applies to federally assisted substance use disorder programs.
- Health Insurance Portability and Accountability Act ("HIPAA")
- Others, e.g.,
  - AIDS/HIV?
  - Mental health?

HOLLAND&HART LLP

HIPAA Civil Penalties

(as modified by recent inflation adjustment)

Conduct	Penalty
Did not know and should not have known of violation	• $114 to $57,051 per violation • Up to $1,711,533per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Violation due to reasonable cause	• $1,141 to $57,051 per violation • Up to $1,711,533 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	• $11,182 to $57,051 per violation • Up to $1,711,533 per type per year • Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	• At least $57,051 per violation • Up to $1,711,533 per type per year • Penalty is mandatory

(45 CFR 160.404; *see also* 83 FR 51378)

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)

HOLLAND&HART LLP

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.*

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.

HOLLAND&HART LLP

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)

HOLLAND&HART LLP

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)

HOLLAND&HART LLP

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)

HOLLAND&HART LLP

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)

HOLLAND&HART LLP

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)

Parents and Personal Representatives

- Under HIPAA, treat the personal rep as if they were the patient.
- Personal rep may exercise patient rights.
- Personal rep = persons with authority under state law to:
  - Make healthcare decisions for patient, or
  - Make decisions for deceased patient's estate.

(45 CFR 164.502(g))

- In Idaho, personal reps =
  - Court appointed guardian
  - Agent in DPOA
  - Spouse
  - Adult child
  - Parent
  - Delegation of parental authority
  - Other appropriate relative
  - Any other person responsible for patient's care

(IC 39-4504)

Divorced Parents

- Non-custodial parent is entitled access info, but must redact address info if custodial parent requests same in writing.

(IC 32-717A)

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.

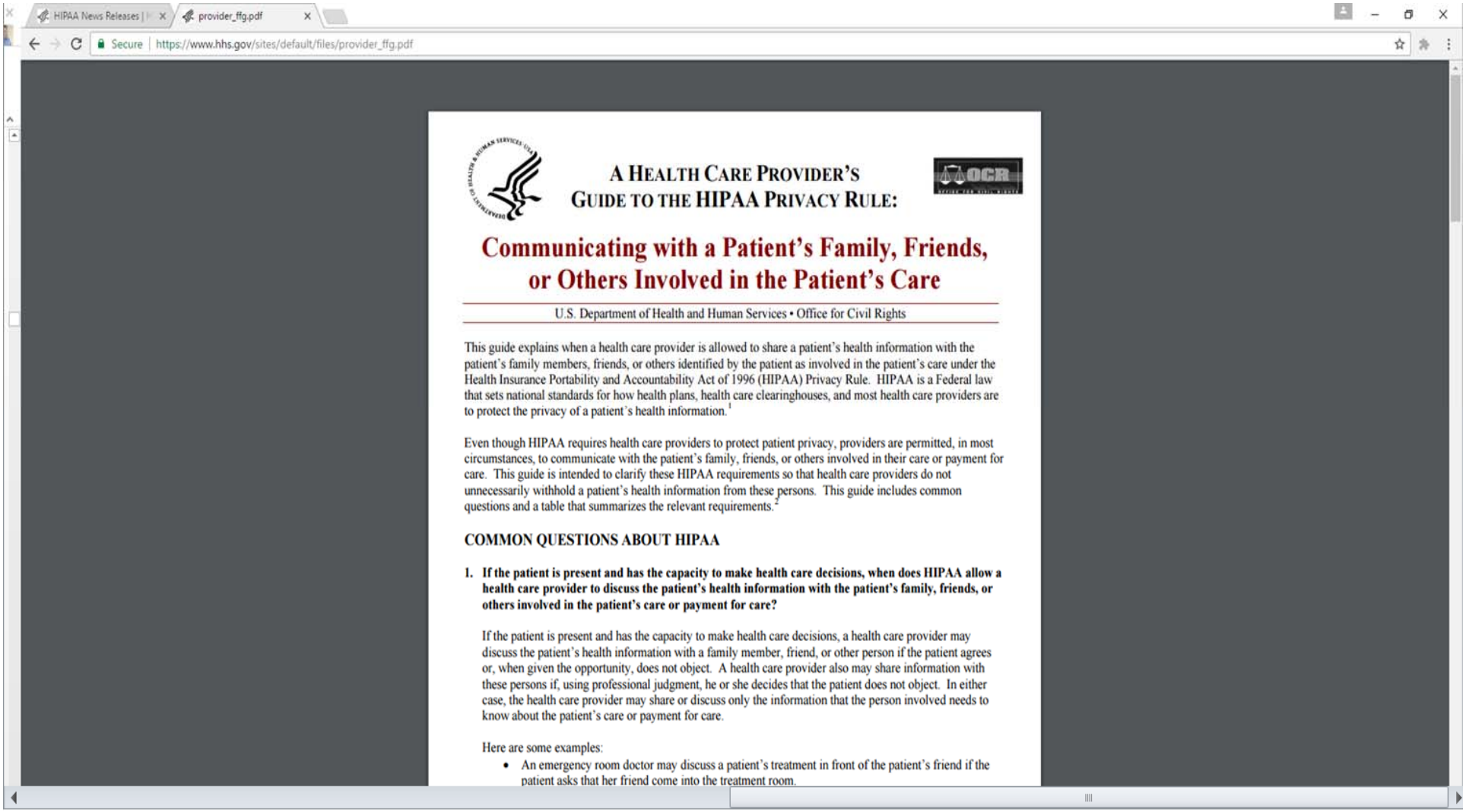
(45 CFR 164.502(g))

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))

https://www.hhs.gov/sites/default/files/provider_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 care. This guide is intended to clarify these HIPAA requirements so that health care providers do not unnecessarily withhold a patient's health information from these persons. This guide includes common questions and a table that summarizes the relevant requirements.[2]

COMMON QUESTIONS ABOUT HIPAA

1. **If the patient is present and has the capacity to make health care decisions, when does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?**

   If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, 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.

   Here are some examples:

   - An emergency room doctor may discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.

HOLLAND&HART LLP

Exceptions for Public Health or Government Functions

- Another law requires disclosures
- Disclosures to prevent serious and imminent harm.
- Public health activities
- Health oversight activities
- Judicial or administrative proceedings
  - Court order or warrant
  - Subpoenas
- Law enforcement
  - Must satisfy specific requirements
- Workers compensation

(45 CFR 164.512)

Ensure you comply with specific regulatory requirements.

HOLLAND&HART LLP

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))

Disclosures Required by Law

- HIPAA permits you to disclose PHI to the extent another law requires disclosure.
  - Limit disclosure to scope of the law.

(45 CFR 164.512(a) and 164.512(f)(1)(i))

- This does not apply if the other law simply permits disclosure.
  - E.g., statute allows disclosure of info to Dept. of Transportation re condition that affects driving.

(78 FR 5618)

- HIPAA preempts less restrictive state laws.

Disclosures Required by Idaho Law

Injury from Firearm or Crime

- Applies to person operating a hospital or other medical treatment facility, physician, resident, intern, PA, nurse or EMT.
- Applies if there is reason to believe the patient treated or requesting treatment has received:
  - (a) Any injury inflicted by means of a firearm; or
  - (b) Any injury indicating that the person may be a victim of a crime.
- Must report to local law enforcement as soon as treatment permits. Report shall include the name and address of the injured person, the character and extent of the person's injuries, and the medical basis for making the report.
- Immunity for reasonable compliance.

(IC 39-1390)

➢ No apparent penalty for failure to report.

HOLLAND&HART LLP

Disclosures Required by Idaho Law

Child Abuse or Neglect

- Applies to physician, resident, intern, nurse, social worker, or others.
- Applies if reason to believe a child under age 18 has been abused, abandoned or neglected, or observe child being subjected to conditions which would reasonably result in abuse, abandonment or neglect.
- Medical staff members notify the person in charge of hospital or his designee; that person makes the report.
- Must report the conditions to law enforcement or Child Protective Services within 24 hours.
- Immunity for good faith report.
- Failure to report is a misdemeanor.

(IC 16-1605; *see also* 45 CFR 164.512(b))

Disclosures Required by Idaho Law

Vulnerable Adult Abuse or Neglect

- Applies to any physician, nurse, employee of health facility, residential facility, and other healthcare professionals.
- Applies if there is reasonable cause to believe that a vulnerable adult is being or has been abused, neglected, or exploited.
  - "Vulnerable adult" means a person 18 years of age or older who is unable to protect himself from abuse, neglect or exploitation due to physical or mental impairment which affects the person's judgment or behavior to the extent that he lacks sufficient understanding or capacity to make or communicate or implement decisions regarding his person.

(IC 39-5302 to -5303)

- Not every abused adult is a "vulnerable adult".
- Still obligated to disclose treatment to victim of a crime.

HOLLAND&HART LLP

Disclosures Required by Idaho Law

Vulnerable Adult Abuse or Neglect

- Must immediately report info to Adult Protective Services; nursing facilities must report to DHW.
- Must also report to law enforcement within 4 hours if reasonable cause to believe that abuse or sexual assault has resulted in death or serious physical injury jeopardizing the life, health or safety.
- Immunity for good faith reports.
- Failure to report is a misdemeanor. In addition, action may be taken against nursing facility licenses.

(IC 39-5303; *see also* 45 CFR 164.512(c))

Disclosures Required by Idaho Law

Vulnerable Adult Abuse or Neglect

- Must promptly inform patient or personal rep of disclosure unless:
  - Provider believes that informing patient would place the individual at risk of serious harm; or
  - If disclosure would be to the personal rep, provider believes the personal rep is responsible for the abuse, neglect or other injury, and that it is not in best interest of patient to disclose the info.

(45 CFR 164.512(c))

Disclosures Required by Idaho Law

Mental Health Provider's Duty to Warn Victim of Threat

- Applies to "mental health professionals", i.e., physicians, professional counselors, psychologists, social workers, and nurses.
- Applies if: (i) patient has communicated an explicit threat of imminent serious physical harm or death to clearly identified or identifiable victim, and (ii) patient has apparent intent and ability to carry out such a threat.
- Must make reasonable effort in timely manner to warn the victim and notify law enforcement agency closest to the patient's or victim's residence of the threat, and supply law enforcement with any information concerning the threat of violence.
- If the victim is a minor, must also warn victim's custodial parent, noncustodial parent, or legal guardian.
- Immunity if act reasonably and consistent with standard of care.

(IC 6-1901 et seq.)

HOLLAND&HART LLP

Disclosures Required by Idaho Law

Custody of Body

- Applies to persons who find or have custody of a body.
- Applies if death:
  - (a) Occurred from violence, whether by homicide, suicide or accident;
  - (b) Occurred under suspicious or unknown circumstances; or
  - (c) Is of a child if there is reasonable suspicion to believe death occurred without a known medical disease to account for the death.
- Must promptly notify either the coroner or law enforcement.
- Must take reasonable precautions to preserve the body and body fluids, and not disturb the scene pending investigation.
- Failure to notify coroner or law enforcement is a misdemeanor.
- Failure to notify coroner or law enforcement with intent to prevent discovery is a felony.

(IC 19-4301A)

Disclosures Required by Idaho Law

- Blood tests which confirm the presence of blood-transmitted or bodily fluid-transmitted virus or disease (IC 39-4505).
- Certain reportable infectious, contagious, or communicable diseases. (IC 39-602; IDAPA 16.02.10.20)
- Births, deaths, stillborns, and induced abortions (IC 39-255, -260, -261, and -272).
- Inflammation of eyes of newborn (IC 39-902)
- Results of PKU tests (IC 39-909)
- Don't forget about local laws or ordinances…

(*See also* 45 CFR 164.512(b))

HOLLAND&HART LLP

Disclosures Required by Idaho Law

Some counties or cities may require reports of:

- Dog bites
- Injury from traffic violations
- Condition suggesting that patient is unsafe driver
- Consensual sex by minors
- Other?

- *Check local laws and ordinances.*

Public Health Activities

- May disclose for certain public health activities.
  - 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.
  - For certain FDA-related actions.

(45 CFR 164.512(b))

Health Oversight

- May disclose 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 government programs.
    - Compliance with government programs.
    - Compliance with civil rights laws.
  - Does not apply to investigations of individual unrelated to provision of health care or claim for health care benefits.

(45 CFR 164.512(d))

HOLLAND&HART LLP

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:
    - Obtain written assurances from party issuing subpoena that either:
      - Patient has been notified and had chance to object, or
      - Reasonable steps taken to obtain a protective order.
    - Take reasonable steps to notify the patient yourself.

Best Option

(45 CFR 164.512(e))

HOLLAND&HART LLP

Filing Records with Court

- Idaho law allows hospitals to respond to a subpoena by filing records with court under seal.
  - Provider must give notice to party issuing subpoena.
  - Provider may require payment for records before filing with court.
  - Party issuing subpoena may state that filing records with court is not sufficient.

  (IC 9-420)
- The statute may be preempted by HIPAA.

Law Enforcement: Legal Process

- May disclose PHI per
  - Court order, warrant, subpoena or summons issued by a judicial officer (i.e., judge or magistrate).
  - 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: Legal Process

- Prosecutors and court clerks are not "judicial officers" within the meaning of 164.512(f).
  - "Judicial officers" = judge or magistrate.
    - Independent judicial review to determine propriety of access. (See 65 FR 82679 and 82682).
  - Prosecutors are "law enforcement".
    - "Law enforcement official" means those who are empowered to "prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from alleged violation of law." (45 CFR 164.103; *see also* 65 FR 82679)
  - Court clerks are not "judicial officers".

(*US v. Zamora*, 408 F. Supp.2d 295 (S.D. Tex. 2006); *US v. Elliott*, 676 F. Supp.2d 431 (D. Md. 2009))

Law Enforcement: No Legal Process

- May disclose PHI to law enforcement if:
  - Report crime on the premises.
  - Request by law enforcement to identify or locate suspect, fugitive, witness or missing person.
    - Disclose only limited PHI.
  - Request by law enforcement about victim of crime, and
    - Victim agrees, or
    - Victim unable to agree and law enforcement represents that PHI needed to determine violation of law by someone other than the patient and PHI will not be used against person, info needed immediately, and disclosure in best interests of individual.
  - Person in custody and info needed:
    - To provide healthcare to person, or
    - For health and safety of others.

(45 CFR 164.512(f)(1))

Workers Comp

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

(45 CFR 164.512(l))

- In Idaho:
  - Must disclose info relevant to occupational injury or disease to employer, surety, manager, fund, or their attorney. (IC 72-432)
  - Must disclose written medical reports to claimant upon request and at no charge. (IDAPA 17.02.04.322)

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))

Employment Physicals, Drug Tests, or IMEs

- HIPAA generally applies to employment physicals, drug tests, school or physicals, independent medical exams ("IME"), etc.
  - Obtain patient's authorization to disclose before providing service.
  - Provider may condition exam on authorization.
  - Employer may condition employment on authorization.

(65 FR 82592 and 82640)

- Generally may not use PHI obtained in capacity as healthcare provider for employment-related decisions.

(67 FR 53191-92)

- Possible exceptions:
  - Disclosure to avoid serious and imminent threat of harm.
  - Disclosures required by OSHA, MSHA, etc.
  - Workers compensation

Business Associates

HOLLAND&HART LLP

Business Associates

- May disclose PHI to business associates if have valid business associate agreement ("BAA").
- Failure to execute BAA = HIPAA violation
  - May subject you to HIPAA fines.
    - Recent settlement: gave records to storage company without BAA: $31,000 penalty.
  - Based on recent settlements, may expose you to liability for business associate's misconduct.
    - Turned over x-rays to vendor ; no BAA: $750,000.
    - Theft of business associate's laptop; no BAA: $1,550,000.

Business Associates

- Business associates =
  - Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity.
  - Covered entities acting as business associates.
  - Subcontractors of business associates.

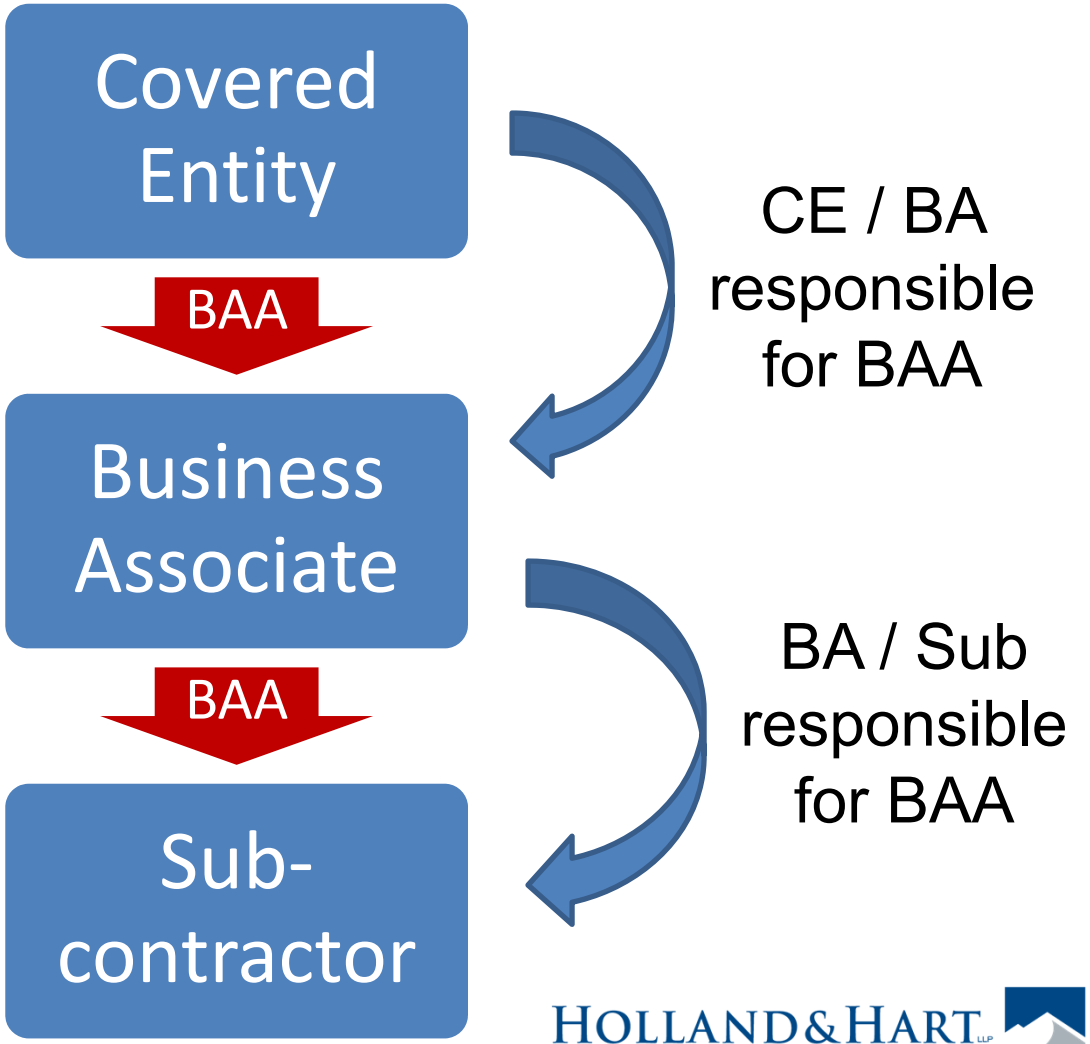
(45 CFR 160.103)

- BAAs
  - Cannot be combined with other documents.
  - Must contain required terms and statements.

(45 CFR 164.314, 164.504(e),

CEs, BAs, and Subcontractors

"[CEs] must ensure that they obtain satisfactory assurances required by the Rules from their [BAs], and [BAs] must do the same with regard to subcontractors, and so on, no matter how far 'down the chain' the information flows." (78 FR 5574)



HOLLAND&HART LLP

Identify BAs

- Business associates you may be missing:
  - Data storage companies, including cloud service providers.
    - See OCR Guidance on Cloud Service Providers, available at https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.
  - Data processing or management companies
  - Document destruction companies
  - Health information exchange
  - EHR vendor
  - E-prescribing gateways
  - Software vendor or IT support
  - Vendors of equipment or services
  - Medical device manufacturers

HOLLAND&HART LLP

Identify BAs

- Business associates you may be missing:
  - Management company
  - Billing company
  - Answering service
  - Transcription service
  - Interpreter or translator if contracted by CE
  - Consultant
  - Auditor
  - Marketing or public relations firm
  - Accountant
  - Lawyer
  - Malpractice carrier
  - Collection agency if performing services for CE

Identify BAs

- Business associates you may be missing:
  - Third party administrator
  - Accreditation organization
  - Patient safety organization
  - State or national industry association that pr
  - Peer reviewers who review records
  - Medical directors
  - Med staff members providing training
  - Med staff members providing admin
  - Others?

Unless workforce or part of organized health care arrangement ("OHCA")

HOLLAND&HART LLP

Not BAs

- **Workforce members.**
  - "[E]mployees, volunteers, trainees, and other persons … under the direct control of [CE]."
- **Persons who do not create, receive, maintain or transmit PHI as part of their job duties for CE.**
  - Janitors, Fed-Ex, plumber, electrician, and others whose job duties do not require access to PHI; access to PHI is incidental.
- **Members of organized health care arrangement.**
  - "A clinically integrated care setting in which individuals typically receive health care from more than one health care provider" (e.g., hospital and medical staff).
  - "[A]n organized system of health care … in which the participating covered entities engage in joint utilization review, quality improvement, or payment activities (e.g., provider networks)."

Not BAs

- Other health care providers with respect to disclosures concerning the treatment of the individual.
  - Other doctors, hospitals, labs, therapists, etc. providing treatment.
- Entities who are mere "conduits" for PHI.
  - Internet service providers, phone companies, postal service, etc., who transmit but do not maintain or regularly access PHI.
- Entities acting on their own behalf or on behalf of patient.
  - Payers, banks, researchers, patient advocate, etc.
- Entities performing management or admin functions for BAs.
  - Services not performed on behalf of CE.
- Government agencies performing their required functions.

Making the Disclosure

HOLLAND&HART LLP

Verification

- Before disclosing PHI:
  - Verify the identity and authority of person requesting info if he/she is not known.
    - E.g., ask for SSN or birthdate of patient, badge, credentials, 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))

- Portals should include appropriate access controls.

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

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)

HOLLAND&HART LLP

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.

Encryption

- Encryption is an addressable standard per 45 CFR 164.312:

  (e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.

  (2)(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

- ePHI that is properly encrypted is "secured".
  - Not subject to breach reporting.
- OCR presumes that loss of unencrypted laptop, USB, mobile device is breach.

Communicating by E-mail or Text

- **General rule: must be secure, i.e., encrypted.**
- **To patients:** may communicate via unsecure e-mail or text if warned patient and they choose to receive unsecure.

(45 CFR 164.522(b); 78 FR 5634)

- **To providers, staff or other third parties:** must use secure platform.

(45 CFR 164.312; CMS letter dated 12/28/17)

- **Orders:** Medicare Conditions of Participation and Conditions for Coverage generally prohibit texting orders.

(CMS letter dated 12/28/17)

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

HOLLAND&HART LLP

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

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

Past Webinars
Publications

HOLLAND&HART LLP

Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com

HOLLAND&HART LLP