Preliminaries

- Written materials.
  - Copy of ppt slides
  - HIPAA Privacy, Security, and Breach Notification Rules
  - Sample Notice of Patient Rights
  - HIPAA Privacy Checklist
  - HIPAA Security Checklist
  - Article, Avoid New HIPAA Penalties
  - Article, HIPAA Omnibus Rule: Checklist for Compliance
  - Article, New HIPAA Breach Notification Standard

Preliminaries

- Lots to cover in relatively short time.
  - Will not go through all the slides.
- This presentation summarizes the more significant aspects of HIPAA, but does not cover all of HIPAA.
  - No substitute for reading the rules.
  - Review the rules when applying HIPAA to your facts.
- Basic HIPAA training webinar recorded and available through www.hollandhart.com.
- We’ll field questions.
  - Use chat feature
  - kcstanger@hollandhart.com
Health Insurance Portability and Accountability Act ("HIPAA")

HIPAA History

- 2003: Privacy Rules, 45 CFR 164.500
  - Requires covered entities to protect privacy of patient info.
  - Gives patients certain rights concerning their info.
- 2005: Security Rules, 45 CFR 164.300
  - Requires covered entities to implement safeguards to protect electronic protected info.
- 2009: HITECH Act
  - Expanded and strengthened HIPAA.
- 2009: Breach Notification Rule, 45 CFR 164.400
  - Requires covered entities to report breaches of unsecured info.
- 2013: HIPAA Omnibus Rule, 78 FR 5566 (1/25/13)
  - Implemented and finalized HITECH Act requirements.

HIPAA Omnibus Rule (Effective 3/26/13)

- Changes breach notification standards
- Implements requirements for business associates
- Modifies rules for hybrid entities
- Limits on marketing, selling info, and fundraising
- Limits on using genetic info in underwriting
- Allows disclosures regarding deceased persons
- Allows disclosures for school immunizations
- Allows expanded research authorizations
- Gives patient right to limit disclosures to health insurers
- Gives patient right to obtain electronic PHI
- Changes notice of privacy practices
- Must comply by 9/23/13
- Omnibus rule changes shown in red
HIPAA and Other Laws

- HIPAA preempts less restrictive laws
  - If HIPAA is more restrictive, HIPAA controls
  - If other law is more restrictive, other law controls
- Other privacy laws
  - Substance Abuse Programs, 42 CFR part 2
  - Professional practices acts and regs
  - Licensing statutes and regs
  - Accreditation standards
  - Ethics standards

HIPAA Enforcement (42 CFR 160.400)

<table>
<thead>
<tr>
<th>Conduct</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| 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 within 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 within 30 days  
  • OCR may waive or reduce penalty |
| Willful neglect, but correct within 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 within 30 days | • At least $50,000 per violation  
  • Up to $1.5 million per type per year  
  • Penalty is mandatory |
HIPAA Enforcement: Civil Penalties

- Number of violations depends on circumstances.
  - A breach affecting a number of individuals: each affected individual would constitute a separate violation.
    - e.g., lost laptop containing info of 100s of patients
  - Failure to implement safeguard: each day of noncompliance would be separate violation.
    - e.g., failure to have required policies or safeguards.
  - Single incident may result in multiple violations
    - e.g., improper disclosure may result from failure to implement required policies or safeguards.
- Violations and penalties add up.

HIPAA Enforcement: Civil Penalties

- Accretive Health pays $2,500,000
  - Theft of laptop; failed to implement security rule requirements
  - First penalty against a business associate
  - Brought by state AG
- Alaska Dept of HHS pays $1,700,000
  - Theft of USB
  - First penalty against state agency
- Mass General pays $1,000,000
  - Left patient charts on subway
  - First major penalties post-HITECH
- North Idaho Hospice pays $50,000
  - Theft of laptop; failed to implement security rule requirements
  - First penalty involving breach of less than 500 persons
  - Self-reported

HIPAA Enforcement: Criminal Penalties

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

<table>
<thead>
<tr>
<th>Conduct</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowingly obtain info in violation of the law</td>
<td>$50,000 fine</td>
</tr>
<tr>
<td></td>
<td>1 year in prison</td>
</tr>
<tr>
<td>Committed under false pretenses</td>
<td>100,000 fine</td>
</tr>
<tr>
<td></td>
<td>5 years in prison</td>
</tr>
<tr>
<td>Intent to sell, transfer, or use for commercial gain,</td>
<td>$250,000 fine</td>
</tr>
<tr>
<td>personal gain, or malicious harm</td>
<td>10 years in prison</td>
</tr>
</tbody>
</table>

(42 USC 1320d-6(a))
HIPAA Enforcement: Criminal Penalties

- Physician and two hospital employees improperly accessed murdered newscaster’s medical info.
- Convictions:
  - Physician: $5000 fine + 1 year probation
  - Employee 1: $2,500 fine + 1 year probation
  - Employee 2: $1,500 fine + 1 year probation

HIPAA Enforcement: Attorney Generals

- May sue for $25,000 per violation + costs

HIPAA Enforcement: Other means

- No private cause of action under HIPAA.
- But HIPAA may become standard of care for:
  - Negligence per se
  - Privacy tort
  - Malpractice
- Patient may recover percentage of fines or settlements.
  - Watch for future rules
- Employer must impose sanctions against employees.
  - Document sanctions per 45 CFR 164.530
- Must self-report “breaches” of unsecured health info.
  - More about this later…
- HHS must conduct audits.
  - See published audit protocol
HIPAA Audit Program Protocol

- Published on OCR website, www.hhs.gov/ocr/privacy
- Lists 169 standards for privacy, security, and breach notification.
- Beware omnibus rule requirements.

HIPAA Enforcement

- The good news: covered entity or business associate may usually avoid civil penalties if they:
  - Implement required policies and safeguards.
  - See Checklists we have provided.
  - Train members of workforce and document training.
  - Use this program or recorded webinar.
  - Respond immediately to possible violation.
  - May mitigate any damage.
  - May avoid breach reporting obligation.
  - Affirmative defense if correct violations within 30 days.
Entities to Whom HIPAA Applies
(45 CFR 160.102 and .103)

Covered Entities
(160.103)
- Health care providers who engage in certain electronic transactions.
- Health plans, including employee group health plans if:
  - 50 or more participants in the plan; or
  - Administered by a third party (e.g., third party administrator or insurer)
- Health care clearinghouses

Business Associates
(160.103)
- Entities who perform certain functions on behalf of covered entities involving creating, accessing, using or disclosing protected health info.
  - Legal, accounting, consulting, data aggregation, management, administrative, accreditation, financial services, claims processing, data analysis, utilization review, quality assurance, billing, practice management.
- Practical test: business associates are persons or entities outside your organization who you want to access your info.
### Business Associates

- Management company
- Billing company
- EMR / IT specialist
- Consultant
- Accountant
- Attorney
- Malpractice insurer
- Interpreters
- Data storage entities
- Data transmission services if have routine access to info
- Subcontractors of foregoing

### NOT Business Associates

- Workforce members, i.e., if you have right to control
- Other providers when they are providing treatment
- Members of organized healthcare arrangement
- Insurance companies unless acting for you
- Mere conduits of information, e.g., mailman
- Janitors

### Business Associates

- Covered entity may disclose protected info to business associate if have business associate agreement (“BAA”).
- BAA must contain elements required by 164.314 and 164.504.
  - Security rule requirements
  - Privacy rule requirements
  - Permitted uses
  - Patient rights
  - Termination provisions
- Business associate must comply with HIPAA even if no BAA in place.

### Business Associates

- Will likely need to amend BAA to comply with omnibus rule.
  - For new or renewed BAAs: modify by 9/23/13.
  - For BAAs that were compliant with rules as of 1/25/13 and do not renew before 9/23/13: modify by 9/23/14.
  - OCR version may not contain added protections you want.
    - Representations and warranties
    - Indemnification
    - Insurance
    - Business associate is not your agent

---

Copyright © 2013, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com
Business Associates

• Covered entity is liable for business associate’s acts if:
  – Covered entity knew of pattern or practice of violations and failed to take corrective action or terminate BAA, or
  – Business associate is agent of covered entity, e.g., covered entity exercises control over method or manner of business associates work.
• Ensure BAA confirms that business associate not your agent:
  – Is independent contractor, not agent.
  – Retains control over means and method of work.
  * Consider including indemnification and insurance clauses.

Business Associates

• Covered entity may also be business associate.
  – Must comply with many privacy and security rules.
    • Limit use or disclosure of info to the extent required by principal.
    • Perform and document security risk assessment.
    • Implement administrative, physical and technical safeguards required by security rule.
    • Execute agreements with subcontractor.
    • Notify principal of breaches.
  – Subject to HIPAA penalties if fail to comply.

HIPAA Privacy Rules
(45 CFR 164.500)
Info Covered by HIPAA

- HIPAA applies to protected health info ("PHI")
  - Individually identifiable health information, i.e., that could be used to identify individual.
  - Concerns physical or mental health, health care or payment.
  - Created or received by covered entity.
  - Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.

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
- "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

Actions Covered by HIPAA

- Use, disclosure, or access
  - Disclosure = disclosure outside your organization.
  - Use = use within your organization.
  - Access = access to the information.
- You cannot access or use protected info internally unless you satisfy rules.
Use and Disclosure Rules (164.502-.506)

- Cannot use or disclose PHI unless—
  - For purposes of treatment, payment, or healthcare operations.
  - For disclosures to family members and others involved in patient’s 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

- Consent is implied if use or disclosure for purposes of—
  - Treatment
  - Payment
  - Health care operations
- Patient’s authorization is not necessary.
  - Exception: psychotherapy notes.
- If agree with patient to limit use or disclosure for treatment, payment, or healthcare operations, you must abide by that agreement.
  - Don’t agree! It increases liability.

- Treatment = treating; managing; consulting; referring patient; etc.
- Payment = billing; pre-authorization; collections; consumer reporting agencies; etc.
- Health care operations =
  - Quality assessment and review activities.
  - Review competence, care or performance of providers.
  - Licensing, accreditation, certification or training.
  - Legal or accounting services, auditing, compliance programs.
  - Business planning and development.
  - Business management and administration.
**Treatment, Payment or Operations**

- May use or disclose for your own treatment, payment or healthcare operations.
- Disclosure for another’s use is limited.
  - **Treatment**: may disclose for another covered entity’s treatment activities.
  - **Payment**: may disclose for another covered entity’s payment activities.
  - **Health care operations**: may disclose if—
    - disclosure is for other entity’s quality improvement, credentialing, or training (i.e., not business, financial, legal purposes), and
    - other entity has a relationship with patient.
  - unless entities are members of an organized health care arrangement.

**Persons Involved in Care**

*(164.510(b))*

- May use or disclose info to family or others involved in patient’s care or payment for care if conditions met.
  - 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 info to scope of person’s involvement.
  - Applies to disclosures after the patient is deceased.

**Facility Directory**

*(164.510(a))*

- May disclose limited info for facility directory if:
  - Gave patient notice and patient does not object, and
  - Requestor asks for the patient by name.
- If patient unable to agree or object, may use or disclose info 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
  - For clergy, may also disclose religious affiliation
Other Law Requires Disclosure
(164.512(a))

- May use or disclose to the extent disclosure required by another law.
  - Law must require disclosure, not just allow it.
  - Must limit disclosure to requirements of the law.
- For example, state laws may require reports of:
  - Child or vulnerable adult abuse.
  - Treatment of victim of crime.
  - Treatment of injury by firearm.
  - Threat of injury by one capable of carrying it out.
  - Certain communicable diseases.
  - Others?

Serious Threat
(164.512(j))

- May disclose info to an authority reasonably able to prevent or lessen serious and imminent threat to health or safety of an individual or the public.
- Report to proper agency who may avert threat.

Public Health Activities
(164.512(b))

- May disclose for certain public health activities, e.g.,
  - 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 child abuse or neglect.
  - For certain FDA-related actions.
  - To report immunizations to school if:
    - State law requires immunizations as condition of enrollment in school; and
    - Parent, guardian, or emancipated patient agrees.
Adult Abuse (164.512(c))

- May report adult abuse, neglect or domestic violence to government authority if:
  - Patient agrees to disclosure,
  - Disclosure is required by law, or
  - Disclosure allowed by law and:
    - Provider believes disclosure is necessary to prevent serious harm to patient or others, or
    - Patient unable to agree and government represents info not used against patient and immediately necessary to enforcement.
- Must inform the individual of disclosure unless not in best interest of patient to do so.

Health Oversight (164.512(d))

- May disclose to agency with authority to oversee healthcare for the agency’s oversight activities authorized by law.
  - E.g., licensing agencies or boards, CMS, OIG, OCR, etc.
  - 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.

Judicial or Administrative Action (164.512(e))

- May disclose if in judicial or administrative proceeding 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.,
      - Obtain satisfactory written assurances that patient was given notice and chance to object, or
      - Notify patient yourself.
    - Reasonable steps have been taken to obtain a protective order.
Law Enforcement
(164.512(f))

- May disclose to law enforcement 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:
    - Info relevant and material to legitimate law enforcement inquiry;
    - Request is reasonably specific and limited to purpose; and
    - De-identified info could not be used.

Law Enforcement:
Locate Suspect, Fugitive, Witness

- Upon request from law enforcement, may disclose limited info 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, tattoo, etc.)
  - NOT info regarding DNA, dental records, or sample or analysis of body fluids or tissues.

Law Enforcement:
Victims of Crime

- Upon request from law enforcement, may disclose limited info 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.
Law Enforcement: Crime on Premises

- If provider thinks that crime has occurred on the premises, provider may disclose info that provider believes in good faith constitutes evidence of crime.
- If provider or one of its workforce members is the victim of a crime, provider or workforce member may report the crime.

Law Enforcement: Crime Away from Premises

- If providing emergency care away from health care facility, may disclose info 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.
- Other rules apply if it involves abuse.

Law Enforcement: Persons in Custody

- May disclose info 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.
Other Exceptions
(164.512)
- To the extent allowed by workers compensation laws.
- To coroners and funeral directors to perform their duties.
- For organ donation.
- For certain research purposes.
- For military personnel.
- For national security and intelligence purposes.

Authorization
(164.508)
- Unless one of the foregoing exceptions applies, must obtain a valid written authorization to use or disclose protected health information.
- Certain uses or disclosures require authorization.
  - Psychotherapy notes, except provider’s use of own notes for treatment purposes.
  - For marketing purposes.
  - For sale of protected info.

Authorization
Required Elements
- Written in plain language.
- Describe info to be disclosed.
- Identify entity authorized to make disclosure.
- Identify entity to whom disclosure made.
- Describe purpose of disclosure.
  - "At request of individual" sufficient if patient initiates.
  - Disclose if receive remuneration for marketing or sale.
  - Include expiration date or event.
  - Dated and signed by patient or representative.
  - State authority of personal representative.
  - CMS requires provider to attach document of authority.
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.
  - Info may be re-disclosed and, if so, may not be protected.

- Cannot rely on invalid authorizations.
  - Expiration date has passed.
  - Does not contain core elements.
  - Core elements are not completed.
  - Combined with other documents.
  - Treatment conditioned on authorization.
  - Known to have been revoked.
  - Information is known to be false.
  - Give copy of authorization to individual unless individual is the one who requested authorization.
  - Retain copy of authorization.

Marketing

(164.501, .508(a)(3))

- Generally need authorization if communication is about a product or service that encourages recipient to purchase or use product or service except:
  - 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, unless covered entity receives financial remuneration from third party for making the communication.
Marketing

- 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 are "marketing" and covered entity must obtain patient's authorization to use or disclose protected info 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.

Marketing

- Even though covered entity receives financial remuneration, authorization is not required if:
  - communication 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".

Sale of Protected Info

(164.508(a)(4))

- Cannot sell protected info unless obtain patient's prior written authorization and the authorization discloses whether covered entity will receive remuneration in exchange for protected info.
- "Sale of protected info" = disclosure of protected info 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 protected info in exchange for the protected info.
Sale of Protected Info

- 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 cost-based 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 (164.514(f))

- Generally need authorization to use or disclose info for fundraising unless you:
  - Disclose limited info 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.

Research (164.512(i) and elsewhere)

- 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 www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/
To summarize

- 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 signed by patient that complies with 45 CFR 164.508.
  - Patient has not objected,
  - Disclosure appropriate under circumstances, and
  - Limit disclosure to person’s involvement.

Disclosure Optional (164.502)

- Privacy rules usually allow you to make disclosures, but do not require 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.

Verification (164.514(f))

- Before disclosing protected info:
  - 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.
Minimum Necessary Standard (164.502, .514)

- Cannot use or disclose more than is reasonably necessary for intended purpose.
  - Omnibus rule deleted “deemed” minimum necessary standard.
- 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.

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.

De-identification and Limited Data Sets (164.502(d), .514(e))

- May provide “de-identified” info if:
  - Statistician certifies that info could not be linked to individual; or
  - Remove long list of specific identifying information.
- May provide info in “limited data set” if:
  - Remove specified info; and
  - Execute data use agreement.
Personal Representatives (164.502(g))

- 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 protected info.
  - Access protected info.
  - Amend protected info.
  - Obtain accounting of disclosures of protected info.
- Personal rep = persons with authority under state law to:
  - Make healthcare decisions for patient.
  - Make decisions for deceased patient’s estate.

Personal Representatives

- Not required to treat personal representative as patient (i.e., do not disclose protected info 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 protected info.
  - 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 aver serious threat.
- See OCR, Communicating with a Patient’s Family, Friends or Others, available at www.hhs.gov/ocr/privacy/hipaa.
HIPAA Security Rule
(45 CFR 164.300 et seq.)

- Applies to electronic protected health info.
- Must conduct risk assessment to determine system vulnerabilities.
- Must implement specific safeguards.
  - Administrative
  - Technical
  - Physical
- Implementation standards.
  - Required
  - Addressable
- Execute business associate agreements.

Security Rule:
Administrative Safeguards (164.308)
- Security management process (e.g., risk management, sanction policy, system activity review)
- Assigned security process
- Workforce security (e.g., authorization and supervision; clearance procedure; termination procedures)
- Information access management (e.g., isolate clearinghouse functions; access authorization; access establishment and authorization)
- Security awareness and training (e.g., security reminders, protection from malicious software; log-in monitoring; password management)
- Security incident response procedures (e.g., response and reporting)
- Contingency plan (e.g., data backup plan; disaster recovery plan; emergency mode operation plan; testing and revision procedures; applications and data criticality analysis)
- Evaluation
Security Rule:
Physical Safeguards (164.310)
- Facility access controls (e.g., contingency operations; facility security plan; access control and validation procedures; maintenance records)
- Workstation use
- Workstation security
- Device and medial controls (e.g., disposal; media re-use; accountability; data backup and storage)

Security Rule:
Technical Safeguards (164.312)
- Access control (e.g., unique user identification; emergency access procedure; automatic logoff; encryption and decryption)
- Audit controls
- Integrity (e.g., authenticate e-protected health info)
- Person or entity authentication
- Transmission security (integrity controls; encryption)

HIPAA Security Rule:
Safeguards
- For help in complying with Security Rule, see http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.
  - Summary of privacy rule
  - Guide for risk assessment
  - Guides for implementing each element
- Government is now enforcing security rule.
- Regardless of government enforcement, security rules are good idea for risk management purposes.
HIPAA Patient Rights
(45 CFR 164.520-.528)

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
(164.520)

- Notice must contain required elements, e.g.,
  - Mandatory heading.
  - Examples of uses, disclosures, and limits.
  - Explain covered entity’s duties.
  - Effective date.
- 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.
  - Update notice with changes in law.
### Notice of Privacy Practices

- Omnibus rule requires additions to notice of privacy practices.
  - Authorizations are required for most uses and disclosures of psychotherapy notes (if applicable), marketing purposes, and sale of PHI.
  - Uses and disclosures not described in notice require authorizations.
  - Patient may opt out of fundraising.
  - Covered entity must notify the patient of breach of unsecured PHI.
  - Patient may restrict disclosures to health insurers if patient pays for the treatment.

### Request Restrictions on Use or Disclosure (164.522)

- 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.

### Restrictions on Disclosures to Health Insurers

- Must agree to request of a patient to restrict disclosure of protected info to a health plan if:
  - Protected info 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.
Restrictions on Disclosure to Health Insurers

- HHS acknowledged the operational problems with new rule but concluded providers should already have methods to flag records under minimum necessary standard.
- Only applies if patient requests restriction.
  - DON’T ASK THE PATIENT!
- Only applies to disclosures to health insurers, not others.
- Does not apply if disclosure is otherwise required by law, e.g., Medicare audits.
- Provider may require payment in full before patient may invoke the requirement.
- If cannot unbundle bill, notify patient they must pay entire bill to trigger rule.

Right to Request Alternative Communications (164.522(b))

- Must accommodate reasonable request to receive info 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.

Right to Access Info (164.524)

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

- May require request in writing.
- Covered entity must accept or deny request within 30 days unless obtain 30-day extension.
  - Omnibus rule deleted 60-day offsite 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.

Access to Info

- If protected info 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.

Access to 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.
Access to Info

- Failure to grant access to patient records is one of most frequently cited violations.
- Cignet Health Center fined $4,300,000.
  - $1,300,000: Failed to respond to 41 patients’ requests to access info.
  - $3,000,000: Failed to cooperate with OCR’s investigation.
  - Actions = “willful neglect” under new penalty structure.

Right to Request Amendment
(164.526)

- 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.

Amendments

- 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.
Amendments

- 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.

Right to Accounting of Disclosures (164.528)

- 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.
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.
Administrative Requirements (45 CFR 164.530)

- 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.

Designate Officials (164.530(a))

- Implement written policies to ensure compliance with rules
  - Modify to match changes in law
  - Coordinate notice of privacy practices
  - See checklist of policies
- Consider using valid forms
  - Authorization
  - Notice of privacy practices
  - Business associate agreement
  - Request to access info
  - Request to amend info
Train Workforce
(164.530(b))

- 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.

Reasonable Safeguards
(164.530(c))

- 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 www.hhs.gov/ocr/hipaa/privacy
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 (164.530(d)-(g))

- 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.

Maintain Documentation (164.530(j))

- 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.
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.

HIPAA Breach Notification

(45 CFR 164.400 et seq.)

Breach Notification

- If there is a breach of unsecured protected health info,
  - Covered entity must notify:
    - Each individual whose unsecured protected health info has been or reasonably believed to have been accessed, acquired, used, or disclosed.
    - HHS.
    - Media, under certain circumstances.
  - Business associate must notify covered entity.
- Reports may likely result in:
  - Patient complaints
  - OCR investigations
  - Costs and potential penalties
Breach Notification:  
“Unsecured” Protected Info
Currently, only two methods to secure protected health info:
- Encryption of electronic protected health info.
  - Transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
  - Notice provides processes tested and approved by National Institute of Standards and Technology (NIST).
- Destruction of protected health info.
  - Paper, film, or hard copy media is shredded or destroyed such that info cannot be read or reconstructed.
  - Electronic media is cleared, purged or destroyed consistent with NIST standards.
- Guidance updated annually.
(74 FR 42742 or www.hhs.gov/ocr/privacy)

Breach Notification:
“Breach”
- Acquisition, access, use or disclosure of protected health info 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.

Breach Notification:
“Breach”
- “Breach” does not include the following:
  - Unintentional acquisition, access or use by workforce member if made in good faith, within scope of authority, and PHI not further disclosed in violation of HIPAA privacy rule.
  - Inadvertent disclosure by authorized person to another authorized person at same covered entity, business associate, or organized health care arrangement, and PHI not further used or disclosed in violation of privacy rule.
  - Disclosure of PHI where covered entity or business associate have good faith belief that unauthorized person receiving info would not reasonably be able to retain info.
Summary:
To determine if breach occurred
1) Was there access, use or disclosure of protected health info?
2) Did it violate the privacy rule?
3) Is there a low probability that the info has been “compromised”?
   • Risk assessment
4) Does one of the exceptions apply, e.g.,
   • Unintentional access by workforce member within job duties + no further violation.
   • Inadvertent disclosure to another person authorized to access PHI + no further violation.
   • Improbable that PHI may be retained.
* Document foregoing.

Breach Notification:
Timing
If you have breach of unsecured protected info:
• Must provide notice as soon as reasonably possible, but no more than 60 days after discovery.
  – Deemed to have discovered the first day your workforce member or agent (other than violator) knew or should have known of breach.
• Train employees to report promptly.
• Require business associates to report immediately.

Breach Notification:
Content of Notice
• Brief description of what happened, including dates of breach and discovery.
• Description of types of unsecured PHI that were involved (e.g., name, SSN, DOB, address, account number, etc.).
• Steps persons should take to protect themselves from harm resulting from breach.
• Brief description of what covered entity is doing to investigate, mitigate, and protect against future breaches.
• Contact procedures to ask questions or learn info, including toll-free phone number, e-mail address, website, or postal address.
* NOT actual PHI that was breached or other sensitive info.
Notice to Individual

- Written notice to individual:
  - By first-class mail to last known address of individual.
  - By e-mail if individual has agreed.
- If individual is deceased,
  - By first-class mail to—
    - Next of kin, or
    - Personal representative under HIPAA.

Notice to HHS

- If breach involves fewer than 500 persons:
  - Submit to HHS annually within 60 days after end of calendar year in which breach discovered per HHS website (i.e., by March 1).
- If breach involves 500 or more persons:
  - Notify HHS contemporaneously with notice to individual or next of kin per HHS website.
  - HHS maintains a list on its website of entities who have had breaches involving 500 or more persons.
Notice to Media

- If breach involves unsecured PHI of more than 500 residents in a state, notify prominent media outlets serving that state (e.g., issue press release).
  - Without unreasonable delay but no more than 60 days from discovery of breach.
  - Generally include same content as notice to individual.
- Does not apply if breach did not affect 500 persons in a single state, e.g.,
  - Would not apply if breach affected 300 persons in state A and 300 persons in state B.

Notice by Business Associate

- Business associate must notify covered entity of breach of unsecured PHI.
  - Without unreasonable delay but no more than 60 days from discovery.
  - Notice shall include to extent possible:
    - Identification of individuals affected, and
    - Other info to enable covered entity to provide required notice to individual.
- BAA should include notice provision.
  - Require immediate notification.

Breach Notification: Delay by Law Enforcement

- Law enforcement may delay notice if it would impede criminal investigation or damage national security.
  - If stated in writing, covered entity or business associate shall delay notice accordingly.
  - If stated orally, covered entity or business associate shall—
    - Document statement and identity of law enforcement official making statement.
    - Delay notice for no more than 30 days unless written statement is given.
Notice of Security Breach: the Costs

- If have breach of unsecured PHI involving 500 patients—
  - Time and cost to investigate facts.
  - Time and cost to prepare, send, and pay for letters to 500 patients, personal representatives, or next of kin.
  - Time and cost to respond to inquiries from patients, e.g., even if 20% respond, that is 100 patients.
  - Cost of toll-free number for 90 days.
  - Cost of media notices and website updates.
  - Notice may lead to additional actions by—
    - Angry patients
    - HHS enforcement
    - Media inquiries
  - Potential loss of business due to adverse publicity.

- Better to comply!

Action Items

- Omnibus Rule

If you are a business associate, comply.
If you are a covered entity, do the following before 9/23/13.
1. Modify policies.
   - Disclosures regarding deceased persons.
   - Disclosures for school immunizations.
   - Restrictions on disclosures to health insurers.
   - Marketing, fundraising, and sale of PHI.
   - Patient access to electronic PHI.
   - Breach notification requirements.
2. Update and post notice of privacy practices.
**Action Items: Omnibus Rule**

   - Ensure you have valid BAAs.
   - Ensure they are not your agent.
4. Update BAAs by 9/23/13 or 9/13/14, as required.
5. Determine how to implement limits on disclosures to insurers.
6. Implement new breach notification standards.
7. Train employees.
   - New policies.
   - New breach notification standards.

*See Article, Checklist for Complying with Omnibus Rule.*

---

**Action Items: HIPAA Compliance**

- **Given lower breach notification standards and increased enforcement, it is a good time to review your entire HIPAA compliance…**

- **HHS has indicated that you may avoid penalties if you take the following 10 steps even if rogue employee violates HIPAA.**

---

**Action Items: HIPAA Compliance**

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.
   - *See Privacy and Security Checklists.*
Action Items: HIPAA Compliance

5. Develop compliant forms.
   – Authorization, privacy notice, patient requests, etc.

6. Execute BAAs with business associates.
   – 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.

9. Respond immediately to any potential breach.
   – Immediately take appropriate steps to mitigate.
     • Retrieve info.
     • Obtain assurances of no further use or disclosure.
     • Warn of penalties of violations.
   – Investigate facts to determine if there was a 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.

Applying the Lessons

• Rite Aid settled HIPAA violation for $1 million.
  – Rite Aid was dumping prescription bottles with protected info in dumpsters accessible to public.
  – Rite Aid failed to implement adequate policies and procedures to appropriately safeguard protected info during the disposal process.
  – Rite Aid failed to adequately train employees on how to dispose of protected info properly.
  – Rite Aid did not maintain a sanctions policy for members of its workforce who failed to properly dispose of protected info.
Applying Lessons

- Receptionist disclosed information improperly.
- In response to OCR investigation, we showed:
  - Had appropriate policies in place
  - Trained employee on policies
  - Promptly investigated, mitigated, and imposed penalties
  - Reported breach
- No action against hospital.

Additional Resources

www.hhs.gov/ocr/privacy
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 listserv
  - Notice of HIPAA changes

HIPAA Resources

- Holland & Hart Healthlaw Updates
- Holland & Hart webinars available at www.hollandhart.com
  - HIPAA training
  - Omnibus rule
- Sample HIPAA documents
  - Privacy and breach notification policies
  - Forms (e.g., notice of privacy practices, request to access info, request to amend info, etc.)
  - Agreements (e.g., BAA, confidentiality agreements, etc.)
  - Letters (response to OCR, notice to patient, etc.)
- Contact kcstanger@hollandhart.com.

Questions?

Kim C. Stanger
(208) 383-3913 or (208) 409-7907
kcstanger@hollandhart.com