

Medical Records Privacy & Security

Presented by:
Isaac M. Willett
BAKER & DANIELS LLP
600 East 96th St., Suite 600
Indianapolis, IN 46240
Phone: (317) 569-4640
Isaac.Willett@bakerd.com



What Laws Apply?

Indiana Law

Federal Law (HIPAA)

Preemption of Indiana Law

(If federal law and state law conflict, follow federal law unless state law is more stringent.)



Indiana Medical Records Laws



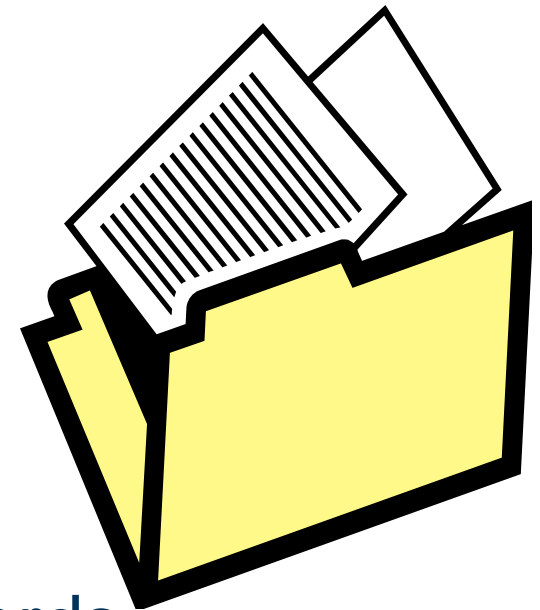
Indiana Medical Records Laws: Medical Records

Medical Records – “written, electronic or printed information possessed by a provider concerning any diagnosis, treatment, or prognosis of the patient”

Provider – Physicians, psychotherapists, dentists, nurses, nursing homes, audiologists, hospitals, etc.

Indiana Medical Records Laws: Medical Records

- What's in a medical record?
 - Name, address, DOB, etc.
 - Diagnostic reports/test results
 - Diagnosis & prognosis
 - Medication and treatment records
- Who owns the medical records?
 - The provider



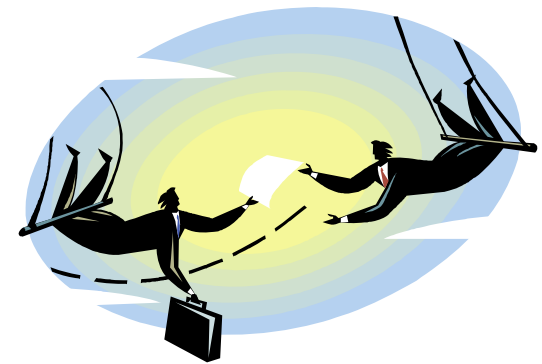


Indiana Medical Records Laws: Confidentiality of Medical Records

- Provider's Permitted Use of Medical Records (I.C. § 16-39-5-3) include
 - Submission of claims for payment
 - Collection of accounts
 - Litigation defense
 - Quality assurance
 - Peer review

Indiana Medical Records Laws: Release of Medical Records

- Release of General Medical Records to:
 - Competent, over 18 (or emancipated) patient; or
 - Parent, guardian or custodian of incompetent patient.



Indiana Medical Records Laws: Release of Medical Records

- Child's Medical Records



- Custodial and non-custodial parents have equal access.
- No access to records for non-custodial when:
 - ◆ Court order; and
 - ◆ Provider has copy and knowledge of the order.

Indiana Medical Records Laws: Release of Medical Records

- Provider must have patient's written consent to release records, including:
 - Patient's name & address
 - Name of provider
 - Name of person to whom records should be released
 - Purpose of release
 - Description of info to release
 - Signature of patient or representative
 - Date request was signed
 - Statement regarding revocation
 - Date, event or condition of expiration

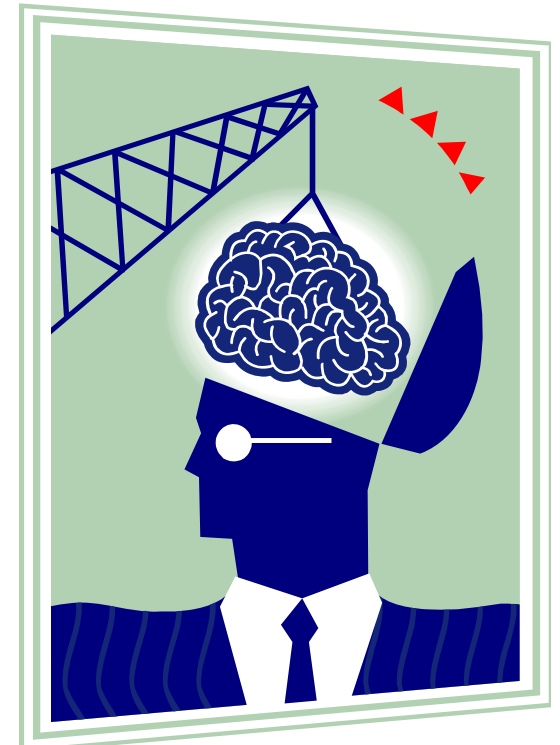


Indiana Medical Records Laws: Release of Medical Records

- Mandatory Reporting
 - Gunshots & serious wounds (I.C. § 35-47-7-1)
 - Animal bites (I.C. § 35-47-7-4; 410 IAC 1-2.3-47)
 - 2nd & 3rd degree burns (I.C. § 35-47-7-3)
 - Child abuse/neglect (I.C. § 31-33-1, et seq.)
 - Endangered adults (I.C. § 12-10-3-10)

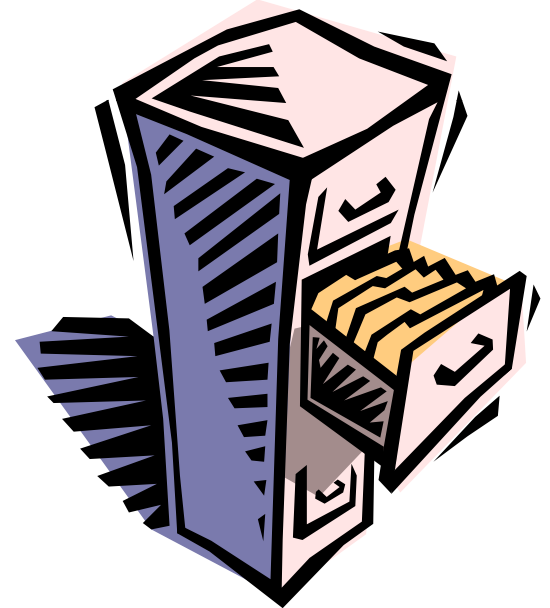
Indiana Medical Records Laws: Other Rules

- Mental Health Records
 - Release to patients
 - Release in investigations and litigation



Indiana Medical Records Laws: Other Rules

- Maintenance of Medical Records, I.C. 16-39-7
 - Medical records/microfilms - 7 years
 - Mental health records - 7 years
 - X-rays - 5 years and inform the patient
 - Mammograms:
 - ◆ 5 years
 - ◆ 10 years if no additional mammograms





HIPAA

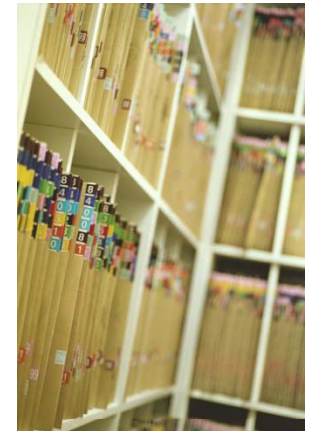


HIPAA

- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Goals:
 - Enhance consumer rights
 - Improve quality of health care
 - Improve efficiency and effectiveness of health care

HIPAA

- Privacy Rule v. Security Rule
 - Both issued by Department of Health and Human Services
 - Privacy Rule focuses on ensuring the patient's health information stays private
 - Security Rule focuses on keeping health information safe and secure
 - Same penalties for violation





HIPAA - Privacy Rule

- Establishes right to access and protect health information
- Defines authorized and required uses and disclosures
- Original effective date was April 14, 2003

HIPAA - Security Rule

- Aims to improve the effectiveness and efficiency of the health care industry by establishing protection for certain “electronic” PHI (ePHI)
- Intended to protect the confidentiality, integrity and availability of ePHI, and to protect against threats to the security/integrity of ePHI
- Requires implementation of various administrative, physical and technical safeguards
- Original compliance date was April 21, 2005

Statutory Changes



- The American Recovery and Reinvestment Act (ARRA)
 - Health Information Technology for Economic and Clinical Health Act (HITECH)
- ARRA/HITECH - changes to the HIPAA privacy and security rules
- Many changes effective February 17, 2010

HITECH – Increased Civil & Criminal Enforcement

- HITECH authorizes three levels of civil penalties
 - Violations without knowledge - \$100 to \$50,000 per violation with caps from \$25,000 to \$1.5 million per year for violations of the same type
 - Violations with reasonable cause - \$1,000 to \$50,000 per violation with caps from \$50,000 to \$1.5 million per year per type
 - Violations due to willful neglect - \$10,000 to \$50,000 per violation with caps from \$250,000 to \$1.5 million per year (depending on if violation is corrected/not corrected)
- **State Enforcement Authority** – HITECH extends civil enforcement authority to state Attorneys General

HIPAA - Privacy Rule

- **Rule:** A covered entity may not use or disclose protected health information except as permitted or required.
 - Who's a covered entity?
 - ◆ Health Plan
 - ◆ Health Care Clearinghouse
 - ◆ Providers who transmit info electronically (includes nursing facilities)
 - What is PHI?
 - ◆ Individually identifiable health information in any form relating to past, present or future physical or mental health of the patient that is created or received by a covered entity.



HIPAA - Privacy Rule

- Use/release of PHI
 - Treatment, payment or health care operations purposes (“TPO”)
 - ◆ Patient consent not needed for these purposes
 - ◆ Examples of TPO

HIPAA - Privacy Rule



– Provider needs patient’s written authorization to use PHI for any purpose other than TPO, unless otherwise excepted

- ◆ Examples
- ◆ Exceptions



HIPAA - Authorization Form

Core Elements

- Description of the PHI to be used/disclosed.
- Person authorized to make disclosure.
- Person authorized to receive PHI.
- Description of purpose.
- Expiration date or event.
- Signature of the resident and date.
 - (Description of authority, if signed by personal representative.)



HIPAA - Authorization Form

Required Statements

- Right to revoke, in writing, and
 - Exceptions and how to revoke
 - Reference to Notice
- Ability or inability to condition treatment
- Potential for information to be redisclosed and no longer protected

HIPAA - Disclosure to Patients or 3rd Parties

- Notify, identify or locate a family member involved with resident's care, or responsible for payment.
- If resident is capable, first obtain or infer his agreement before disclosing info to family or friends.
- If resident not available or capable, you may still disclose if you determine in your professional judgment that it's in the resident's best interest.

Minimum Necessary

Privacy Rule

- Covered Entity must make reasonable efforts to limit the information used or disclosed to the minimum necessary to accomplish the intended purpose
- Exceptions
 - Treatment
 - Disclosure to patient
 - Disclosure required by law

HIPAA - Patient Restrictions on Use

- Resident may request restrictions on use/disclosure.
- Privacy Rule: Facility does not have to agree to restrictions.
 - If it does, it may not disclose PHI in violation of the restriction.
 - Exceptions for emergencies.
- Restriction does not apply to disclosures
 - Required by law
 - Regarding victim of abuse
 - Court proceeding.

Restriction Requests

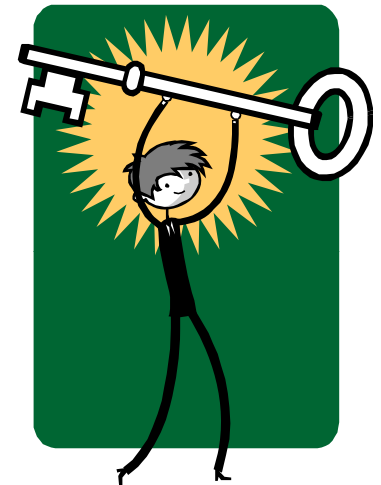
- HITECH – Requires granting of request to restrict disclosure to health plans for payment and health care operations (and not for purposes of carrying out treatment), if the PHI pertains solely to a health care item or service for which individual has paid out of pocket in full

Restriction Requests

- HITECH – Requires granting of request to restrict disclosure to health plans for payment and health care operations (and not for purposes of carrying out treatment), if the PHI pertains solely to a health care item or service for which individual has paid out of pocket in full

HIPAA - Privacy Rule

- Providing Access to Patients:
 - Covered entity must provide the access requested by the individual to the PHI about the individual in designated record sets.
 - If same PHI is in more than one designated record set or more than one location, need only produce PHI once.





Denial of Access

- Provide a timely, written denial containing
 - basis for denial,
 - if applicable, statement of review rights and description of how to exercise,
 - description of complaint procedures.
- Review of Denial

HIPAA - Privacy Rule

- Providing Access to Patients cont.:
 - Form of Access: Covered entity must provide access in the form or format requested by the individual.
 - ◆ If information is not readily available in the requested form/format, then produce it in a readable hard copy form or such other format agreed to with the individual.
 - ◆ Covered entity may provide individual a summary of PHI instead of records if (1) individual agrees in advance to such summary and (2) individual agrees in advance to the fees for such summary.

Access To PHI

- HITECH - Expands access obligation where Covered Entity uses or maintains an electronic health record
 - Individual may access/obtain a copy of the PHI in electronic format
 - Individual may direct Covered Entity to deliver a copy of the electronic health record to a designated recipient

HIPAA - Privacy Rule



- Time and Manner of Access:
 - Covered entity must provide access in timely manner.
 - Must arrange convenient time and place for individual to inspect or obtain copy of PHI or mail copy of the PHI to individual (at individual's request).
 - Can require patient to request access in writing.
- Fees: Must be reasonable and cost-based, including only the cost of:
 - Copying, supplies and labor.
 - Postage.
 - Preparing an explanation or summary if agreed upon.



HIPAA - Right to Amend Medical Records

- Residents may request that you amend their medical record.
- If you agree, you must
 - Notify resident of the fact
 - Provide the amended record to person identified by resident as having received the original incorrect PHI.
 - Provide the amended record to persons you know have the resident's PHI and who have relied upon it to the detriment of the resident.



HIPAA - Accounting of Disclosures

- Residents have the right to know about disclosures.
- This requires you to document disclosures when they are made so you can provide the information.
- Exceptions:
 - Treatment, payment, healthcare operations
 - Disclosures to resident, family members involved in resident care.
 - Pursuant to residents authorization.

Disclosure Accounting

- HITECH – Eliminates TPO exceptions where Covered Entity uses or maintains an electronic health record
 - 3 years
 - Account for disclosures, including Business Associate or identify Business Associates
 - Subject to regulatory rulemaking

Marketing

Privacy Rule: In general, need patient's authorization before using PHI for marketing

- Marketing is defined broadly
- Exceptions:
 - ◆ Face-to-face
 - ◆ Promotional gift of nominal value



Marketing

HITECH Act

1. Communication by a Covered Entity/Business Associate encouraging recipients of the communication to purchase or use a product or service shall not be considered a “health care operation”, unless
 - i. for treatment
 - ii. case management/coordination of care
 - iii. to describe product-service provided by, or included in a plan of benefits of, Covered Entity making the communication
2. Not a health care operation if Covered Entity receives payment in exchange for making the communication unless qualifies for exception

No Selling Of PHI

HITECH

- With certain limited exceptions, prohibits covered entities and Business Associates from receiving remuneration in exchange for an individual's PHI, unless the Covered Entity obtains a valid authorization from the individual





Business Associate Agreement Changes

Before HITECH: **Contractual** obligation to
comply with HIPAA

HITECH: **Statutory** obligation to comply with
HIPAA's privacy and security provisions

- independent legal obligation to comply
- subject to civil and criminal enforcement

Federal Medical Records Laws: HIPAA - Privacy Rule

- Business Associates (“BA”)
 - Who/what is a BA?
 - Need a written contract with the BA regarding how PHI will be protected.
 - BA is now fully subject to HIPAA just like the CE.



Business Associates Agreements

- Establish permitted and required uses and disclosures
- Require BA to:
 - Not use or disclose other than as permitted by the contract or required by law
 - Use appropriate safeguards
 - Report unauthorized uses/disclosure
 - Ensure agents agree to same restrictions and conditions
 - Comply with access requirements

Business Associates Agreements

- **Require BA to: (continued)**
 - Make available for amendment
 - Account for disclosures
 - Make internal books and records available to HHS
 - Return or destroy PHI at termination or extend protection
- **Authorize termination if BA breaches material term of contract**

Federal Medical Records Laws: HIPAA - Privacy Rule

- Notice of Privacy Practices
- Privacy Officer
- Training
- Retention Requirements
- Safeguards
- Sanctions
- No Retaliation



The Security Rule



Federal Medical Records Laws: HIPAA - Security Rule

- Safeguards:
 - Administrative
 - Physical
 - Technical
- Implementation: Required v. Addressable
 - Reasonable and Appropriate
- Scalability and Flexibility of Security Rule
 - Size, complexity and capabilities of your organization
 - Costs of security measures
 - Probability and criticality of risks to ePHI





- Administrative Safeguards:

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Contingency plan
- Evaluation
- Business Associate contracts and other arrangements



- Physical Safeguards:



- Facility Access Controls
- Workstation use
- Workstation security
- Device and media controls





- Technical Safeguards:

- Access control
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security



Using PHI

- You are required to minimize the possibility that:
 - Visitors will see or hear private information.
 - ◆ Computer screens
 - ◆ Staff conversing
 - ◆ Flow sheets
 - Staff will see or hear private information that they don't need to see or hear to do their jobs.



Practical Security Measures

- Computer screens not in plain view
- Regularly change passwords
- Safeguard access to work areas
- Information accessible only to authorized staff, including medical records, lab reports, and faxes
- Controlled disclosure of information directly, email, fax



Additional Practical Practices

- Keep resident records locked, or at least in a place where visitors do not have routine access.
- Maintain a log or sign-in sheet that visitors must sign & date before permitted access to areas that may contain PHI.
- Handle resident charts in ways that prevent visitors from reading them.



Additional Practical Practices

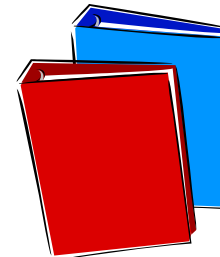
- Hold shift change meetings away from visitor traffic areas.
- Shred paper containing PHI.
- Conversations between co-workers regarding residents must occur away from visitors or staff who don't need to know.
- Minimize the chance that telephone conversations discussing a resident's condition are overheard.



Federal Medical Records Laws: HIPAA - Security Rule

- Security Rule Administrative Requirements:
 - Security Assessment
 - Security Officer
 - Complaint Procedures
 - Train the Workforce
 - Internal Sanctions for Violations

- Documentation Requirements:
 - Policies and procedures
 - Documentation



HIPAA COMPLIANCE AND ENFORCEMENT





The Federal Process

- HIPAA complaints are filed with the Department of Health and Human Services, Office of Civil Rights (OCR)
- The complaints are investigated in the OCR office
- Practitioner will be notified of complaint and given time to respond
 - Will not receive a copy of the patient's complaint



The Federal Process (cont.)

- OCR will review complaint and response.
- OCR can seek additional information, including conducting an on-sight investigation, witness interviews or an in-office document audit
- OCR will then determine whether sanctions are appropriate

Enforcement Statistics*

- Over 50,989 HIPAA Privacy Complaints received (since 4/03)
- Over 45,493 (89%) resolved
 - 10,515 – investigation and enforcement
 - 5,462 – investigation and finding no violation
 - 29,496 – cases closed, not eligible for enforcement

*From U.S. Department of Health & Human Services' website:
www.hhs.gov/ocr/privacy/hippa/enforcement/highlights/index.html (information as of March 31, 2010)



Enforcement

CVS Pharmacy, Inc. (January, 2009)

- \$2.25 million and implement Corrective Action Plan to ensure appropriate disposal of PHI
- Issues identified included failure to:
 - implement adequate policies and procedures,
 - train employees
 - maintain and implement a sanctions policy



Enforcement

- Two recent cases indicate that the government is taking a aggressive approach to enforcing HIPAA / HITECH
 - Cignet Health of Prince George's County, Md., ordered to pay a \$4.3 million civil monetary penalty for violating the HIPAA privacy rule – February 2011
 - The General Hospital Corporation and Massachusetts General Physicians Organization Inc. agreed to pay the U.S. government \$1 million to settle potential violations of the HIPAA Privacy Rule



Top Five Issues In Investigated Cases Closed with Corrective Action*

2009

Impermissible Uses and Disclosures

Safeguards

Access

Minimum Necessary

Complaints to Covered Entity

*From U.S. Department of Health & Human Services' website: [www.hhs.gov/ocr/privacy/enforcement/data/top5 issues.html](http://www.hhs.gov/ocr/privacy/enforcement/data/top5%20issues.html)

Impermissible Use and Disclosure

- Corrective actions included:
 - Apology
 - Sanctioned employee responsible
 - Trained billing/coding staff on appropriate claims submission
 - Revised policies/procedures to require specific request from worker's compensation carrier before submitting test results

Safeguards/Impermissible Uses and Disclosures



- Pharmacy employee placed customer's insurance card in another customer's prescription bag.
- OCR clarified card was PHI and needed to be safeguarded.
 - Steps taken:
 - ◆ Pharmacy revised its policies regarding PHI and retrained its staff.



Access

- Individual denied access to medical records on basis that portion of the record was created by physician not associated with the practice
- OCR noted while amendment provision of Privacy Rule permit denial of request for amendment when Covered Entity did not create that portion of record, no similar provision limits right of access
- Steps taken:
 - Revised access policy and procedures to affirm patient's have access to record regardless whether another entity created information contained within it.

Access

- Practice denied access to medical records due to outstanding balance for services
- Steps taken:
 - OCR provided technical assistance explaining that, in general, Privacy Rule required Covered Entity to provide access to record within 30 days of request, regardless of balance due
 - Practice provided copy of record to individual



Access

- Nurse practitioner accessed medical records of ex-husband
 - Steps taken:
 - ◆ Access to electronic records system terminated
 - ◆ Conduct reported to appropriate licensing authority
 - ◆ Nurse practitioner provided remedial training
- Supervisor accessed, examined and disclosed hospital employee's medical records
 - Steps taken:
 - ◆ Letter of reprimand placed in Supervisor's personnel file
 - ◆ Supervisor received additional training and counseled on use of medical information of a subordinate

Minimum Necessary

- Hospital employee left telephone message with daughter of patient detailing patient's condition and treatment plan. Message left at home number despite patient's instructions to contact her through work number.
 - Steps taken:
 - ◆ New procedures implemented to address minimum necessary requirements
 - ◆ Employees trained to review registration information for patient contact directions
 - ◆ Procedures incorporated into staff training – refresher series and yearly training.

Criminal Cases Brought Under HIPAA

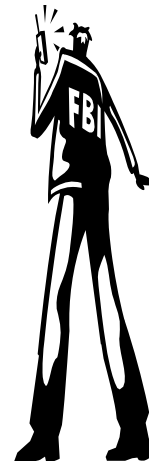
- 1) 2004 – first criminal conviction – Richard Gibson, an employee of the Seattle Cancer Care Alliance, a treatment center for cancer patients, obtained the name, date of birth, and Social Security Number of a patient. The information was used to obtain credit cards in that patient's name.
 - illegally disclosed individually identifiable information about a patient for economic gain
 - 16 months in prison
 - 3 years supervised release
 - Restitution



13 BHLR 1623 (Nov. 11, 2004)

Criminal Cases

- 2) March of 2006 – Physician practice employee convicted for selling (an FBI agent's) individually identifiable health information (to a confidential FBI informant)
- plead guilty, sentenced to serve six months in jail followed by four months of home confinement with a subsequent 2-year term of supervised release
 - Two aggravating factors:
 - i) employee sold the confidential medical records, and
 - ii) records belonged to a federal agent.



Criminal Cases

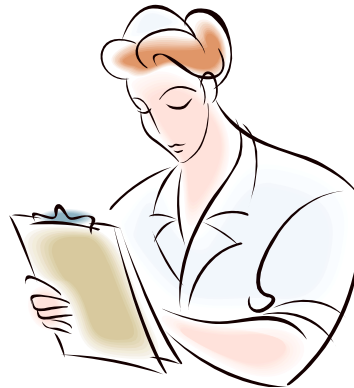


- 3) January 24, 2007 – Jury convicted man in first HIPAA violation case that has gone to trial.
- Employee at Cleveland Clinic in Florida accessed computerized patient files and downloaded individually identifiable health information on more than 1,100 Medicare patients. She sold the information to her cousin, who caused the stolen information to be used in connection with the submission of more than \$7 million in fraudulent Medicare claims, with approximately \$2.5 million paid to providers and suppliers.
 - Employee pled guilty to conspiracy and testified against her cousin; sentenced to serve 3 years probation, including 6 months home confinement and pay restitution.
 - Other individual was convicted; sentenced to 7 years, 3 months in prison and 3 years of supervised release and to pay \$2.5 million in restitution.

Criminal Cases

4) Northeast Arkansas Clinic – Nurse accessed patient’s medical file and shared contents with her husband who planned to use information in an upcoming legal proceeding.

- pled guilty to wrongfully disclosing a patient’s PHI and using it for personal and malicious intent
- now faces up to 10 years in prison, \$250,000 in fines or both



HIPAA GUIDANCE

OCR Website:

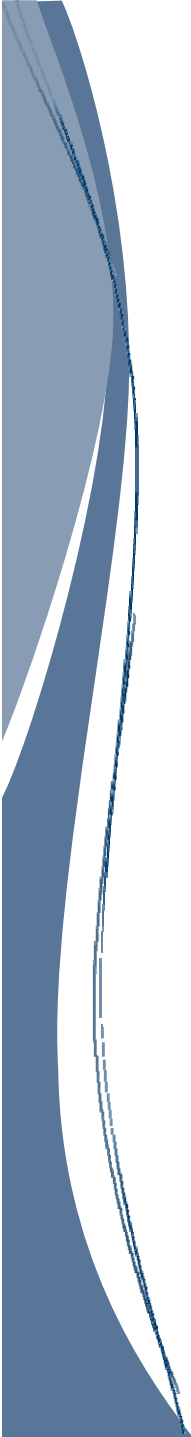
www.hhs.gov/ocr/hipaa/





Breach Notification Requirements for Unsecured Protected Health Information

- Interim Final Rule, August 24, 2009



General Rule: Covered Entity shall, following the discovery of a breach of *unsecured protected health information*, notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of a breach.



HITECH Act – Security Breaches

- Notification is only required if the breach involves “*unsecured Protected Health Information*”
- What is “Unsecured Protected Health Information”?

PHI not rendered unusable, unreadable or indecipherable to unauthorized individuals through use of technology or methodology specified by Secretary of DHHS

HITECH Act - Security Breaches

“Breaches” do not include the following:

- Unauthorized person not reasonably able to retain the PHI;
- Unintentional access or use by employee/individual acting under authority of the Covered Entity in course of duties and in good faith, if the PHI is not further acquired, accessed, used or disclosed; or
- Inadvertent disclosure by authorized individual at a facility operated by a Covered Entity or Business Associate to another similarly situated individual at the same facility, provided that there is no further acquisition, access, use, or disclosure



Definition of “Breach”

Acquisition, access, use, or disclosure of protected health information in a manner not permitted under any HIPAA exception which compromises the security or privacy of the protected health information.

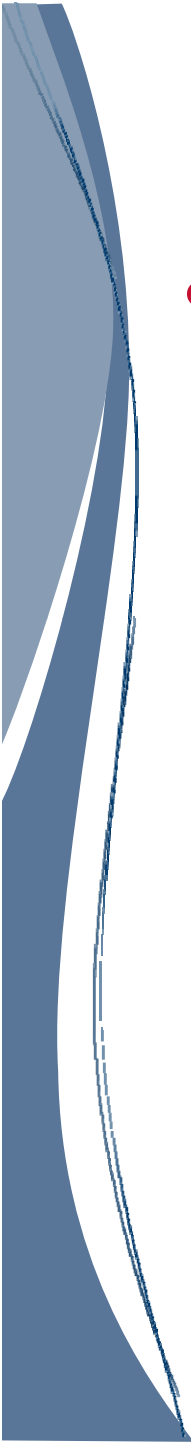
“Compromises the security or privacy of the protected health information” means poses a significant risk of financial, reputational, or other harm to the individual.

HITECH Act - Security Breaches

Increased Requirements for Notifying Patients of Security Breaches

- Must notify individuals without unreasonable delay
 - In no case later than **60 calendar days** after discovery
- Applies to PHI in both electronic and paper format



- 
- Breaches treated as discovered:
 - Covered Entity – as of first day breach is known, or, by exercising reasonable diligence would have been known
 - Knowledge deemed if known or by exercising reasonable diligence would have been known to any member of workforce or agent (other than person committing the breach).
 - Business Associate - similar



Business Associate Notification Obligations

- Notify Covered Entity following discovery
- Notice without unreasonable delay and no later than 60 days from discovery
- Identify each individual affected and information requested to be provided by Covered Entity



HITECH Act - Security Breaches

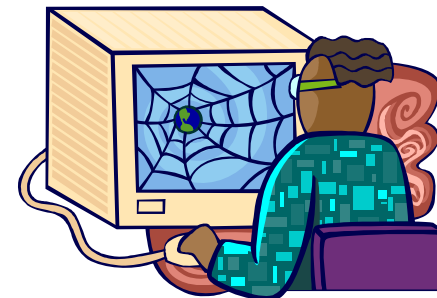
Written notice to patients must include the following:

1. Description of what happened, including the date of breach and date of discovery;
2. Description of the type of unsecured PHI involved;
3. Steps patients should take to minimize harm from breach;
4. Description of Covered Entity's efforts to investigate the breach, minimize its damage, and prevent future breaches; and
5. Methods of contacting Covered Entity to ask questions or obtain more information.

HITECH Act - Security Breaches

Notification Obligation (less than 500 patients):

- Written notice via first class mail
- If lack contact information for 10 or more patients, conspicuously post notice on home page of website or through major print or broadcast media
- Keep log of breaches



HITECH Act - Security Breaches

Notification Obligations (500 or more patients):

- Notify all individuals as discussed
- Notify Secretary of HHS
- Notify a major media outlet
- Covered Entity's name will be added to list on HHS website



Steps to Take Now

1. Review HIPAA changes and how they may impact your practices
2. Review BA Agreements and implement necessary changes
3. Review and revise policies and procedures, especially breach notification procedures
4. Train workers on new rules
5. Keep current on HIPAA as new rules and guidance are released

Questions?





Thank You

Isaac M. Willett

Isaac.willett@bakerd.com