The Health Information Portability and Accountability Act

By John R. Wible

March, 2005

1. Outline

- Overview
- Definitions and Applicability
- Administrative Set Up
- NOPP
- Privacy Rule and Privacy
- Releases with Authorization
- Releases without Authorization
- Accounting for Releases
- Breaches, Complaints and Sanctions
- Bioterrorism
- Security
- Additional Information

Overview – Why Document Any Way?

The "Golden Rule of Documentation:" if it ain't wrote down . . . it didn't happen**!**

Wible's Corollary - the way it is wrote down is the way it happened regardless of the way it happened.

HIPAA and Documentation

- Substantiates proof of services
- Provides continuity of care
- Documentation must be objective facts, not opinions
- HIPAA is all about documentation

Purpose of HIPAA
P.L. 104-191(1996)

Federal law that creates national standards for privacy of protected health information

- Access to PHI
- Accountability for PHI
- Privacy of PHI
- Security of PHI
- Automating the business process of claims administration
- Gets us Ready for the Online Medical Record

To What or Whom Does HIPAA Apply?

HIPAA applies only to "Covered Entities." The three "Covered Entities" under the Privacy Rule are:

- Health care providers that conduct certain "covered transactions" electronically
- Health care clearinghouses
- Health plans

Consequences of Being a Covered Entity

If you are a covered entity, you have duties under HIPAA, among them:

- Organizational Requirements
- Notice and Beneficiary Rights and Requirements
- Use and Disclosure Rule Requirements
- Security Requirements
- Transaction Code Requirements

HIPAA –What it Does
It Requires "Reasonable Efforts"

- Requires that there be no release of PHI other than as permitted by HIPAA
- Requires private areas for conversations
- Reasonableness is the key
- Common sense helps, too
- Really requires a lot of things we should have always been doing

HIPAA -What it doesn't do

- Does not override state laws that provide more patient privacy than HIPAA
- Many communications are not required to be encrypted
- Does not require major facility restructuring
  - No soundproof rooms
- Does not require that all risk of incidental disclosures of patient information be eliminated

  Examples:
  - Cubicles or private areas
  - Shield-type dividers
  - Sign-in sheets

HIPAA - What it Also Doesn't Do

No Reporting Change . Especially from the Health Department standpoint
Providers still report to us as usual.

HIPAA what it Also Doesn't Do - Relationships

Nor does it mean that the relationship between the provider and the Health Department changed.

HIPAA and State Law

State medical privacy rules are preempted by the HIPAA Privacy Rule only if they are less stringent than the Privacy Rule or contrary to it.

Definitions and Applicability

- Authorizations
- Protected Health Information (PHI)
  - Individually Identified Health Information
  - De-Identified Health Information
- Health Care Providers
- Health Care Plans and Clearinghouses
- Affiliated Entities
- Hybrid Entity
- Covered Transactions
- Business Associates (BAs)
- Minimum Necessary Concept

Authorization

A document a patient signs to authorize a Covered Entity to use or disclose an individual's PHI for any purpose described in the document

PHI and Its "Daughters"
Health Care Provider

- This term is broadly defined under HIPAA to include individual physicians, physician group practices, dentists, health care practitioners, hospitals, nursing facilities, assisted living facilities, hospice and other similar facilities
- It includes all the staff at such facilities
- They furnish, bill or receive payment **ELECTRONICALLY** for health care services in the normal course of business
- It does not include facilities or persons who do not provide health care such as schools, fire departments, police agencies

Health Care Plan

A health plan is any individual or group health plan that provides, or pays the cost of, health care.

- Typically, an insurance company like Blue Cross/Blue Shield
- It includes group health plans, Medicaid agencies and Medicare, health insurance issuers and HMOs, and any other plan which pays for health care

Health Care Clearinghouse

A health care clearinghouse is a public or private entity that transforms health care transactions from one form to another

- It includes billing services, re-pricing companies, and, in some cases, banks
- They "crunch numbers" involving PHI

Affiliated Covered Entity

- Legally separate covered entities that designate themselves as a single covered entity under common control or ownership
- May or may not be in close proximity
- Examples could be Department of Public Health or all Baptist Hospitals

Hybrid Entity

- Single entity that is a Covered Entity but that engages in both covered and non-covered functions and that designates health care components as provided in the privacy regulations. 45 C.F.R. §164.504(a)(2000).
  - Example: a conglomerated health and welfare plan that includes plans covered by the Privacy Rule as well as disability and life insurance plans not covered by the Privacy Rule.)
  - Example: Public Health Department which provides individual health care services but also provides other non-individual or non-health care services such as disease control and environmental services

Covered Transactions

- Health care claims (bills) or encounter information
- Health care payment/ remittance advice
- Coordination of benefits
- Health care claim status
- Enroll/disenroll information in health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments
- Other transactions involving PHI

Business Associates

Business Associates (BA) are typically a non-covered entity or vendor that performs, on behalf of covered entity, a function or activity involving the use or disclosure of PHI

- Examples: lawyers, accountants, actuaries, consultants
- Usually a professional, not the cleaning service. However, ADPH likes to consider anyone who has unrestricted and unsupervised access to our area a BA
- Though typically a non-covered entity, a BA can be a covered entity in its own right (i.e., a clearinghouse)

Doing Business with Business Associates

•Covered entities must require BAs to meet HIPAA privacy and security requirements by contract using specific terms set out in regulations. See 45 CFR § 164.504(5)
•ADPH has a standard BA agreement adapted from the Feds
•BAs do not have to monitor compliance like covered entities do
•However, BA agreements should require BA to report a breach to the agency so the agency can make sure appropriate is done since HHS could audit the agency

Business Associate Agreement

There must be a BA Agreement
•Agreement is to protect the privacy and security of PHI created or held by the business associate on behalf of the covered entity
• It sets out the responsibilities of the business associate.
• May include representations by the covered entity on which the business associate can rely.
•Particular attention to indemnity provisions is important in amending Business Associate contracts
•A sample Business Associate contract is available on the HHS website at http://www.hhs.gov/ocr/hipaa/assist.html

Minimum Necessary Concept

- The concept of minimum necessary is that Covered Entities and their Business Associates should not use or disclose PHI beyond what is reasonably necessary for the purpose of the use or disclosure
- This is a key concept under the Privacy Rule
- Concept is inapplicable if the patient signs written authorization

Administrative Setup

Covered Entities have administrative requirements under HIPAA and should be in compliance by now. Agencies must:

- Perform an internal "gap analysis" to determine where the fall short of meeting HIPAA requirements
- Appoint a privacy officer
- Write policies and procedures and necessary documents
- Institute necessary changes to comply with internal HIPAA policies and procedures
- Build "firewalls" between the "need to knows" and the "don't need to knows"
- Train, train, train all existing and new employees

HIPAA Privacy Officer

The agency designates a Privacy whose duties include:

- Implementing privacy policies
- Overseeing training
- Assuring that safeguards are in place to protect PHI
- Establishing sanctions for misbehavior and apply them as necessary

- Mitigating the harmful effects of wrongful disclosures
- Maintaining necessary Privacy Rule documentation for 6 years
- Establishing a complaint procedure for patients who believe their Privacy Rule rights have been violated.

Policies and Procedures

Policies and procedures must address at least the following:

- Privacy uses and disclosures
- Notice of Privacy Procedures (NOPP)
- Authorization forms
- Security
- "Minimum necessary"
- Complaints and breaches
- Records retention
- Plans for physical, administrative and technical safeguards
- Verification procedures
- Policies on no waiver of rights/retaliation

Additional Documents

- Access request forms
- Amendment request forms
- Restriction request forms
- Confidential communication request forms
- Complaint forms
- Disclosure accounting forms
- Disclosure log/minimum necessary log
- HIPAA Quash
- Business associate agreements

How to build a "firewall"

- Evaluate which employees should have access to PHI (separate the "need to knows" from the "don't need to knows")
- Implement the procedure to ensure
  - that only the designated employees have access to PHI,
  - that even the designated employees only have access to the minimum necessary amount for administrative functions
- Describe the "firewall" procedures in the plan document

Training

- HIPAA Training Requirements. See 45 CFR § 164.528
  - General manual
  - New Employees
  - Existing Employees
  - Policy on Confidentiality
- Patient Request for Protection of PHI 45 CFR § 164.522

Notice of Privacy Practices (NOPP)

HIPAA requires that the agency have and distribute to patients a Notice of Privacy Practices. See 45 CFR § 164.520

- It details the agencies privacy practices as they relate to each patient
- Copies must be offered and available to patients
- The Local Agency Identified
- NOPP should be posted at facility and on your Website

NOPP

- Patients should acknowledge receipt of the NOPP. See 45 CFR § 164.520
- ADPH has this acknowledgement in the CHR.
- Concept of minimum necessary must be addressed in the NOPP. 45 CFR §164.514

Summary of the HIPAA Privacy Rule:

Health plans, health care providers and health care clearinghouses may use PHI (protected health information) only as permitted or required by the Privacy Rule.

Use and Disclosure Decision Tree

- Are you a covered entity?
- Is it PHI?
- Is the use or disclosure permitted or required by the Privacy Rule?
- Does it fall within the minimum necessary requirements?
- Is verification required?
- Is documentation required (use disclosure log?)
- Is an authorization necessary?
- Is it subject to an exception?

Privacy Regulations 45 C.F.R. Parts 160 and 164

You can use protected health information (PHI) without the patient's authorization for:

- Treatment - provision, coordination or management of health care and related services
- Payment - includes the various activities of health care providers to obtain payment or be reimbursed for their services
- Operations – administrative, financial, legal, and quality improvement activities that are necessary to support the core functions of treatment and payment

Disclosures with and Without Authorizations

Authorizations – Contents

- The typical release of PHI is with a written authorization
- HIPAA Authorizations Must Address the following:
  - identify the specific persons or classes of person that are authorized to make the disclosures
  - identify the persons or classes of persons to whom the disclosure would be made
  - contain a relevant expiration date
  - include a statement of the individual's right to revoke the authorization

Authorization Form

- One authorization form may be used to authorize uses and disclosures by classes or categories of persons or entities
- One authorization form may be used to authorize classes of persons to whom disclosures are authorized
- The entire medical record may be disclosed
- There must be an expiration date which can be indefinite, if so stated

Signing the Authorization

- You must verify the signor
- Copy, fax or e-mail of signed authorization is valid if reliable
- The authorization can apply to PHI created after the date authorization signed if it encompasses later created information
- Notary or witness not required
- Retain copies for 6 years

Disclosures Without Written Authorization

- Disclosures to Public Health
- Disclosure to Law Enforcement
- Protection of the President of other government officials
- Domestic violence and child and elder abuse authorities
- Subpoenas – civil or criminal or grand jury
- Terrorism and Bioterrorism Events and Drills
- "Otherwise provided by Law"

Disclosure to Public Health

Covered entities may disclose PHI without authorization to a public health authority:

- For the purpose of preventing or controlling disease, injury, or disability [45 CFR § 164.512(b)]
- For vital records purposes
- For conducting public health surveillance
- To make disclosures that are required by other laws, including laws that require disclosures for public health purposes.

Disclosure to Law Enforcement

Who is "Law Enforcement?"

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
(1) Investigate or conduct an official inquiry into a potential violation of law; or
(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Disclosure By Law Enforcement

- Since law enforcement agencies are not "covered entities," the may disclose information without regard to HIPAA
- Disclosures are governed by the rules that have traditionally been applied involving confidentiality

The issue is whether a "covered entity may disclose PHI to law enforcement

Disclosure to Law Enforcement

Disclosure without written authorization may be made to law enforcement authorities . See 45 CFR § 164.512

- To state and federal authorities
- Pursuant to process and as otherwise required by law. 45 CFR §164.512(f)(1)
  - wounds treated
  - Dog bites
- For identification and location purposes (limited information only). See 45 CFR §164.512(f)(2)

Requests for Disclosure to Law Enforcement

The request may come in by:

- Operation of law – wounds and dog bites
- A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; A grand jury subpoena; or
- An administrative request – a verbal notice is sufficient is the officer is identified.

Requirement to Release

- The information sought must be relevant and material to a legitimate law enforcement inquiry
- The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
- De-identified information could not reasonably be used.

Disclosure for Location Purposes

With certain exceptions for disclosures required by law, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that only certain limited information is given

Only Certain Information

The covered entity may disclose only the following information:

- Name and address;
- Date and place of birth;
- Social security number;
- ABO blood type and rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Exception

Except as permitted by the previous slide, the covered entity may not disclose for the purposes of identification or location any PHI related to

- the individual's DNA or DNA analysis
- dental records
- typing, samples or analysis of body fluids or tissue.

Disclosure to Law Enforcement(2)

- In response to request for such information about an individual who is or is suspected to be a victim of a crime. 45 CFR §164.512(f)(3)
- For purpose of alerting law enforcement official about a suspicious death. 45 CFR §164.512(f)(4)
- For purpose of reporting evidence of criminal conduct occurring on premises of covered entity. 45 CFR §164.512(f)(5).
- A provider who is providing care in response to a medical emergency my alert law enforcement regarding information pertaining to crime. 45 CFR §164.512(f)
- Child or Elder Abuse
- Immediate threat to public health

Crime Victims

A covered entity may disclose PHI in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime if the individual agrees to the disclosure; or

Disclosures about Decedents

A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

Crime on the Premises

A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

Emergencies

A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

- The commission and nature of a crime;
- The location of such crime or of the victim's) of such crime; and
- The identity, description, and location of the perpetrator of such crime.

Emergencies from Abuse, Neglect or Domestic Violence

If a covered health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, different rules apply. See *supra.*

Uses and Disclosures to Avert a Serious Threat to Health or Safety

A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, 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; and
- Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

Uses and Disclosures to avert a serious threat to health or safety.

- Is necessary for law enforcement authorities to identify or apprehend an individual:
- Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

- Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in §§ 164.501.

Law Enforcement's Representations

Disclosure without agreement may be made if

- The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
- The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree; and
- The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Limitations on Release

A use or disclosure may not be made if the information is learned by the covered entity:

- In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure,
- In the course of counseling or therapy; or
- Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy

National Security

A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

Protection of the President

A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

Correctional institutions and Other Custodial Situations

A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

- The provision of health care to such individuals;
- The health and safety of such individual or other inmates;
- The health and safety of the officers or employees of or others at the correctional institution;

- The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
- Law enforcement on the premises of the correctional institution; and
- The administration and maintenance of the safety, security, and good order of the correctional institution.

Reports of Domestic Violence or Child Abuse and Neglect

- § 164.512 permits a covered entity to use or disclose protected health information without the written consent or authorization of the individual to "a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;"
- This is different from disclosure to law enforcement in general because is has none of the limitations placed on the disclosures to law enforcement in general.

Judicial Authorities - Subpoenas

- Subpoenas must be HIPAA compliant
- Must have language that advises and protects the third party subpoenaed.
- ADPH employees follow ADPH policy on Subpoenas (under revision)

Accounting for Releases

- In the patient's chart
- In the general HIPAA Log

Disclosures, Accounting, Denial, Amendments

- Written Accounting of Disclosures. See 45 CFR § 164.528
  - The Agency (County) HIPAA Accounting Form
  - 60 day response time
- Denial of Request for PHI/Disclosure Restriction – above
- Amendments to PHI 45 CFR § 164.526
- Record all in the chart and in the log

Breaches of Privacy

- Procedure
- Notifications
- Reporting
- Remediation
- Discipline
- Criminal Penalties
- Civil Causes of Action
- To whom do the penalties apply?

Complaint and Breach Procedure

45 CFR § 164.530(d) provides for complaints by any patient concerning use or disclosure of PHI

- In the NOPP, "where to complain?" must be addressed.
- May be to HHS Office of Civil Rights
- More likely, to agency privacy officer

Agency also has duty to have internal procedure to deal with breaches. See 45 CFR § 164.530(I-j).

- ADPH uses "AIR Form" reports followed up by the Office of General Counsel

Complaints

When complaints or notice of breaches are received by privacy officer, the agency has a duty to:

- Investigate
- Mitigate
- Resolve
- Respond
- Document activities relating to the investigation, mitigation and response in HIPAA Log
- No report to HHS is required, though the process is subject to compliance audit

Complaints/Sanctions – Agency Action

- The agency's response may require amendment of privacy policies and procedures.
- Response may requires employee sanctions for employee breaches. See 45 CFR § 164.530(e-g)
- ADPH defines this in Policy 03-03

Civil Penalties for failure to comply with HIPAA Privacy Rule?

- Civil penalties of up to $100 per violation, with the total amount imposed on an employer for all violations of an identical requirement during a calendar year not to exceed $25,000
- Note that the penalty goes against the agency, not the employee. Employee is to be sanctioned by the agency

Criminal Penalties

- A person's knowing use or disclosure of PHI in violation of HIPAA may result in criminal penalties of up to $50,000 in fines and one year in prison.
- Uses or disclosures made under false pretenses may result in criminal penalties of up to $100,000 in fines and 5 years in prison.
- HIPAA Privacy Rule violations committed with intent to sell, transfer or use PHI for commercial or personal gain or malicious harm are punishable by a fine not to exceed $250,000 and/or 10 years in prison.
- Recent case in the Northwest has a hospital employee in big trouble.

Civil cause of action?

Does a violation of the HIPAA Privacy Rule create a civil cause of action?

Not directly, but indirectly it does. The HIPAA Privacy Rule does not within itself create a civil cause of action. However, a failure to follow HIPAA privacy procedures may become the "standard of care" in common law breach of privacy actions under state law

HHS Office of Civil Rights Enforces the HIPAA Privacy Rule

The Department of Health and Human Service ("HHS") Office of Civil Rights enforces HIPAA**.** Complaints must be filed with the Secretary of HHS within 180 days of the date that the complainant knew or should have known of the act or omission on which the complaint is based. See 45 C.F.R. §160.306

HHS Preferred Complaint Procedure

When a written complaint is filed, typically

- OCR/CMS will call you in attempt to resolve
- If not resolved, HHS will investigate
- Looking for good faith compliance
- If not compliant, show good faith efforts toward compliance or submit a corrective plan
- Focus is on education and assistance, not investigation and audits
- Will impose monetary penalties if necessary

HHS Penalty Procedure

If the civil penalty procedure is invoked the following applies:

- HHS sends a written notice of intent to impose penalty
- Agency has 60 days to request a hearing
- If no request for a hearing, penalty can be imposed without the right to a hearing or appeal
- HHS can collect the penalty in federal court
- There is a 6 year statute of limitations from date on which latest act or omission occurred
- Hearings will be before an ALJ who must issue decision within 60 days after time for submission of post-hearing briefs and reply briefs.

HIPAA in the Field – Disasters and BT Incidents

- Is HIPAA still in force in a disaster? -Maybe, maybe not.
- How do we respond? The same way we've always responded in a disaster. Use principles of "minimum necessary" and "common sense"

Applicability – HHS Says:

- Agencies will need to get PHI to respond to emergencies;
- Communications in such times is difficult at best;
- Therefore even a "covered entity" can disclose PHI in such an event.
- See 45 CFR 164.512(b) for public health activities.

Applicability- In a Disaster

The Privacy Rule permits disclosure

- Disclosure of PHI to "public officials" to lessen the effects of the emergency. 45 CFR 164.512(j)
- To law enforcement for their necessary activities. 45 CFR 164.512)(f); (see *supra.)*
- To national security and intelligence agencies. 45 CFR 164.512)(k)(2);
- To judicial authorities. 45 CFR 164.512

HIPAA – The Bottom Line

HIPAA is not designed to get in the way of a true emergency !

Additional Materials

- Websites

Statute - http://aspe.hhs.gov/admnsimp/pl104191.htm
Regulations - http://www.hhs.gov/ocr/hipaa/finalreg.html
HHS Interpretations and FAQs -
http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php