Public Health Law 101: The Law of Privacy and Confidentiality

Faculty

John R. Wible, General Counsel
Office of General Counsel
Alabama Department of Public Health

ADPH Office of General Counsel
(334) 206 - 5209

Documentation

- Substantiates proof of services
- Provides continuity of care
- Documentation must be objective facts, not opinions

The Golden Rule of Documentation

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!

Confidentiality - Access to Records in General

- All patient information is strictly confidential
  - –Policy on confidentiality 2003-003
- Some bad scenarios
- Bad scenarios equal bad liability

Conditions for Release of Information

- Prior written consent
  - –Patient
  - –Parent/guardian
- Subpoena in accordance with departmental/institutional policy
- Otherwise provided by law

TB/STD/DB Records are Confidential

- Not revealed even by subpoena
- Not admissible into evidence except for commitment hearings
- ADPH requests for notifiable disease records to be forwarded to Legal
  - Call 334-206-5209
- See ADPH Policy 04-02 for specifics

Disease Control Guidelines

- Information considered public
  - Final completed report written in black, not identifying any persons
  - The name of businesses, establishments, restaurants involved in an investigation
  - Aggregate statistical information

Disease Control Guidelines

  - Any other public records
  - Regular environmental and daycare inspection reports

Confidential Information (EPI)

- Epidemiologic interview sheets
- Information provided by a required reporting entity
- Work papers, notes and analyses
- Actual numbers of cases, sample sizes or any other description which may identify any person

Confidential Information (EPI)

- Correspondence including on a particular investigation
- Complaint generated environmental and other inspection reports
- Incomplete drafts of reports
- Other documents received privately

Released With Authorization

- A notifiable disease record generated by the Department or in the possession of the Department (such as electronic laboratory reports or facsimile lab reports) that concerns the symptoms, condition or other information specific to an individual

Written Authorization not Required

- Transfer information from one county health department to another or to the state office
- Transfer information to physicians, health professionals with contract or other provider arrangements to provide care

Written Authorization not Required

- Some practitioners require consents to transfer out of abundance of caution

What Makes a Valid Authorization?

- Description of use info to be released
- Name or description of info receiver
- Name of patient
- Description of the use of the info
- Expiration date or continuous
- Right of revocation by patient

What Makes a Valid Authorization?

- Notice of possible re-disclosures
- Signature of pt or representative
  - See CHR Form 6A and instructions

Release of Contact Information

- Don't
  - Release the medical record or information regarding STD/TB/disease control without the written consent of the patient
    - Even with consent, it should not include contact information

Release of Contact Information

- Don't
  - Write identifying information about how the patient contracted the disease

Confidentiality - Access to Minor's Medical Records

- If a minor is qualified to consent and signs the "consent for treatment," only the minor can sign to release the information regarding those services

Confidentiality - Access to Minor's Medical Records

- If the parent/guardian signs the consent for treatment, the parent/guardian or the minor may consent for the release

Access to Minor's Medical Records Parents' Rights

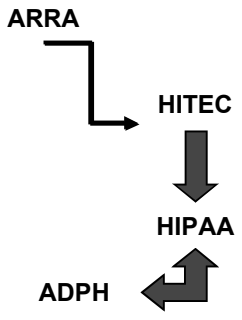
- All information pertaining to a child must be equally available to both parents
  - –However, if the child gave consent for services, neither parent may have access to the records without that child's consent
  - –*Code of Ala*, § 30-3-154

The Health Information Portability and Accountability Act (HIPAA) (Amended by HITEC)

HIPAA Background

- Passed August 21, 1996
- Designed to simplify healthcare delivery
- Provided for portability of pre-existing health conditions
- Standardized confidentiality and security
- First such federal act of its kind
- HHS makes the rules

The Stimulus Package



Key Questions for Public Health Practitioners

- What is HIPAA?
- What is the HIPAA Privacy Rule?
- Who does the Privacy Rule cover?
- How is PHI regulated?
- How are uses/disclosures of PHI regulated?
- What is the Security Rule?
- How does it work?

HIPAA Privacy Rule: How PHI is Covered

- Boundaries
  - –Set limits on uses & disclosures
- Fair information practices
  - –Allow individuals some level of access to their health data
- Accountability
  - –Make covered entities accountable for handling and abuses

How Uses/Disclosures Are Regulated

- Uses or disclosures of PHI require either
  - –Written authorization or
  - –Individual opportunities to object
- Covered Entities (CEs) may use or disclose PHI without individual's informed consent for exceptions specified in rule

Key Questions for Public Health Practitioner

- What is the relationship of the Privacy Rule to other laws?
- How are violations addressed?
- Is a public health agency a covered entity?

HIPAA & the Basis for Health Information Privacy Protections

- HIPAA - increase individual access to health insurance by
  - –Reducing health insurance costs
  - –Lowering claims costs
  - –Efficiently transmitting electronic data under enhanced privacy protections

HIPAA & the Basis for Health Information Privacy Protections

- HIPAA
  - – First national set of standards for protecting health information privacy
  - – The Privacy Rule implements HIPAA
  - – Privacy Rule regulates the use and disclosure of PHI by CEs

The Privacy Rule: What is Covered?

- Protected Health Information (PHI)
  - Individually-identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally
  - 45 C.F.R. §160.103

Uses Without Written Consent

- Treatment
- Payment
- Operations
- Where required by law

Who is Covered?

- Covered Entities (CEs)
  - Health care providers that bill
  - Hybrid entities (*like ADPH*)
  - Health care plans
  - Health care clearinghouses
    - 45 C.F.R. §160.103

Business Associates

- Business associates follow the same level of protection in the privacy rule and include
  - Claims or data processors
  - Billing companies and financial service providers
  - Quality assurance providers and utilization reviewers

Business Associates

- Lawyers, accountants & other professionals
  - 45 C.F.R. §160.103

Business Associates & AARA

- Must also adhere to Security Rule like CEs
- Establish administrative, physical, and technical safeguards for PHI
- Establish policies and procedures for safeguards
- Only use or disclose PHI in accordance with HIPAA

Business Associates & AARA

- Violation for knowing of a pattern of activity or practice by the CE that would constitute a violation and not reporting to HHS
- Same types of penalties and criminal sanctions as CEs for HIPAA violations

HIPAA Privacy Rule: Who is Not Covered?

- Life insurance companies
- Auto insurance companies
- Workers' compensation carriers
- Employers
- Others who acquire, use, and disclose vast quantities of health data

HIPAA Privacy Rule: Who is Not Covered?

- AARA may place some requirements
  - –PHI cannot be bought and sold

HIPAA Privacy Rule: What is Not Covered?

- PHI does not include
  - –Education records covered by FERPA
  - –Employment records held by a covered entity in its role as employer
  - –Non-identifiable health information
    - 45 C.F.R. 160.103

HIPAA: What it Doesn't Do

- Does not override state laws that provide more patient privacy than HIPAA
- Does not require that all risk of incidental disclosures of patient information be eliminated
  - –Cubicles
  - –Shield-type dividers
  - –Sign-in sheets

HIPAA and ADPH Privacy

- See ADPH HIPAA Privacy Policy 06-008
  - –"Minimum Necessary" Concept
  - –Patient verification
  - –Fax confidentiality
  - –The "HIPAA Log"
  - –Breach sanctions
- See CHR manual as well

How Uses/Disclosures are Regulated

- Minimum necessary rule
  - When using or disclosing PHI, a covered entity must make reasonable efforts to limit such information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request

Impact of the Privacy Rule on Public Health

- Externally
  - Impacts flow of identifiable health data into or out of public health agencies
- Internally
  - Impacts practice of public health or public health research by public health agencies or its partners

HIPAA - Disclosures Permitted

- "Minimum" info may be disclosed to
  - Public officials
  - Public health
  - Law enforcement
  - National security & intelligence agencies
  - Judicial authorities
  - Researchers
  - DHR for abuse reporting

Disclosure to Law Enforcement Officials

- Not required
- Pursuant to subpoenas or by verbal request
- As "otherwise required by law"
- For ID and location purposes
- Do not give disease information
- Individual is a victim of a crime

Disclosure to Law Enforcement Officials

- To alert about a suspicious death
- When criminal conduct occurs on premises
- In emergency setting, to alert regarding information pertaining to crime

Disclosure for National Security

- CEs may disclose PHI to authorized federal officials for the conduct of intelligence, counter-intelligence, and other national security activities

Disclosure to Public Health

- Permitted to
  - "Public health authority that is authorized by law to collect and receive such information for the purpose of preventing and controlling disease, injury, or disability, including… reporting of disease… and the conduct of public health surveillance…."

External Impact of the Privacy Rule on Public Health

- Examples of specific public health-based exceptions include disclosures
  - To maintain the quality, safety, or effectiveness of FDA products
  - To notify persons exposed to communicable diseases

Child or Elder Abuse Notice

- Examples of specific public health-based exceptions include disclosures
  - About victims of abuse, neglect, or domestic violence
  - To prevent serious threats to persons or the public

Decedent's Information

- May be released to
  - Law enforcement
  - Transporting emergency medical personnel
  - Coroners and their personnel
  - Mortuary personnel
  - Bureau of Health Statistics

HIPAA and Research With Authorization

- Research
  - "Systematic investigation designed to develop or contribute to generalizable knowledge"

HIPAA and Research With Authorization

- The Privacy Rule permits use or disclosure of PHI for research if the subject of the PHI has granted specific written permission through an authorization that satisfies 45 CFR §164.508

Research Without Authorization

- Reviews preparatory to research
- Decedents
- Waiver of authorization or alteration of an authorization by an IRB
- De-identified information
- Limited data set with certain identifiers deleted
- Grandfathered consent

HIPAA Security Rule

- Primary objective
  - "Protect the confidentiality, integrity, & availability of EPHI when it is stored, maintained, or transmitted"

HIPAA Security Rule

- Applies to identifiable *electronic protected health information (EPHI)* related to
  - Past, present or future medical or mental condition
  - The individual's health care
  - Payment records

Security Rule - 3 Categories

- Administrative safeguards
- Physical safeguards
- Technical safeguards

Documentation Standard

- Maintain documentation of policies and procedures for 6 years
- Make documentation available to workforce who administer the policy
- Review documentation periodically
- Ensure the confidentiality, integrity, and availability of EPHI

ADPH Security Policy

- Requires security of the premises
  - Door locks
    - See ADPH Security Policy No. 05-16
- Security of electronic records (computer security)
- Security of the paper
- Security of your mouth

Use of Department Computers

- Use ADPH furnished equipment and software
- CSC/Tech Support will purchase and install all network-connected devices
- Use password protection & disclaimer
- CSC/Tech Support will install software updates

Use of Department Computers

- Connect laptops to the network once a month
- Back up critical data
  - –See ADPH Policy 2005-016 and Security Manual

Use of Computers

- Change password every 60 days
- Use only for lawful activity
- Report suspected viruses & attacks
- Supervisors notify CSC on new employee starting or leaving
- Appropriate salvage of computers
- Limit department workspace
- Wear badges

Patient Accounting

- Patients may ask for a listing of disclosures of their PHI for up to six years prior
- The following disclosures are NOT required to be accounted for
  - –Treatment, Payment, Healthcare Operations (TPO)

Patient Accounting

- –Disclosures to the patient or persons involved with their care
- –Disclosures authorized by the patient or authorized representative

Patient Accounting

- Other disclosures not required to be accounted for
  - –National security or intelligence purposes
  - –Correctional institutions or law enforcement
  - –Incidental disclosures
  - –Limited data sets used for research purposes

Accounting

- An accounting is required for disclosures of which the patient may not be aware
- If we have it in electronic form, we may be required to give it in electronic form

HIPAA Log

- A single file which relates to pt files
- Kept with medical records
- Documents "non-routine" disclosures
  - –Date of the disclosure
  - –The name/address of receiver
  - –Brief description of PHI disclosed
  - –Brief statement of the purpose of the disclosure

Required Logged Items

- Unauthorized releases on the AIR Form
- Releases required by law
- Releases based upon subpoena
- Releases to law enforcement for ID
- Requests to limit releases
- Requests to amend or correct PHI

Required Logged Items

- Requests by the patient for accounting
- Reports about victims of abuse, neglect, or domestic violence

Disclosures Not Required to Log

- TPO disclosures
- Disclosures made to the patient or rep.
- Pursuant to a valid authorization
- National security or intelligence purposes

Disclosures Not Required to Log

- To a correctional institution or law enforcement official that has custody of a patient
- To a health oversight official

HIPAA Breaches

- When there is a breach of protected info, the CE has a duty
  - To report to or notify clients
  - To report to HHS and the media if >500
  - To mitigate the damage
  - To examine employees, policies, equipment and facilities to prevent it happening again

Breaches - Penalties

- Breach may subject employees and the CE
  - To criminal penalties
    - Up to $250,000
  - To HHS civil penalties or lawsuits
  - To adverse employment action

Program Management

- The HIPAA program and certain other similar programs are under the management of the Risk Management Committee
- Committee proposes HIPAA policy changes

Program Management

- Committee receives and processes all accident/incident reports including possible HIPAA breaches
- The Committee oversees Red Flag instances

Red Flag Regulations

- Federal Trade Commission regulations designed to protect against identity theft
- As a "creditor," ADPH has "covered transactions" with clients/patients
- ADPH has a duty to be on the lookout for certain red flags

Categories of "Red Flags"

- Alerts, notifications, or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personally identifying information, such as a suspicious address

Categories of "Red Flags"

- Unusual use of – or suspicious activity relating to – a covered account
- Notices from customers, victims, law enforcement authorities, or businesses about possible identity theft

See Also Policy Documents

- 98-07 Fax Policy
- 03-03 Confidentiality Policy
- 03-10 Notice of Privacy Practices (NOPP)
- 03-33 Personnel Records Policy
- 03-30 Vital Records Policies
- 04-02 Receipt of Legal Documents

See Also Policy Documents

- 04-03 Personnel Manual
- 05-16 HIPAA Security Policy/Manual
- 06-08 HIPAA Privacy Policy

CDC Training Resources Law and Public Health Emergencies

- Public Health Emergency Law 3.0
- Forensic Epidemiology 3.0

Available at:

www.cdc.gov/phlp