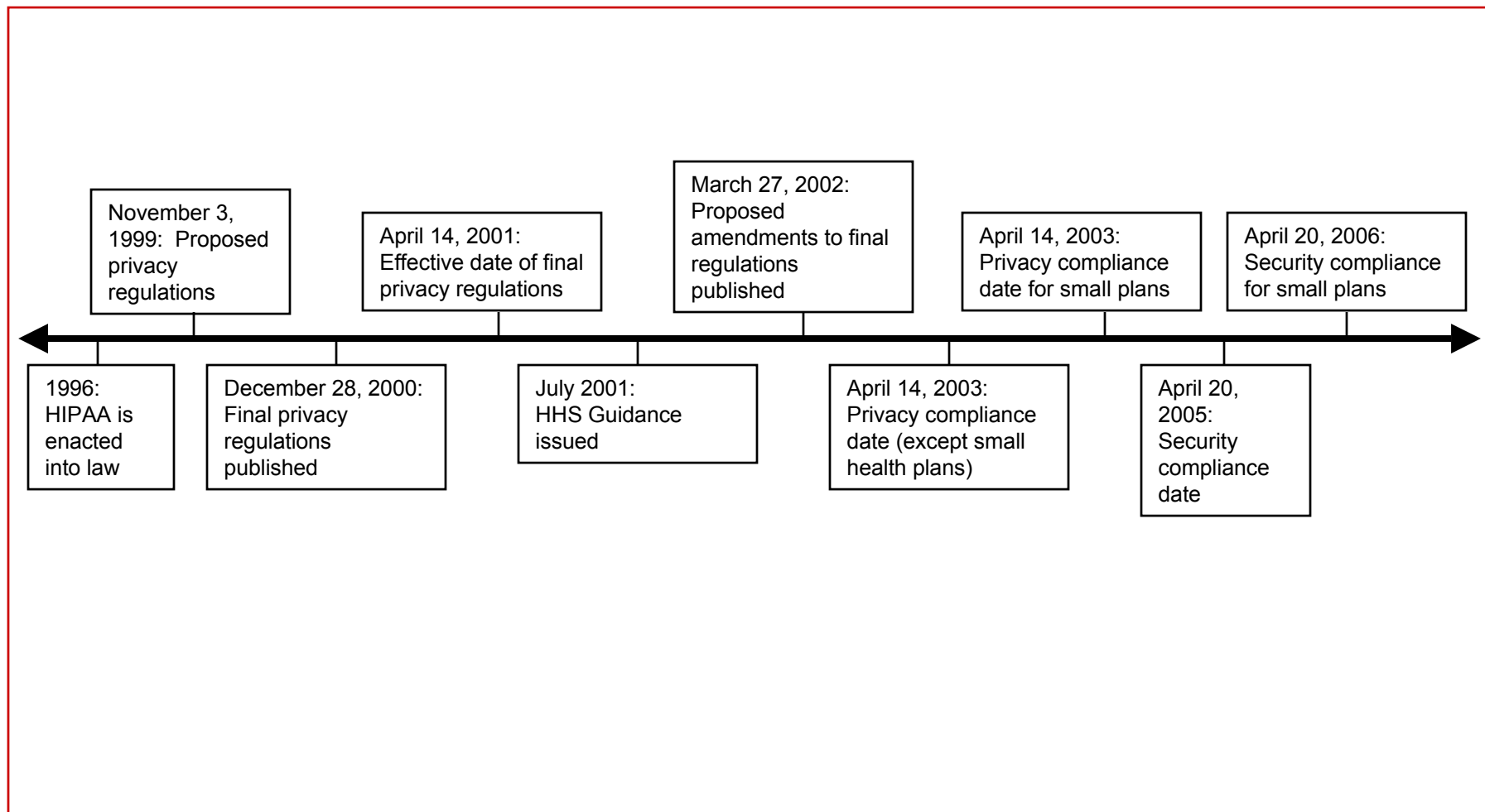


Advanced HIPAA Privacy Compliance Strategies: Those Nagging Issues That Don't Seem to Go Away

Rebecca L. Williams, RN, JD
Partner; Co-Chair of HIT/HIPAA Practice Group
Davis Wright Tremaine LLP
Seattle, WA
beckywilliams@dwt.com



HIPAA Privacy — A Timeline



HIPAA Roulette



The Enforcement Rule

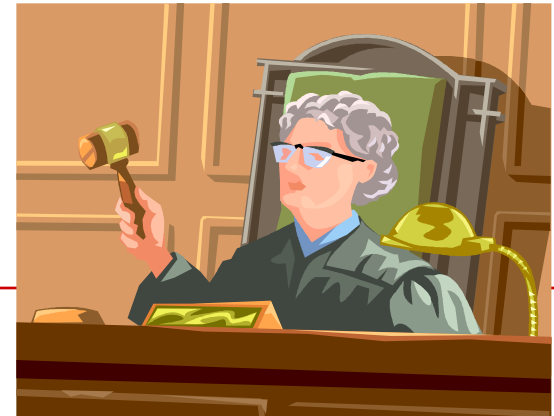


A change in the status quo?

The Enforcement Rule

◆ Final Rule

- ❖ Published: February 16, 2006
- ❖ Effective date: March 16, 2006
- ◆ Uniform civil enforcement approach for all administrative simplification – DOJ remains responsible for criminal enforcement
- ◆ Signal for change in enforcement?
 - ❖ Continuing commitment to cooperation and assistance
 - ❖ HHS discretion continues
 - ❖ Mandates civil money penalties where a violation is found



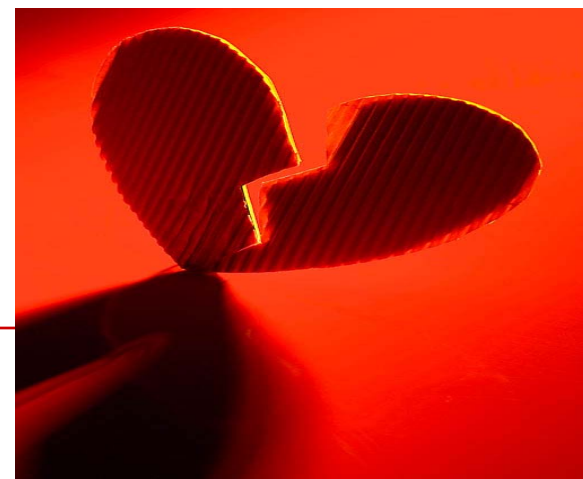
The Ex-Factor



- ◆ Breaking Up is Hard to Do
- ◆ When Good Employees Go Bad

The Ex-Factor

- ◆ Top risks for intentional misuse, improper disclosures and false accusations:
 - ❖ Ex-relationships: divorces, custody disputes, break-ups, new significant others, and so on and so on
 - ❖ Ex-employees
 - ❖ Even high school/grade school grudges
- ◆ Tip: When there is “history,” dig a little deeper
- ◆ Tip: Privacy Officer should be attuned to “gossip”
- ◆ Revisit termination process



Complaint Process and Other Responses



Response to Ex-Factor and Other Violations: Complaint Process

- ◆ Must provide process to receive complaints
- ◆ Must document all complaints and their disposition
- ◆ Tip: Make it easy for a patient to complain
 - ❖ Written only vs. any medium
- ◆ Tip: Be aware of direct complaints that may become OCR complaints
- ◆ Tip: Pay attention to the follow-up



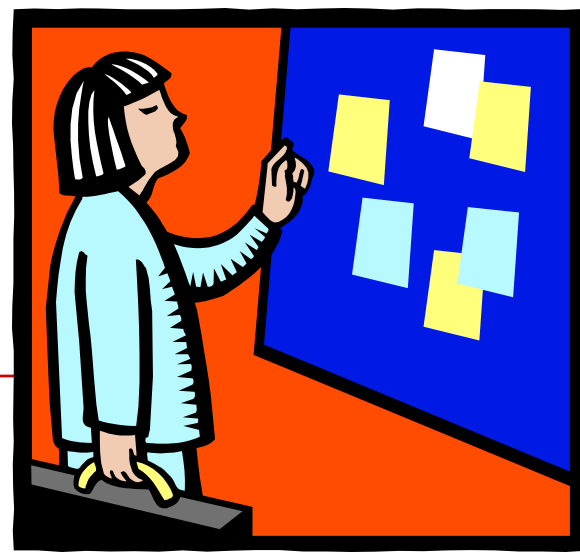
Consumer Breach Notification



When do you have to report yourself?

Consumer Breach Notification

- ◆ Many state laws mandate notification
- ◆ HIPAA has no specific notification requirement but
 - ❖ Covered entities have a duty to mitigate
 - ❖ Accounting of disclosure for breaches (that are not incidental disclosures)
- ◆ Beware: No good deed goes unpunished
 - ❖ Good citizens
 - ❖ Bad PR, class actions, etc.



Business Associates



Continues to be a top area of confusion/frustration

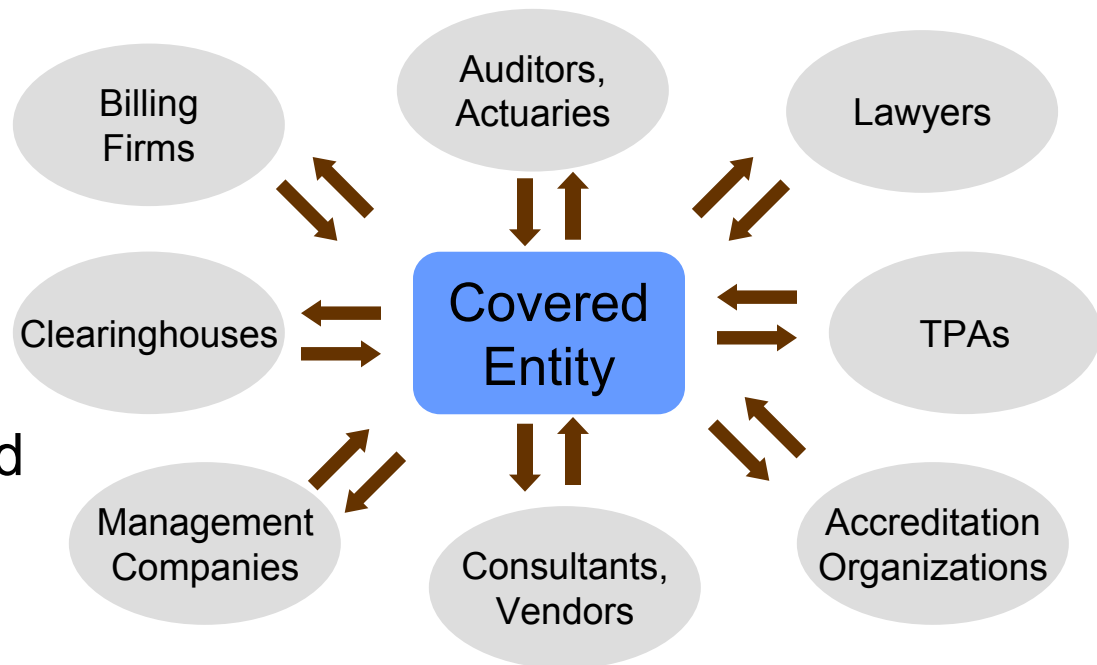
Who is a Business Associate?

◆ A person who, on behalf of a covered entity or OHCA —

❖ Performs or assists with a function or activity

- Involving PHI or
- Otherwise covered by HIPAA

❖ Performs certain identified services



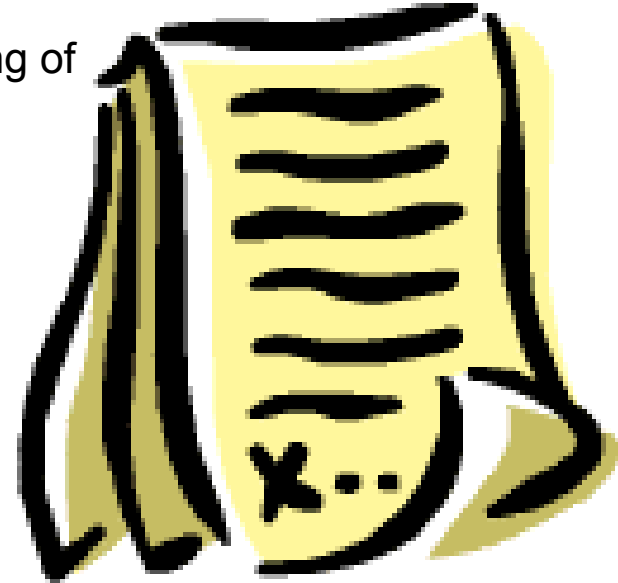
Who Are Business Associates?

- ◆ Medical device company . . . Probably not
- ◆ Research sponsor . . . Usually not
 - ❖ Does not work to circumvent research rules
- ◆ Record storage/destruction . . . Depends
- ◆ Accreditation organizations . . . Yes
- ◆ Software vendor . . . Maybe
- ◆ Collection agencies . . . Yes
- ◆ Lawyers . . . Definitely maybe



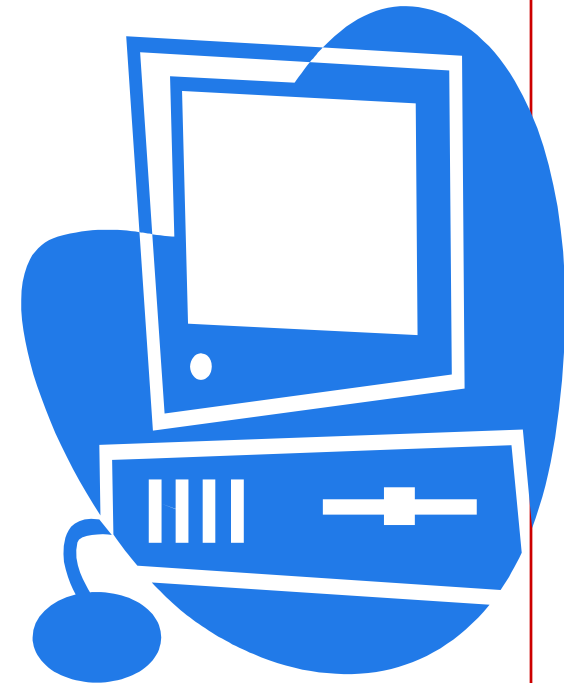
What Must Be in a Business Associate Contract — Privacy Rule

- ◆ Use and disclose information only as authorized in the contract
 - ❖ No further uses and disclosures
 - ❖ Not to exceed what the covered entity may do
- ◆ Implement appropriate safeguards
- ◆ Report unauthorized disclosures to covered entity
- ◆ Facilitate covered entity's access, amendment and accounting of disclosures obligations
- ◆ Allow HHS access to determine CE's compliance
- ◆ Return/destroy protected health information upon termination of arrangement, if feasible
 - ❖ If not feasible, extend BAC protections
- ◆ Ensure agents and subcontractors comply
- ◆ Authorize termination by covered entity



What Must Be in a Business Associate Contract — Security Rule

- ◆ Implement administrative, physical and technical safeguards that reasonably and appropriately protect the
 - ❖ Confidentiality,
 - ❖ Integrity and
 - ❖ Availability
 - ❖ Of *electronic* protected health information
- ◆ Ensure any agent implements reasonable and appropriate safeguards
- ◆ Report any security incident
- ◆ Authorize termination if the covered entity determines business associate has breached



Business Associate Contracts

- ◆ Tip: Contract management system
- ◆ Tip: Do not forget the security requirements
 - ❖ When ePHI is involved, the privacy version is not enough
- ◆ Process to identify business associates
 - ❖ Revisit existing relationships and contracts
 - ❖ Address future relationships
- ◆ Process to effectively deal with contracting
 - ❖ Templates
 - ❖ Elevate issues as needed
- ◆ Liability of a covered entity for its business associates



The Forgotten Health Plan



Health Plan

- ◆ Covered providers have employee benefit plans that likely are covered entities
- ◆ Treated as a separate entity
- ◆ Verify compliance efforts
 - ❖ Don't forget FSAs and EAPs
- ◆ Security compliance for small health plans (under \$5 million in receipts) is coming up
- ◆ Privacy FAQ
 - ❖ Send reminder of how to obtain a Notice of Privacy Practices every three years



Accounting of Disclosures



- ◆ What is covered
- ◆ What is the best way to track
- ◆ Communications with patients

Accounting of Disclosures

- ◆ Patient has the right to receive an accounting of disclosures of the patient's PHI
- ◆ Accounting includes:
 - ❖ Date of disclosure
 - ❖ Recipient name and address
 - ❖ Description of information disclosed
 - ❖ Purpose of disclosure



Accounting of Disclosures

◆ Exceptions:

- ❖ Treatment, payment and operations
- ❖ Individual access
- ❖ Directories, persons involved in care
- ❖ Pursuant to authorizations
- ❖ National security or intelligence
- ❖ Incidental disclosures
- ❖ Limited date set
- ❖ Prior to April 14, 2003



Accounting of Disclosures – Problems

- ◆ Cumbersome process with relatively few requests
- ◆ Patients often want information that is excepted
- ◆ Tricky issues
 - ❖ Date ranges acceptable (e.g., access to a universe of records during limited time)
 - ❖ For disclosures made routinely within set time:
 - Intervals acceptable (e.g., “gunshot wound within 48 hours after treatment” plus date of treatment)
- ◆ Dealing with Business Associates



Accounting of Disclosures — Approaches

- ◆ Different potential approaches
 - ❖ Log all disclosures at time of the disclosure
 - ❖ Do analysis at time of any patient request
 - ❖ Abbreviated accounting
- ◆ Tip: Clarify the request before beginning (but do not discourage request)



Copying Fees

HIPAA versus State Maximum



Copying Fees

- ◆ State law often imposes maximum copying fees
 - ❖ May include administrative fee (e.g., retrieving or handling)
 - ❖ Per page fee
- ◆ HIPAA requires reasonable cost-based fees for individual access
- ◆ Statutory maximum is not necessarily consistent with HIPAA requirement
- ◆ Fee may depend on purpose and who requests record



De-Identification



- ◆ How
- ◆ When to use

De-Identification

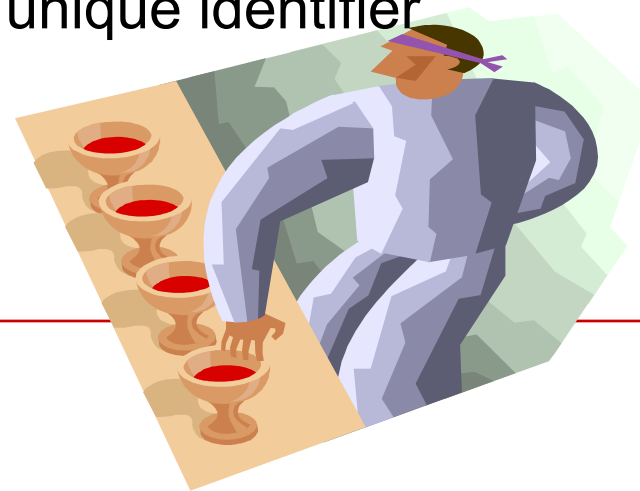
◆ Information is presumed de-identified if—

❖ Qualified person determines that risk of re-identification is “very small” or

❖ The following identifiers are removed:

Name	Address	Relatives	Employer
Dates	Telephone	Fax	e-mail
SSN	MR#	Plan ID	Account #
License #	Vehicle ID	URL	IP address
Fingerprints	Photographs	Other unique identifier	

❖ And the CE does not have actual knowledge that the recipient is able to identify the individual



De-Identification

- ◆ Beware the “other unique identifier” requirement
 - ❖ Especially difficult with large number of records
 - ❖ Beware small communities
- ◆ Identify what workforce needs to know de-identification rules. For example,
 - ❖ Marketing
 - ❖ Newsletters
 - ❖ Medical staff who lecture or publish



Limited Data Sets



- ◆ What are they
- ◆ When to use limited data sets
- ◆ How to disclose limited data sets

Limited Data Set — Not Quite De-Identified

- ◆ Limited Data Set = PHI that excludes direct identifiers except:
 - ❖ Full dates
 - ❖ Geographic detail of city, state and 5-digit zip code
- ◆ Not completely de-identified
- ◆ Special rules apply



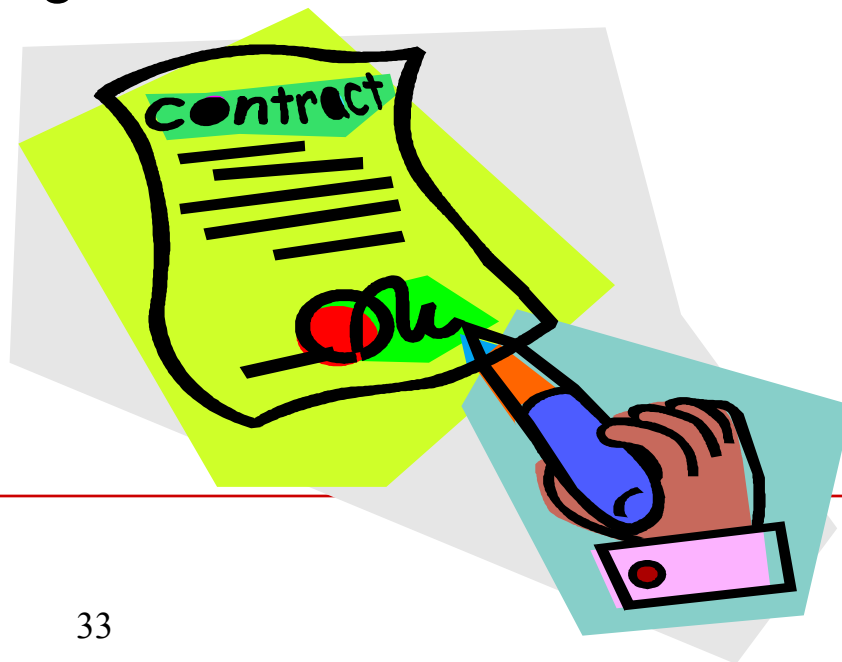
Data Use Agreements

- ◆ Limited Purposes:
 - ❖ Research,
 - ❖ Public health
 - ❖ Health care operations
- ◆ Recipient must enter into a Data Use Agreement:
 - ❖ Permitted uses and disclosures by recipient
 - ❖ Who may use or receive limited data set
 - ❖ Recipient must:
 - Not further use or disclose information
 - Use appropriate safeguards
 - Report impermissible use or disclosure
 - Ensure agents comply
 - Not identify the information or contact the individuals



Data Use Agreements

- ◆ Likely uses
 - ❖ State hospital associations
 - ❖ Public health agencies (for non-mandatory reporting)
 - ❖ Research where identifiers are not necessary
- ◆ Not included in an accounting of disclosures



Disclosures to Law Enforcement



Disclosures to Law Enforcement

Required by law

Court orders, subpoenas . . .

Administrative request

Request about a crime victim

Child abuse or neglect

Adult abuse, neglect or
domestic violence (limited)

Death in suspicious
circumstances

Criminal activity in off-site
medical emergencies

Crime on the premises

Avoid serious and imminent
threat

Identification of suspect,
fugitive, material witness
or missing person
(limited)

Admission to a violent
crime (limited)

Specialized law
enforcement



Disclosure to Law Enforcement

- ◆ Preemption considerations
 - ❖ State law plays a critical role in analysis
- ◆ Develop detailed policies and procedures
 - ❖ Tip: Identify go-to people
 - ❖ Tip: Two tier approach
 - Basic approach for majority of workforce
 - Detailed approach for those making the decisions
- ◆ Tip: Consider a community meeting with providers and law enforcement to agree on ground rules



Legal Proceedings



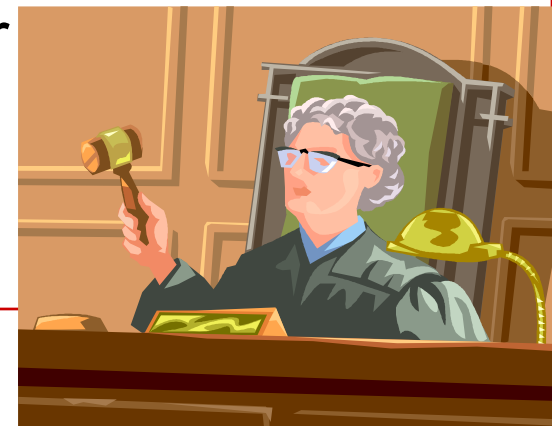
Disclosures for Legal Proceedings

- ◆ If a party to litigation/proceeding
 - ❖ May use and disclose PHI for own health care operations (as well as other exceptions)
 - ❖ “Operations” include conducting or arranging for legal services to the extent related to health care functions
 - Defendant in malpractice suit
 - Plaintiff in collection matter (also payment)
 - ❖ Minimum necessary
 - De-identification
 - Qualified protective order
 - ❖ Business associate contract for outside counsel needed



Disclosures for Legal Proceedings

- ◆ If covered entity is not a party, find an exception
 - ❖ Required by law (e.g., court order)
 - ❖ Health care oversight (e.g., licensure hearing)
 - ❖ Authorization
 - ❖ Response to subpoena or other lawful process
 - Satisfactory assurances that requestor made reasonable efforts either to notify relevant patients or secure a qualified protective order
 - Covered entity may do the same
 - Specific requirements for each



Disclosure for Legal Proceedings

- ◆ Preemption Considerations: Beware state law
- ◆ Accounting of Disclosures
 - ❖ Depends on exception
 - ❖ No: health care operations, payment, authorization
 - ❖ Yes: subpoena, health care oversight
- ◆ Tip: Don't assume a lawyer knows the law (with HIPAA at least)



Misunderstandings and Unrealistic Expectations



HIPAA does not always live up to expectations

Misunderstandings and Unrealistic Expectations

- ◆ Must train workforce
 - ❖ Biggest threat
 - ❖ Greatest resource
- ◆ Training needs to be relevant and tailored
- ◆ Assess levels of awareness
 - ❖ Manage
 - ❖ Measure
 - ❖ You must encourage workforce awareness
- ◆ Abuse of legitimate access
 - ❖ Difficult to detect on audit
- ◆ Facilitate workforce reporting of suspicions and making suggestions



Misunderstandings and Unrealistic Expectations

- ◆ Should we train/educate patients?
- ◆ Areas of confusion
 - ❖ Opting out of facility directory
 - Foster understanding of consequences
 - ❖ Requests for additional privacy protections
 - Patient has right to ask
 - Covered entity has right to say “No”
 - Covered entity is bound by a “Yes”
 - Promote consistency
 - ❖ Accounting of disclosure
 - ❖ Not all disclosures without authorization are improper



