

“HIPAA 101” The Basics & Business Associates



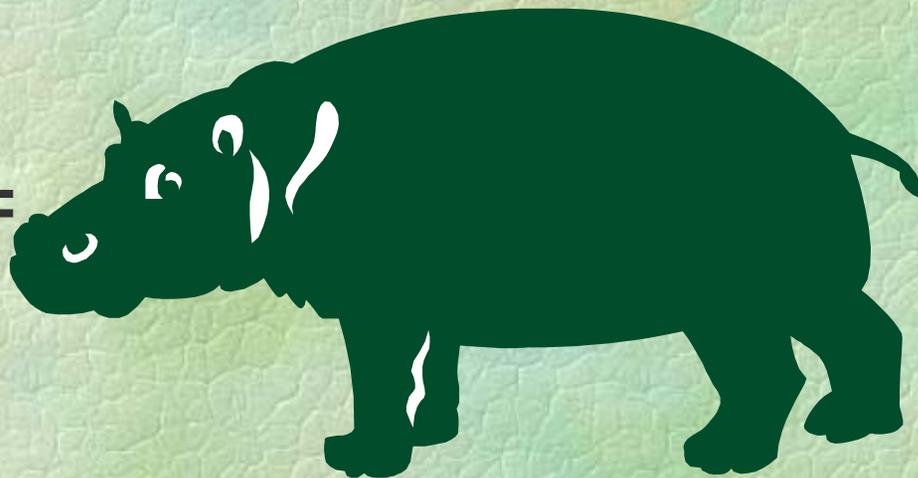
Colorado Contract Improvement Team
August 21, 2002

Kathleen Sutherland Archuleta
Office of the Attorney General

PRESENTATION GOALS

- ☛ General Overview of HIPAA:
“Enough to be Dangerous”
- ☛ Focus: Privacy Rule Business Associate Contracting Requirements
- ☛ Briefly: Other HIPAA Relationships and Agreements
- ☛ HELP!: “Who you gonna call?”

HIPAA =



?!?!?!

WHAT IS HIPAA?

- ☞ H e a l t h I n s u r a n c e P o r t a b i l i t y a n d A c c o u n t a b i l i t y A c t (Public Law 104-191)
- ☞ Signed into law August 21, 1996
- ☞ Significant impact on health care industry (and others!)
 - “Most sweeping change since Medicare”
 - Costs may be three to four times that of Y2K
 - Unlike Y2K, HIPAA is NOT a technology-only issue

PURPOSE OF HIPAA

☞ Health Insurance Portability

- Improve the portability and continuity of health insurance coverage for groups and individuals

☞ Accountability

- Combat waste, fraud, and abuse in health insurance and health care delivery

☞ Administrative Simplification

- Simplify administration of health care system by adopting standards that facilitate electronic transmission of data among health plans and providers

ADMINISTRATIVE SIMPLIFICATION SUBCHAPTER

- ☛ Standardize electronic exchanges of information to improve efficiency (Transactions/Code Sets)
- ☛ Protect the privacy of “individually identifiable health information” (PHI) (Privacy)
- ☛ Implement standards for security of data processing systems (Security)
- ☛ Develop standard identifiers - providers, employers, and health plans (Identifiers)

WHY ADMINISTRATIVE SIMPLIFICATION?

☞ Cost of communicating in many
“languages” . . .

IMPLEMENTATION FRAMEWORK

- ☞ DHHS implementing “Admin Simp” provisions through rulemaking process
- ☞ Rules are being issued in “waves”
 - Notice of Proposed Rulemaking (NPRM)
 - Comment Period (usually 30-60 days)
 - Final Rule (180 days to 24 months to compliance)
 - Informal “Guidance” and Interpretation
- ☞ Modifications to “Final” Rules

PRACTICAL TIP: TERMINOLOGY

- ☞ Statute (United States Code or “USC”)
 - Public Law (“P.L.”) 104-191
 - 42 U.S.C. § 1320d
 - Part of Social Security Act (Subchapter XI, Part C)
- ☞ Federal Register (www.access.gpo.gov/su_docs/aces/aces140.htm)
 - Notice of Proposed Rulemaking (“NPRM”)
 - Final Rule
 - “Effective” vs. “Compliance” Dates
 - “Preamble” vs. Regulation Text (“Rule”)
- ☞ Code of Federal Regulations (“CFR”)
 - 45 C.F.R. Parts 160, 162 and 164

RULE STATUS

- Transactions / Code Sets

- Final Rule: 8/17/00
- Compliance: 10/16/02 (10/16/03 with ASCA plan)
- 1st Modifications NPRM: 5/31/02

- Privacy

- Final Rule: 12/28/00
- “Guidance”: 7/6/01 (small retraction 1/14/02)
- Compliance: 4/14/03
- 1st Modifications NPRM: 3/27/02
- “Final” Modifications: 8/14/02

RULE STATUS

- Security

- NPRM: 8/12/98
- Final Rule: Late Summer/Early Fall 2002?

- Identifiers

- Employer ID Final Rule: 5/31/02
- National Provider ID NPRM: 5/7/98 (Final Fall 2002?)
- Health Plan ID NPRM: Fall 2002?
- Patient ID NPRM: ????

- Others??

- Enforcement
- Claims Attachments

PREEMPTION OF STATE LAW

Preemption under HIPAA:

☛ HIPAA: “Heads Up”

- Public Law 104-191; Section 262 (SSA Section 1178)

HIPAA (any provision, requirement, standard or implementation specification of HIPAA) shall supersede any contrary provision of State law.

☛ Preemption applies to all of HIPAA, not just the privacy portion

- 45 CFR Part 160, Subpart B (201-205)

Exceptions to Preemption

- State laws addressing controlled substances
- Where DHHS determines a State law is necessary
 - To prevent fraud and abuse
 - To ensure appropriate regulation of insurance /health plans
 - For reporting on healthcare delivery or costs
 - To serve a ***compelling need*** related to public health, safety or welfare
 - DHHS must determine invasion of privacy is warranted when balanced against the need.

Exceptions to Preemption

- **Public health laws** for reporting disease, injury, child abuse, birth or death, or public health surveillance, investigation or intervention
- Laws requiring **health plans** to report or provide access to information for audits, program monitoring, or facility or individual licensure or certification
- Laws relating to the privacy of health information that are ***contrary to*** and ***more stringent than*** the HIPAA requirements

Preemption: Contrary

☛ **Contrary means —**

- Covered entity could not comply with both State law and the HIPAA requirement

or

- State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA

Preemption: More Stringent

☞ **More stringent** means that State law —

- Has stricter limits on use or disclosure of health information
 - Except for disclosures to DHHS or patient
- Gives greater rights of access to or correction of health information by the patient
 - Does not affect State laws authorizing or prohibiting disclosure of information about a minor to parent or guardian
- Has harsher penalties for unauthorized use or disclosure

Preemption: *More Stringent*

- Provides greater information to individuals regarding use, disclosure, rights or remedies
- Has stricter requirements for authorizing or consenting to the disclosure of information
- Has stricter standards for record-keeping or accounting for disclosures of information
- With respect to any other matter provides greater privacy protection to the patient

How Preemption Will Work

- Preemption will focus on specific elements and aspects of State laws
 - HIPAA will be the baseline (“floor”)
 - State law will be given effect only to the extent that:
 - (a) there is no HIPAA law on the issue;
 - (b) State law is more stringent; or
 - (c) there is an exception
 - Exceptions will apply to specific State laws, not entire State schemes (provision by provision)

“COVERED ENTITIES”

WHO MUST COMPLY?

“Covered Entities”

☞ Health Plans

- Individual or group plans that provide or pay the cost of medical care

☞ Health Care Clearinghouses

- Entities that process or facilitate processing non-standard data elements into standard data elements, or vice versa

☞ Health Care Providers *who conduct (electronic) standard transactions*

- Furnishes, bills or is paid for health care services or supplies in the normal course of business

PRACTICAL TIP: HIPAA “JURISDICTION”

☞ “All In / All Out” Rule:

- If you’re “in,” all HIPAA Rules apply (to all forms of PHI)
- If you’re “out,” none of the Rules apply (at least directly)

☞ “Covered Functions” Test:

- It’s not who you are or what you’re called, it’s what you do that determines whether you’re “in” or “out”

Examples of Health Plans

- ERISA defined group health plan
- Health insurance issuer
- HMO
- Medicare
- Medicaid
- Medicare supplement
- Long-term care policy
- VA health care system
- State high risk pool
- Employee welfare benefit plan
- Health plan for active military
- CHAMPUS
- Indian Health Services
- Federal Employees Health Benefit Plan
- SCHIP plan (CHP+)
- Or any combination of the above

HIPAA Health Plan Exclusions

- Policy/plan/program that provides or pays cost of certain “excepted benefits”:
 - Workers’ compensation programs
 - Correctional institutions
 - Disability insurance programs
 - Automobile insurance carriers
 - Property and casualty insurers
 - Nursing home fixed-indemnity policies
- Certain government-funded programs (other than listed plans)

Health Care Provider

(who conducts standard transactions)

- Any person or organization who furnishes, bills, or is paid for health care in the normal course of business
- Health care is defined as care, services or supplies related to the health of an individual. It includes but is not limited to:
 - Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to physical or mental condition, or functional status, of an individual or that affects the structure or function of the body
 - Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription

Health Care Clearinghouse

☞ A public or private entity that performs either of the following functions:

- Processes or facilitates the processing of health information received from another entity in a non-standard format or containing non-standard data content into standard data elements or a standard transaction
- Receives a standard transaction from another entity and processes or facilitates the processing of health information into non-standard format or non-standard data content for the receiving entity

“CRITICAL PATH” ISSUE

 IS YOUR AGENCY OR
INSTITUTION A COVERED
ENTITY?

***EVERYONE* IS IMPACTED BY HIPAA IN SOME WAY**

DIRECTLY

- As a “Covered Entity”
- As an individual health care consumer

INDIRECTLY

- To extent that organization deals with PHI and or has relationships with CEs involving PHI

**TRANSACTIONS RULE
&
SECURITY RULE**

Standard Transactions

☞ Transaction and Code Set Rule: “Speak the Same Language”

- Health Care Claim or Encounter (837)
- Health Care Claim Payment and Remittance (835)
- Health Care Claim Status Inquiry/Response (276, 277)
- Health Care Eligibility Inquiry/Response(270, 271)
- Enrollment and Disenrollment in a Health Plan (834)
- Referral Certification and Authorization (278)
- Health Plan Premium Payments (820)
- Health Care Claim Attachments (delayed)
- First Report of Injury (delayed)

PRACTICAL TIP: “COVERED ENTITY” ANALYSIS

- ☞ Whether or not you are a covered provider depends on whether or not you are conducting what would otherwise be “standard transactions” electronically
- ☞ Scrutinize the transaction definitions
 - Who is on the sending and receiving end?
 - What is the purpose of the transaction?

Code Sets

- HIPAA has mandated the use of national standard code sets
 - E.g., procedure code, diagnosis code, drugs and biologicals
- Elimination of “Local Codes”
 - States heavily rely on these for Medicaid waiver programs, among others
- Nationally, Medicaid programs are being forced to “crosswalk” local codes into limited Level 2 HCPCS codes
 - Serious operational and fiscal implications of “work arounds” not found

Administrative Simplification Compliance Act (ASCA)

“Extension”

- ☛ Late 2001 Congress provided for “extension” of compliance deadline for CEs that:
 - File detailed compliance plan before 10/16/02 (original compliance date)
 - Testing must begin in April 2003
 - Compliance required by 10/16/03
- ☛ NOT an automatic extension of deadline
- ☛ Plan **MUST** be filed not later than 10/15/02
 - File electronically (CMS web site / confirmation)
 - File by mail (send certified / return receipt)

Security - Proposed Regulations

☞ Proposed regulations require:

- Ability to control access to data
- Ability to protect data from accidental or intentional disclosure to unauthorized persons
- Ability to protect information from alteration, destruction or loss

☞ Security Rule requires **outcomes**, not technologies (flexible & “scalable”)

Security: Administrative Requirements

- ☞ Covered entities are required to have:
- Documented security management process
 - Computer system/network accreditation
 - Contingency and disaster recovery plans
 - Data processing policies and information access controls
 - Internal audit function
 - Security incident reporting procedures
 - Adequate supervision and training for staff

PRACTICAL TIP: SECURITY

☞ DON'T PUT OFF THINKING ABOUT
SECURITY IMPLEMENTATION!

☞ Even though final Security Rule has yet to be issued, Covered Entities already have basic obligation to *“maintain reasonable and appropriate administrative, technical and physical safeguards”*

- HIPAA Statute (SSA 1173(d)(2))
- Privacy Rule 45 CFR 164.530(c)

PRIVACY RULE

Privacy Rule - Background

- ☞ As the ease of exchanging PHI increases, there is a corresponding need to increase privacy protection
- ☞ The Privacy Rule provides a national standard “floor” to address the fundamental privacy rights of individuals with respect to PHI
- ☞ The privacy rule defines *what* information must be protected, as contrasted with the security rule which defines *how* that information must be protected

Protected Health Information (PHI)

☞ Individually identifiable health information —

- Information (past, present, future) relating to:
 - An individual's physical or mental health or condition
 - Provision of health care to an individual
 - Payment for health care to an individual
- Identifies an individual, or there is a reasonable basis to believe it can be used to identify an individual

Privacy – General Rule

☛ A covered entity may not use or disclose PHI *except*:

- For treatment, payment or health care care operations (TPO) (164.506)
- Pursuant to individual “authorization” for any other purposes (164.508)
- Without authorization for governmental and other specified public interest purposes (164.512)

PRACTICAL TIP: TERMINOLOGY

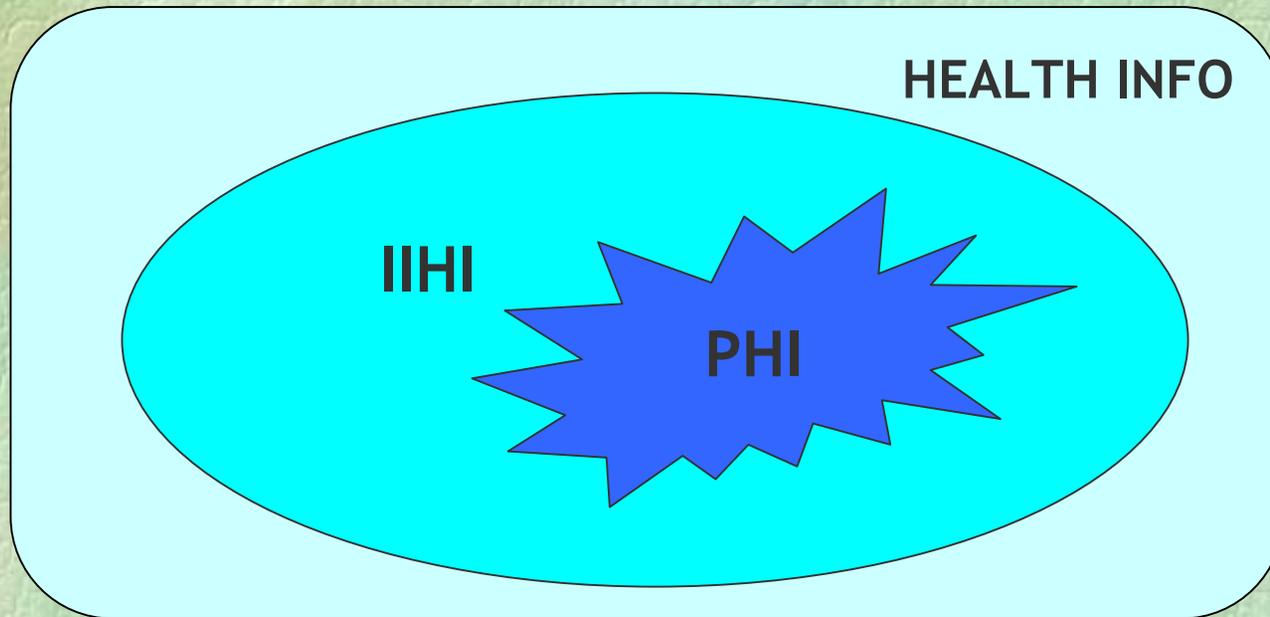
🐉 “USE” vs. “DISCLOSURE”

- “Use” is internal to CE (single function component)
- “Disclosure” is external to CE

PRACTICAL TIP: TERMINOLOGY

🧐 HI vs. IHI vs. PHI

🧐 WHAT'S THE DIFFERENCE!?



Protected Health Information (PHI)

- ☞ All PHI transmitted or maintained *by a covered entity*
- ☞ In whatever form it exists:
 - Electronic, written, oral
- ☞ Excludes “de-identified” information
 - Detailed requirements for de-identification in Privacy Rule
- ☞ Excludes “education records” covered by FERPA (20 USC 1232g) and certain treatment records described at 20 USC 1232g(a)(4)(B)(iv)
- ☞ Excludes certain CE “employer records”
 - (see NPRM issued 3/27/02 & modifications to Privacy Rule published 8/14/02)

Required Disclosures

- ☛ To the individual, pursuant to request
- ☛ To the Secretary of HHS, to determine compliance

Permitted Disclosures (164.512) Government and Other Purposes

- As required by other laws
- Public health activities
- Victims of abuse, etc.
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Decedents – coroners and medical examiners
- Organ procurement
- Research purposes, under limited circumstances
- Imminent threat to health or safety (to the individual or the public)
- Specialized government functions
- Workers' compensation

PRACTICAL TIP

 **DON'T ASSUME
"512 DISCLOSURES" ARE
FREE FROM CONDITIONS!**

 SECTION 164.512 MAY STILL REQUIRE A CE
(AND THE PHI REQUESTER) TO FOLLOW SPECIAL
PROCEDURES TO ALLOW PHI DISCLOSURE

“MINIMUM NECESSARY”

45 CFR 164.502(b)

- ☛ Generally, any use or disclosure of PHI (or request for disclosure from another CE) must be limited to the “minimum necessary” PHI to accomplish intended purpose of use, disclosure or request
- ☛ “Minimum necessary” standard does not apply:
 - to disclosures to / requests by a provider for treatment purposes
 - to individual who is subject of PHI
 - use/disclosure pursuant to individual’s authorization
 - to Secretary of DHHS (for compliance purposes)
 - to use/disclosure required by law (164.512(a))

Privacy Rights of Individuals

- ☞ Receive Notice of Privacy Practices (NPP)
- ☞ See and copy own records
- ☞ Request amendments
- ☞ Obtain accounting of disclosures
- ☞ Request restrictions and confidential communications
- ☞ File complaints (with CE or DHHS)

Documentation / Record Requirements

- ☞ Covered entities are required to have:
 - Copies of NPP written acknowledgements & signed authorizations
 - Log of non-routine (i.e., non-TPO) disclosures
 - Written statements of denial of requests for information
 - Responses to requests for amendment
 - Notices of disagreement from individuals
 - ***Contracts with business associates***
 - Multitude of policies and procedures

Special Rules: Administrative Procedures

- ☛ CEs must have policies, procedures, and systems to protect health information and individual rights:
 - Designation of a privacy officer and contact person for complaints/info
 - Privacy training for workforce
 - Administrative, technical & physical safeguards to prevent intentional or accidental misuse of PHI
 - Means for individuals to lodge complaints
 - Sanctions for employee violations
 - Mitigation procedures for inappropriate disclosures (CE and BA)

Special Rules: Organizational Requirements 164.504

- ☞ “Hybrid entities”
 - designated “health care component(s)”
- ☞ CEs with multiple covered functions
- ☞ “Affiliated covered entities” (ACE)
- ☞ “Organized health care arrangements” (OHCA)
- ☞ Group health plans

Special Rules: Organizational Requirements

☛ Hybrid Entity

- Single legal entity that is a CE whose activities include “covered functions” and non-covered functions
- Covered with respect to its health care component(s)
- Must designate health care component in writing
 - **Components may perform covered function directly or as BA**
- May not disclose PHI outside components, except as permitted to third parties under the Rule

Hybrid Entity - Implications

- Privacy Rule requires you to “build walls” (administrative and technical safeguards) between the Health Care Component(s) (covered functions) and the rest of the entity, so that the non-covered portions do not have inappropriate access to PHI

Special Rules: Organizational Requirements

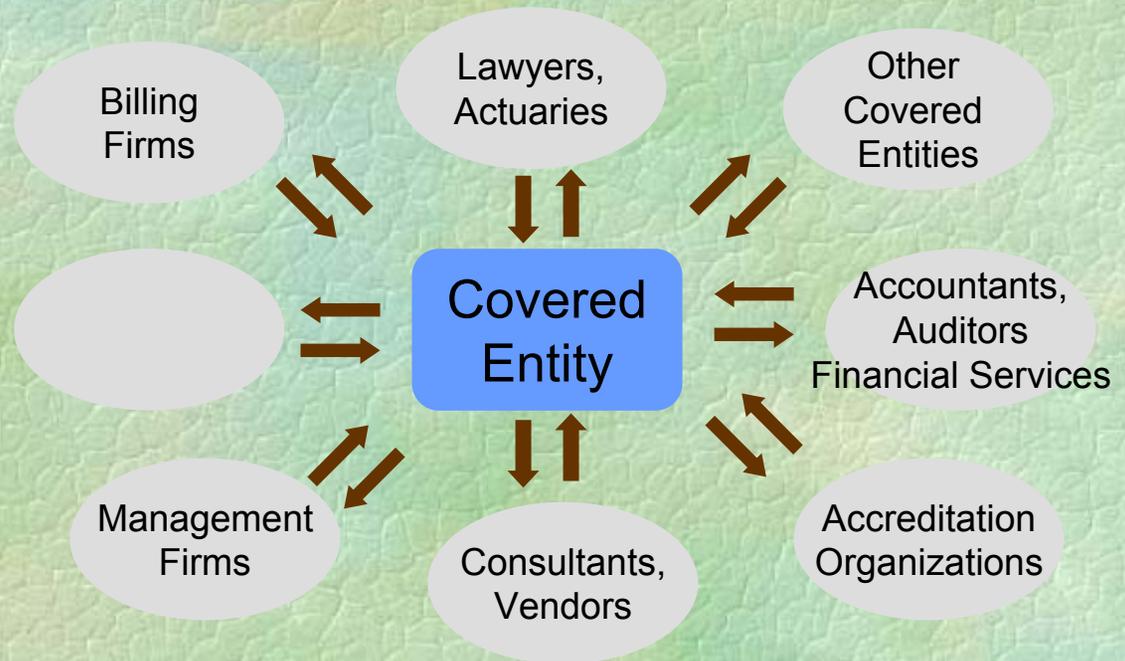
☛ Covered Entities with multiple covered functions

- Must comply with the requirements for each function
- May disclose PHI only as necessary for the function for which the disclosure is made
- Cannot “share” PHI across functions (e.g., provider with plan), unless otherwise permitted under Rule

BUSINESS ASSOCIATES

Use and Disclosure – Who Is a Business Associate?

- A person/entity (other than member of *workforce*) who receives IIHI and –
 - On behalf of a covered entity performs or assists with a function or activity involving use or disclosure of PHI or otherwise covered by HIPAA
 - Provides certain identified services to a covered entity
- May itself be a covered entity



Business Associates

“Satisfactory Assurances”

164.502(e)

- ☛ A covered entity may disclose PHI to BA (& may allow BA to create/receive PHI on its behalf) if it obtains “satisfactory assurances” that business associates will appropriately safeguard the information
- ☛ Business associate contract required (required contract terms specified in rule)

Core Business Associate Obligations ("Non-negotiable") (164.504(e))

- ☞ Must establish permitted/required uses/disclosures of PHI by BA
- ☞ Must not allow BA to handle PHI in a manner that would violate Rule if done by CE
- ☞ Must not use or disclose protected health information in violation of the law or contract
- ☞ Report violations to CE as soon as known
- ☞ Implement safeguards against improper use or disclosure

Core Business Associate Obligations ("Non-negotiable") (164.504(e))

- ☞ Ensure that any agents or subcontractors agree to fulfill contractual and legal obligations
- ☞ Afford individual access to records; make available records for amendment by the individual; account to the individual for use or disclosure other than for treatment, payment or operations
- ☞ Make info available to DHHS Secretary
- ☞ At termination of the contract, return or destroy protected health information
- ☞ Authorize termination by CE if CE determines material breach

If CE and BA are both “Governmental Entities” (164.504(e)(3)):

- ☛ Special provisions allow “other arrangements,” including a Memorandum of Understanding
- ☛ “Jointly Administered Government Program” Exception to the BA Standard may apply
 - Sharing info between JAGPs providing public benefits is permitted without a BA contract (*if* certain conditions are met)

BA Standard DOES NOT Apply:

- ☛ Disclosures by CE to provider re treatment of individual
- ☛ Certain disclosures from group health plan / HMO to plan sponsor
- ☛ Uses/disclosures by plan that is government program providing public benefits (if certain conditions met)

PRACTICAL TIP

BOTTOM LINE:

 BA must comply with Rule provisions applicable to the functions it performs on behalf of/for CE

Liability for Business Associates

☞ If covered entity knows of a pattern of activity constituting a breach by the business associate, then

- Must take reasonable steps to
 - Cure the breach (mitigation) or
 - End the violation
- If unsuccessful,
 - Must terminate if feasible or
 - Report to DHHS



☞ Substantial and credible evidence standard

☞ Liability to CE under contract and/or independent liability if a CE itself

**OTHER HIPAA
RELATIONSHIPS
&
AGREEMENTS**

TRADING PARTNER AGREEMENT (TPA)

- ☞ TPA defined: “Agreement related to exchange of information in electronic transactions”
- ☞ Addresses how entities accept and process (standard) transactions
- ☞ NOT mandatory, but advisable
- ☞ Need not be a formal agreement (“companion document” approach)
- ☞ 162.915 TPA “Prohibitions”
 - 4 elements TPA may NOT require

CHAIN OF TRUST (CoT)

- ☞ CoT provisions in proposed Security Rule
- ☞ Required where data (PHI) exchanged electronically between CE and another entity
- ☞ Not limited to standard transaction data
- ☞ Purpose to require business partner to protect integrity & confidentiality of data

PRACTICAL IMPLICATIONS

- ☞ TPs exchanging standard transactions will be required (under Security Rule) to have CoT provisions in place (through TPA)
- ☞ Being a TP of another entity does not necessarily make you a BA (or vice versa)
- ☞ Where data is exchanged electronically (whether or not standard transaction), BA & CoT provisions will be required
- ☞ May be entities (not TP or BA) to which a CE sends data electronically where CoT required
 - e.g., mandatory reporting registry

RISKS OF NONCOMPLIANCE

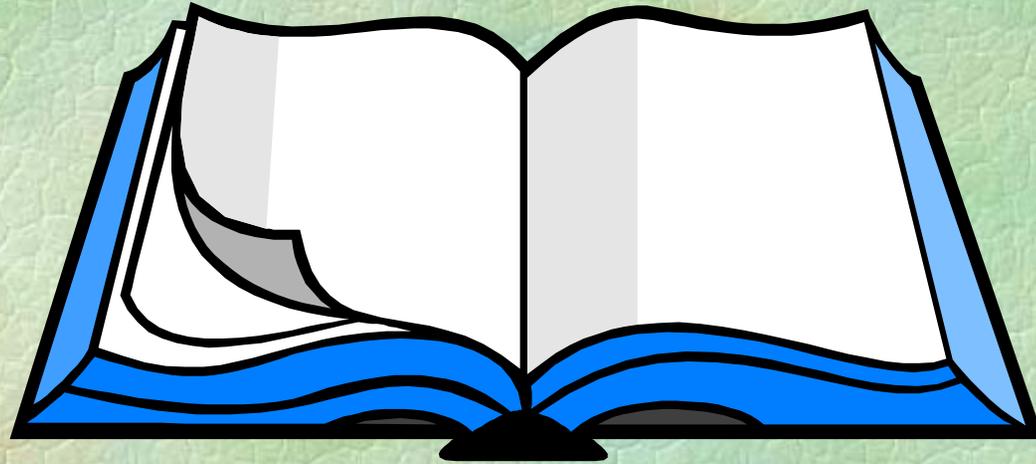
- ☛ Service interruption of major health programs
 - Inability to pay / process claims & interact with business partners
- ☛ Costly litigation: individual / class action suits
 - No HIPAA Right of Action BUT state tort law, implied K law theories
 - HIPAA = new “standard of care”
- ☛ Federal Civil & Criminal Penalties (OCR / DOJ)
 - \$100 - \$250,000 per violation; 1-10 years prison

**“WHO YOU GONNA
CALL?”**

Colorado - Meeting the Challenge Statewide Approach

- ☛ Governor's Task Force on HIPAA
Implementation: Executive Order (February 6, 2002)
- ☛ Agency/Institution HIPAA Coordinator and Steering Committee
- ☛ AG HIPAA Team
- ☛ Other Resources
 - Web Resources
 - CoSNIP (Next Meeting September 19, 2002)
 - Form CCIT BA Work Group

PRACTICAL TIP



🍃 READ THE THE RULE!

🍃 READ PREAMBLE!

The Five Stages of HIPAA

- ☛ Denial
- ☛ Anger
- ☛ Bargaining
- ☛ Depression
- ☛ Acceptance



QUESTIONS?



kathleen.archuleta@state.co.us