Alan S. Goldberg, Esq.
HIPAA SUMMIT VII
Boot Camp Text
September 14, 2003
©www.hipaahero.com®

Who Am I

- Goulston & Storrs, 1967 --
- JD Boston College Law School
- LLM (Taxation) Boston Univ. Law School
- Past Pres. American Health Lawyers As'n
- US Navy Judge Advocate General's Corps
- Adjunct Professor of Law
  - Boston College Law School
  - Univ. of Maryland School of Law
  - Suffolk University Law School

It's all in the cards

Boston Lawyer
San Diego 1968

CDR Rabb JAGC
LT Goldberg JAGC
I'm From Wash., DC
& I'm Here to Help You
TV President Josiah Bartlet Has
Health Care Secret In West Wing
Go to Sleep
Counting HIPAAs

Professor Goldberg's
Honest Lawyer Privacy Policy

- Nothing I say in this room is private
- Everything you say in this room is public
- We have zero privacy in this room: get over it!

Healthcare Still Runs On

Dead Tree Media
We Have Lots of Law
Gramm-Leach-Bliley

- Financial institutions PLUS
- *Protects Nonpublic* personal information

- H I P P A WRONG!
- H I P A WRONG!
- H I P P O WRONG!
- *H* I P A A *I*t's *P*owerful *A*nd *A*wesome

Privacy Added To End of Employee Benefits Law

*A*dministrative *S*implification *S*ubtitle

No HIPAA Lies

Only HIPAA Truths

HIPAA Is Tippa
Privacy & Security Iceberg
HCFA (CMS) Internet
Security Policy

- 1997 – Drop Dead Internet
- 1998 - Internet Communications Security & Appropriate Use Encryption, authentication
- Temporary pre-HIPAA

HIPAA Is About <u>Security</u>

On internet nobody knows you're a dog

Conditions of Participation

- Medicare program has 1,000,000 certified providers & one billion claims/year
- Patient has right to personal privacy & confidentiality of personal & clinical records

Conditions of Participation

- Resident may approve or refuse release of personal & clinical records to any individual outside facility

Conditions of Participation

- Resident right to access all records pertaining to resident including current clinical records within 24 hours (excluding weekends & holidays)
- May buy, at cost not to exceed community standard, photocopies of records or any portions of them upon request

Conditions of Participation

- Resident has right to be fully informed in language that resident can understand resident's total health status, including resident's medical condition

Medicaid State Ops. Manual

- MDS data are part of resident's clinical record
- Protected from improper disclosure by facilities

MDS Privacy Resident's Rights

- Nursing homes must inform each resident about electronic transmission of MDS to State & CMS

Massachusetts Rights of Assisted Living Residents

- Be treated with consideration & respect & with due recognition of personal dignity, individuality, & need for privacy
- Privacy within resident's unit, subject to rules of residence reasonably designed to promote health, safety & welfare of residents

Rights of Assisted Living Residents

- Private communications, including receiving & sending unopened correspondence, access to telephone, & visiting

Rights of Assisted Living Residents

- Confidentiality of all records & communications to the extent provided by law

Rights of Assisted Living Residents

- To privacy during medical treatment or other rendering of services within the capacity of the residence

- To informed consent to the extent provided by law

  Rights of Assisted Living Residents
- Manager shall ensure that written notice of rights, obligations & prohibitions is posted in prominent place in the residence

Not New to Doctors HIPAA cratic Oath, 400 BC

- Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, *I will not divulge*, as reckoning that all such should be kept secret.

HIPAA from 40,000 feet up
Manage Your Expectations

Zebras, Horses, HIPAAs
What are the three BIG HIPAA lies?

My Software Is HIPAA Compliant

My Hardware Is HIPAA Compliant

I Am
HIPAA Compliant

HIPAA BULL

HIPAA Applicability

- Health plan
- Health care clearinghouse
- Health care provider that transmits health information electronically in connection with covered transaction

HIPAA Applicability

- What were you doing at 11:59 PM on the evening of April 13, 2001?

Lost HIPAAginity

Health Plans Born Without It!

Health Care Provider

- Provider of medical or health services
- Any other person or organization who furnishes, bills, or is paid for health care in normal course of business

Not Covered Entities

- Employers
- TPAs
- Property/casualty/disability/auto plans event if pay for health care
- Workers compensation
- Stop-loss carriers & reinsurers

HIPAA Health Care

- Care, services, or supplies related to health
- Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, & counseling, service, assessment, or procedure with respect to physical or mental condition, or functional status, or that affects structure or function of body
- Sale or dispensing of drug, device, equipment, or other prescription item

HIPAA Is About:

- Standards for data transmission
- Privacy
- Security

HIPAA Is About

S t a n d a r d s

Why We Need Standards

Standard Transaction

- Transmission of information between two parties to carry out financial/administrative activities related to health care

Standard Transaction

- (1) Health care claims or equivalent encounter information.
- (2) Health care payment & remittance advice.
- (3) Coordination of benefits.
- (4) Health care claim status.
- (5) Enrollment & disenrollment in health plan.

Standard Transaction

- (6) Eligibility for health plan.
- (7) Health plan premium payments.
- (8) Referral cert. authorization.
- (9) First report of injury.
- (10) Health claims attachments.
- (11) HHS prescribed transactions.

HIPAA Is About Privacy

Loose Lips Sink Privacy

Protected Health Information

- Any individually identifiable health information transmitted by or maintained in electronic media or in any other form or medium

Individually Identifiable

- ID of patient, relatives, employers, household
- (A) Names; (B) Geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, & geocodes; (C) birth date, admission date, discharge date, date of death; (D) E-mail addresses; (E)

Telephone, Fax, Social Security, Medical record, Health Plan Beneficiary, Account, Certificate/license, Vehicle, License Plate; (F) Full face photo

Two Elements = Compound

The Golden Rule from The Book of HIPAA

- A covered entity may ***not*** use or disclose protected health information, except as permitted or required

Only Two Required Disclosures

- To individual whose information is to be disclosed
- To Secretary of HHS to determine compliance with HIPAA
- Other uses/disclosures only if permitted & CE elects to use or disclose or required by other law

HIPAA Privacy

- *Protected health information*: individually identifiable health information transmitted by or maintained in electronic media or in any other form or medium
- *No Consent* : use/disclose for payment, treatment, health care operations
- *Authorization*: outside use or disclosure

Provider Does Not Need Patient Consent

Now you see it, now you don't

- Clinton: consent prohibited
- Clinton: consent required
- Bush: consent not required but permitted

Should Adults Consent?

- It depends on what the meaning of "CONSENT" is….

Senators Say: "Consent Is Needed"

HIPAA BULL!!!!!

NOTICE OF PRIVACY PRACTICES

- "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

Notice of Privacy Practices

- Acknowledgment required even if consent obtained
- Writing or electronic
- Good faith efforts
- Layered notice on top

Patient Rights

- To see their health information
- To know about disclosures of their health information

CMS Contractor Call Center

- Verify it is beneficiary by asking for his/her: Full name; Date of birth; HIC number; & One additional piece of information such as SSN, address, phone number, effective date(s), whether he/she has Part A and/or Part B coverage
- Release any entitlement & claim information & answer any questions pertaining to beneficiary's Medicare coverage

CMS Contractor Call Center

- A beneficiary's spouse, relative, friend or advocacy group (excluding State Health Insurance Assistance Program (SHIP) employees & volunteers)
- The beneficiary gives verbal authorization for you to speak with the caller. (The beneficiary does not have to remain on the line during the conversation, or even be at the same place as the caller – you may obtain

the beneficiary's authorization to speak with the caller via another line or three way calling.)

CMS Contractor Call Center

- Verify the identity of the beneficiary by asking the beneficiary for his/her: • Full name; • Date of birth; • HIC number; and • One additional piece of information such as SSN, address, phone number, effective date(s), whether he/she has Part A and/or Part B coverage. A verbal authorization on file is good for 14 days. The CSR may advise the beneficiary & the caller that if the beneficiary wants the caller to receive information for more than 14 days, the beneficiary should send in a written authorization
- Release any entitlement & claim information & answer any questions pertaining to the issue in question coverage

Patient Rights

- Written notice of info. practices
- Inspect & copy health information

- Amend health information
- Accounting of disclosures
- Request restrictions – optional
- Reasonable requests for confidential communications

Personal Representative

- Must follow direction of PR
- UNLESS reasonable concern about abuse, neglect, or endangerment

Protected Health Information

- Employment records of covered entity as employer are *not* protected health information
- But PHI received in health care capacity is PHI

Protected Health Information

- 6 years (other than disclosures for payment, treatment, health care operations)
- Corrections, restrictions

Incidental Use/Disclosure

- Incidental to otherwise required or permitted use or disclosure
- If minimum necessary & reasonable safeguards requirements met

Incidental Use/Disclosure

- Talking to a resident in a semi-private room
- Talking to other providers if passers-by are present
- Using sign-in sheets
- Keeping resident chart at bedside

Sharing of PHI

- For payment or treatment of patient of other entities
- Operations such as QA & antifraud & abuse
- Operations of another CE that has or had a relationship with a resident

Health Care Operations

- Q/A, training, accreditation, licensing
- Medical review, auditing & legal services
- Business planning, development, & management

Other Entity

- Covered entity may disclose PHI for treatment/payment activities of other covered entities or other health care providers, & for certain health care operations of other entities

Authorization Beyond Consent

- Covered entity may ***not*** use or disclose protected health information without valid written & time-limited authorization

Minimally Necessary

- Using/disclosing/requesting protected health information from another covered entity
- Covered entity must make ***reasonable efforts*** to limit protected health information to minimum necessary to accomplish intended purpose

Except for Treatment

- ***No*** "minimally necessary" for ***disclosures*** to or requests by (but ***not*** use by) a health care provider for treatment

Workforce

- Employees, volunteers, trainees, & others who work under direct control of a covered entity, whether or not paid

- Must train & oversee

Business Associate

- Provides financial, actuarial, accounting, consulting, claims, data aggregation, management, administrative, legal, accreditation, financial services for CE
- Must have individually identifiable health information

Business Associate

A business associate shall:

1. Not use/disclose protected health information other than as permitted by contract or required by law
2. Use appropriate safeguards to prevent use or disclosure
3. Report unauthorized use or disclosure of which Business Associate becomes aware

Business Associate

A business associate shall:

4. Ensure that agents agree to same covenants & restrictions
5. Make available PHI for individual access
6. Make available PHI for amendment & incorporate amendments
7. Make available PHI for accounting

Business Associate

A business associate shall:

8. Make compliance books & records available to HHS for purposes of determining Covered Entity's compliance
9. At end of arrangement return or destroy all PHI & return any copies or keep & protect if infeasible

Business Associate

10. The contract must authorize termination if Covered Entity determines that Business Associate violated material term of contract

Unless inconsistent with statutory obligations of the Covered Entity or Business Associate

Covered Health Plans

Group Health Plan

- ERISA Emp. Wel. Ben. Plan
- =>50 participants or TPA
- Insurer, HMO, 'Care, 'Caid
- Or any other individual or group plan that pays for cost of care

ERISA Plans

- Employee Retirement Income Security Act (ERISA) governs approximately 2.5 million health benefit plans sponsored by private sector employers nationwide
- Provide a wide range of medical, surgical, hospital and other health care benefits to 131 million Americans

Disclosures to Sponsor

- Plan documents restrict use/disclosure
- May disclose summary health info.
- To obtain premium bids & modify, amend, terminate plan
- Amend plan to establish permitted & required uses/disclosures
- Ensure agents/subs. getting PHI agree to same restrictions/conditions as plan sponsor

Sponsor Requirements

- Don’t use information for employment-related actions/decisions or other benefit plans
- Report inconsistent disclosures
- Show internal practices/books/records on PHI use/disclosure to HHS for compliance

Sponsor Requirements

- Destroy/return PHI when no longer needed
- Provide for adequate separation from plan
- Restrict employee access/use
- Lawyer/client privilege

Sponsor vs. Plan

- Fiduciary responsibilities
- Cost allocations
- Insurance
- Personnel additions

- Two entities, not one

Disclosures to Sponsor

- To carry out administration
- Restrict insurer/HMO disclosures
- No disclosure for employment-related actions/decisions or in connection with other benefit plan of sponsor
- Sponsor ***not*** covered entity or business associate or workforce

Enrollee Rights

- Notice from plan ***OR***
- Notice from insurer/HMO
- But plan must maintain/provide limited notice
- "This notice describes how medical information about you may be used & disclosed & how you can get access to this information…."

Special Plan Notice

- On compliance date to all covered individuals
- Thereafter at time of enrollment
- Within 60 days of material revisions to notice
- At least every three years tell them how to get notice of rights

Exceptions for Plans

- Benefits solely thru insurer/HMO
- Do not create/receive PHI other than summary or participation information

Group Plans

- Group health plan may disclose enrollment/disenrollment information to plan sponsor
- Employer may know whether individual is in or disenrolled from employer health plan

Psychotherapy Is Special under HIPAA

Psychotherapy Notes

• Notes recorded (in any medium) by health care provider who is a mental health professional documenting or analyzing contents of conversation during a private counseling session or a group, joint, or family counseling session and *that are separated from the rest of the individual's medical record*

Health Plans & Psych. Notes

- Health plans may *not* condition payment, eligibility, or enrollment on the receipt of an authorization for the use or disclosure of psychotherapy notes, even if the health plan intends to use the information for underwriting or payment purposes

Two Filing Cabinets: HR & Health Care

HIPAA & Banks

Different Strokes for Different Folks

- *Organizing* – Organized Health Care Arrangement
- *Affiliating* – Affiliated Covered Entities
- *Hybridizing* – Hybrid Entities
- *Associating* – Business Associates

HIPAA Is About Security

Single Security Standard

- "There is no recognized single standard that integrates all the components of security (administrative procedures, physical safeguards, technical security services, & technical mechanisms) that must be in place to preserve health information confidentiality & privacy as defined in the law. Therefore, we are designating a new, comprehensive standard, which defines the security requirements to be fulfilled…."

HIPAA Security Law

- Each person described in HIPAA law shall maintain reasonable & appropriate administrative, technical & physical safeguards--
- To ensure the integrity & confidentiality of the information

HIPAA Security Law

- To protect against any reasonably anticipated:
- (i) threats or hazards to security or integrity of information &
- (ii) unauthorized uses or disclosures of information; &
- Otherwise ensure compliance by officers & employees

HIPAA Security Standards

- General Administrative Procedures
- Physical Safeguards to Guard Data Integrity, Confidentiality, & Availability
- Technical Security Services to Guard Data Integrity, Confidentiality, & Availability
- Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network

Where Was the Final HIPAA Security Rule?

- In a lockbox?

- In a secure location?

First Technologarian
Privacy vs. Security

- *Privacy:*
- Individually identifiable health information in any format (paper, electronic, etc.) (PHI)
- *Security:*
- Electronic protected health information (EPHI)

Basic HIPAA Security

- Maintain reasonable & appropriate administrative, technical, & physical safeguards to --
- (A) ensure the integrity and confidentiality of the information;
- (B) protect against any reasonably anticipated--
  - (i) threats or hazards to the security or integrity of the information; &
  - (ii) unauthorized uses or disclosures of the information; &
- (C) otherwise to ensure compliance with this part by the officers & employees of such person.

Business Associate

- Covered entities are not required to provide training to business associates

or anyone else that is not a member of their workforce

HIPAA Preemption

- Final security rule preempts state law
- Final privacy rule does *not* preempt contrary/more stringent state law
- Final standards/data sets rule preempts state law

Security Rule Preemption

- The general rule is that the security standards in this final rule supersede contrary State law
- Covered entities may be required to adhere to stricter State-imposed security measures that are not contrary to this final rule

HIPAA Preemption

- Will your governor & legislature impose stricter & more stringent privacy & security requirements for your state?
- States of confusion!

Security for Management

- Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management)

No HIPAA for Undertakers
Got a date?

- Enactment date
- Publication date
- Effective date
- Enforcement date
- Compliance date

Goldberg Dates HIPAA

- OCT 14 02 – gap bus. assoc. contract
- OCT 15 02 – file ASCA plan
- OCT 16 02 – *data code sets/trans. rule
- APR 14 03 – *enforce privacy rule
- APR 16 03 – final six month testing
- OCT 16 03 – extended code sets/trans

- APR 14 04 – final bus. assoc. contract
- APR 21 05 – *final security rule compliance

*except small health plans

Sign On Dotted Line

HIPAA Documents

- Business Associate Agreement
- Chain of Trust Agreement
- Trading Partner Agreement
- Limited Data Set Data Use Agreement
- Certification/Testing

Business Associate Agreement

- Written contract
- Model provisions provided by HHS but not mandatory
- NOT A SAFE HARBOR
- Third party beneficiary
- Stop Gap BA contract

Chain of Trust Agreement

- Contract entered into by two business partners in which the partners agree to electronically exchange data & protect the integrity & confidentiality of the data exchanged
- Part of HIPAA security administrative procedures (optional) to guard data integrity, confidentiality, & availability

Trading Partner Agreement

- *Privacy Rule* agreement related to exchange of information in electronic transactions, whether distinct or part of larger agreement, between each party to agreement
- May specify, among other things, duties & responsibilities of each party to agreement in conducting a standard transaction

Limited Data Set Use Agreement

- Agreement by recipient of limited data set information (that does not include directly identifiable information) to limit use for research, public health & health care operations (BUT STILL PHI)

Certification/Testing

- Risk management
- Loss prevention
- Investigation strategy
- Litigation defense

Administrative Simplification Compliance Act - 2001

- AN ACT To ensure that covered entities comply with the standards for electronic health care transactions & code sets adopted under part C of title XI of the Social Security Act, & for other purposes

ASCA

- Before October 16, 2002, submit to HHS plan of how covered entity will come into compliance with data sets requirements not later than October 16, 2003
- Plan shall be a summary of:
- Analysis reflecting the extent to which, & reasons why, covered entity *not* in compliance
- Budget, schedule, work plan, & implementation strategy for achieving compliance

ASCA

- Whether covered entity plans to use/might use contractor or other vendor to assist in achieving compliance
- Timeframe for testing that begins not later than April 16, 2003
- Plans may be submitted electronically
- HHS provided optional form for electronic or paper filing *not later than* October 15, 2002

ASCA

- From and after 10/16/03 the Medicare Program's one million certified providers (with some exceptions) must go HIPAA electronic

ASCA

- Covered entity that fails to submit timely ASCA plan & that is not in compliance on *or after October 16, 2002*, may be excluded at HHS discretion from Medicare program
- Availability of such exclusion does *not* affect imposition of civil penalties

ASCA

- From April 14, 2003 to October 16, 2003, a health care provider or health care clearinghouse that transmits any health information in electronic form in connection with *a described transaction* shall comply with the requirements of the final privacy rule *without regard to whether transmission meets the data code sets standards*

NCVHS Analysis of Plans

- NCVHS shall regularly publish, & widely disseminate to the public, reports containing effective solutions to compliance problems identified in the plans so analyzed
- Such reports shall not relate specifically to any one plan but shall be written for the purpose of assisting the maximum number of persons to

come into compliance by addressing the most common or challenging problems encountered by persons submitting such plans

No Business Associate Contract With Janitors
HIPAA is not Mr. Roger's Neighborhood, but...

Enforcer With a Heart
Your Government Is Watching You
Enforcement

- HHS sanctions for violations
- Federal civil sanctions
- Federal criminal sanctions
- State sanctions
- Contractual sanctions
- Professional sanctions

HIPAA Corporate Compliance Program

- DOJ Sentencing Guidelines
- Can abate costs/penalties & enforcement actions

Chief Privacy Official
Chief Compliance Official
Chief Security Official

HIPAA BULL

Privacy Rule

- Enforcement provisions already included
- More coming but not under HIPAA AdSi

Cooperation

- HHS will, to extent practicable, seek cooperation of covered entities in obtaining compliance

We're Here to Help You

- HHS may provide technical assistance to covered entities to help them comply voluntarily

Complaints

- Person who believes covered entity is not complying with HIPAA may file complaint within 180 days+

Must Mitigate

- Covered entity must mitigate, to extent practicable, *known* harmful effect of violations involving use/disclosure of protected health information by business associates

Investigations

- HHS may investigate complaints & review policies, procedures, & practices of covered entity & circumstances regarding alleged compliance acts & omissions

Access to Records

- Covered entity must keep records & submit compliance reports, as, when & how HHS requires
- In exigent circumstances if documents may be hidden or destroyed, covered entity ***must*** permit access by HHS at any time without notice

Findings

- If investigation/compliance review indicates failure to comply, HHS may attempt informal resolution
- If violation occurs & informal resolution not possible, HHS may issue written findings documenting non-compliance

Investigations

- HHS may investigate complaints
- Review of policies, procedures, or practices of covered entity & circumstances regarding alleged acts/omissions concerning compliance

Compliance Review

- Covered entity must cooperate with investigation

- Permit access during normal business hours to premises & records *including protected health information*
- Access *already exists* under Medicare/Medicaid/state license

Risk Assessment HIPAA BULL!!!!!

Judge Jones says:

- [I]n light of the strong federal policy in favor of protecting the privacy of medical records….”

Judge Jones says:

- “In accord with the [HIPAA privacy] Standards issued by [HHS[….”

NICE HIPAA

HIPAA For Dummies

- Civil sanctions for violation of standards
- Except if you *did not know*
- Exercising *reasonable diligence* you *would not have known* of violation
- Penalty waived if violation due to *reasonable cause* & *not willful neglect*
- 30 days+ to cure & technical advice
- $100 for each violation or $25,000/year

BAD HIPAA

VERY BAAAD HIPAA

HIPAA For Crooks

- *Knowingly:* unlawful use or disclosure
- $250,000 + 10 years in jail if with *intent* to sell, transfer or use health information for commercial advantage, personal gain, or malicious harm

FIRST HIPAARARIAN

National Association of Attorneys General

Bad HIPAA Conspiracy

- Could a person conspire with a covered entity to cause a violation of HIPAA for crooks?
- Defendant charged with conspiracy to violate HIPAA need not be able to violate HIPAA

Bad HIPAA Misprison of a Felony

- Could a person, having actual knowledge of commission of a HIPAA felony, fail to notify HHS & take affirmative steps to conceal?
- Defendant charged with misprison of a HIPAA felony need not be able to violate HIPAA

Bad HIPAA Obstruction of Justice

- Could a person obstruct justice by interfering with the enforcement of HIPAA?
- Defendant charged with obstruction of justice need not be able to violate HIPAA

Bad HIPAA
"Knowingly"

- Has actual knowledge of actions
- Deliberate ignorance or reckless disregard of truth
- Mere intent to act instead of specific intent to violate law
- Not innocent mistake or negligence

Bad HIPAA
"Intent"

- Has actual knowledge that actions would violate HIPAA
- Need not intend specific result
- Result of actions inevitable

- Voluntary act or omission

Covered Entity As Business Associate: Double Trouble

- (3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a)

Avoid Enforcement

- Use reasonable diligence to know as much as you can about HIPAA
- Establish policies that evidence a reasonable approach to prevention
- Don't be neglectful or reckless
- Try to cure breaches within 30 days
- Ask for an extension if necessary
- Seek technical advice if necessary

Private Litigation Risk

- HIPAA AdSi rules will become the rule of the street for tort (negligence) litigation
- State authorities permit commencement of consumer protection litigation by private litigant

Private Litigation Risk

- Contract litigation involving agreements entered into before or after HIPAA AdSi rules
- Indemnification agreements

Private Litigation Risk

- Insurance protection
- Exceptions, exclusions, conditions in policy terms
- Retention
- Excess/Umbrella
- Manuscript

Weld et al. vs. CVS et al.

- CVS scanned databases for drug company criteria
- Mailings to customers from CVS promoting drugs
- Alleged conspiracy with drug companies against "class"

Judge Jones says:

- [I]n light of the strong federal policy in favor of protecting the privacy of medical records…."

Judge Jones says:

- "In accord with the [HIPAA privacy] Standards issued by [HHS[…."

Louisiana Judge says:

- In the instant case, relators & the United States argue that the HIPAA Standards do not apply because the final compliance date for health care providers is April 14, 2003.

- LA law is NOT more stringent
- ...I agree with District Judge Jones of the Northern District of Virginia....”

Status of Litigation

- *Plaintiffs’ Zero, HIPAA Won!*
- *South Carolina Med’l As’n*
  - *CASE DISMISSED*
- *As’n of Amer. Physicians & Surgeons*
  - *CASE DISMISSED*

Behavioral Health vs. HIPAA Regulatory Permission to Use/Disclose

- Office for Civil Rights will enforce final privacy rule

- Centers for Medicare & Medicaid Services will enforce final transactions rule & security rule

S E E A M E S S

- Deadline Countdown
- Today is Sunday, September 14, 2003.
  The testing deadline (April 16, 2003) for electronic transactions and code sets has passed (ASCA plan deadline, no rule)
- There are 32 days left until the October 16, 2003 compliance date for electronic transactions and code sets

- 9/8/03 CMS FAQs
- What will Medicare's contingency plan be?
- Answer - Medicare's contingency would be to continue to accept and send transactions in legacy formats – in addition to HIPAA compliant transactions - while trading partners work through issues related to implementing the HIPAA standards. The contingency plan will be the same for all Medicare's fee-for-service contractors

- 9/8/03 CMS FAQs
- A decision on whether to deploy a contingency will be made by September 25, 2003. Medicare will continue its active outreach and testing efforts to bring its trading partner community into compliance with the HIPAA standards

- 9/11/03 STATEMENT OF LESLIE V. NORWALK, ACTING DEPUTY ADMINISTRATOR, CENTERS FOR MEDICARE & MEDICAID SERVICES

- CONTINGENCY PLAN AND COMPLIANCE WITH THE HIPAA TRANSACTION AND CODE SETS ON OCTOBER 16, 2003
- October 16 is just 35 days away, and all covered entities should be actively working with their trading partners on outreach, testing and contingency planning. This deadline is the law and we all have to deal with it. It's not something that can be ignored or brushed aside

- Now we are working on the possibility of Medicare implementing a contingency plan. And I urge other health plans to announce their contingency plans as soon as possible to allow their trading partners enough time to make any needed changes to their business operations to make sure any disruptions in their health care operations are minimal

- On July 24, 2003, the Department of Health and Human Services (HHS) issued guidance regarding the enforcement of the HIPAA transactions and code set standards after October 16, 2003. Industry support remains strong for the HIPAA transaction and code set standards. However, we are not confident that providers are ready or that they have enough time for adequate testing.

- HHS recognizes that transactions often require the participation of two covered entities and that noncompliance by one covered entity may put the second covered entity in a difficult position. The Departmental guidance clarified that covered entities, which made a good faith effort to comply with HIPAA transaction and code set standards, may implement contingencies to maintain operations and cash flow

- Medicare's contingency plan is to continue to accept and process transactions that are submitted in legacy formats while their trading partners work through issues related to

implementing the HIPAA standards. Medicare will make a decision on whether to deploy this contingency no later than 9/25/03

- In reviewing its trading partner readiness and whether to deploy its contingency, Medicare will assess the number of Medicare submitters who are testing and in production with our contractors. If Medicare deploys this contingency, it will be for all Medicare fee-for-service contractors. Medicare will continue its active outreach and testing efforts to bring its trading partner community into compliance in the days before and, if necessary, after October 16, 2003

- 9/8/03 CMS FAQs
- What is an acceptable contingency plan? Answer An acceptable contingency plan is whatever is appropriate for the individual plan's situation in order to ensure the smooth flow of payments. Health plans will need to make their own determinations regarding contingency plans based on their unique business environments

- 9/8/03 CMS FAQs
- A contingency plan could include, for example, maintaining legacy systems, flexibility on data content or interim payments. Other more specific contingency plans may also be appropriate. For example, a plan may decide to continue to receive and process claims for supplies related to drugs using the NCPDP format rather than the 837 format currently specified in the regulations. ***The appropriateness of a particular contingency or the basis for deploying the contingency will not be subject to review***

Congressional Testimony

- HCFA [CMS] lacks specially trained personnel to oversee security

- HCFA's contractors are *outright obstructive* to providing sound security
- Compounding these errors was HCFA's inability to catch or prevent errors

Guidance Overview

- 17 "reasonable(ly)" steps, criteria, reliance, efforts, safeguards, precautions
- 18 "professional(ly)"
- 7 "professional judgment"
- 23 "appropriate(ly)"

HIPAA BULL!!!!!

Clarifications

- HIPAA does NOT require:
- Private rooms
- Soundproofing of rooms
- Encryption of wireless radio
- Encryption of telephone systems
- Silence in semi-private rooms
- Using Navajo Indian language

Fannie Mae

Freddie Mac

Sallie Mae

HIPAA Mae

Compliance in a box?

- HIPAA BULL

See a psychiatrist if you still don't get it....

The HIPAA Clock Is Ticking

- What should a HIPAA covered entity or business associate do now?

Are you still looking for your HIPAA solution?

ARE *YOU* THE WEAKEST LINK?

Which Way Are We Going?

Don't Get Behind HIPAA

Learn the HIPAA HERO® Way

Professor Goldberg's

Y3K Year 3000 Readiness Disclosure

- To the best of my knowledge, this presentation will not cause the interruption or cessation of, or other negative impact on, business or other operations, attributable directly or indirectly to the processing (including but not limited to calculating, comparing, sequencing, displaying, or storing), transmitting, or receiving of date data from, into, and between the 20th and 22nd centuries, and during the calendar year 1998 and thereafter (including but not limited to the calendar years 1999-3000), and leap year calculations, or give rise to the inability of one or more computer software or hardware programs, machines or devices accurately to receive, store, process or transmit data on account of calendar information applicable to such programs, machines or devices, including without limitation calendar information relating to dates from and after the date hereof.

Why is this man smiling?

Practice Safe HIPAA!

www.healthlawyer.com

That's All Folks!