HIPAA SUMMIT IX Boot Camp

Alan S. Goldberg, JD, LLM

www.healthlawyer.com

Who Am I

- **Goulston & Storrs, 1967 --**
- **JD Boston College Law School**
- **LLM (Taxation) Boston University**
- **Past Pres. American Health Lawyers As'n**
- **Council Member, ABA Health Law Section**
- **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**

First Technologarian

***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 Security

On internet nobody knows you're a dog

Conditions of Participation

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**

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 applies to: --

- **Health plan**
- **Health care clearinghouse**
- **Health care provider that transmits health information electronically in connection with HIPAA covered transaction**
- **Drug card vendors**

HIPAA Applicability

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

Lost HIPAAginity

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 – BUT….**
- **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**

Direct Covered Health Care 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 caller is beneficiary by asking for: Full name; Date of birth; HIC number; & One additional piece of information such as SSN, address, phone number, effective date(s), whether caller has Part A and/or Part B coverage**

CMS Contractor Call Center

- **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**

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**

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**

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

HIPAA NOTICE OF SECURITY PRACTICES

- **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU WILL BE SECURED AND PROTECTED. PLEASE REVIEW IT CAREFULLY."**
- **Not required by Security Rule but should this be considered?**

Privacy vs. Security

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

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 <u>preempts</u> state law**
- **Final privacy rule does *<u>not</u>* <u>preempt</u> contrary/more stringent state law**
- **Final standards/data sets rule <u>preempts</u> 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!**

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**

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**

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 rules but not under HIPAA AdSi**

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**

OCR Civil Actions

- **Received & initiated reviews of over 7,577 complaints**
- **Closed 57%, including cases in which: --**
- **OCR lacks jurisdiction under HIPAA**
- **Allegation of violation prior to the compliance date, or of violation by entity not covered by Privacy Rule, or where activity alleged does not violate the Rule**
- **When covered entity has declined to disclose protected health information in circumstances where the Privacy Rule would permit disclosure**
- **Where the matter has been satisfactorily resolved through voluntary compliance – such as where individual is provided access to medical record based on a complaint of denial**

Most frequent complaints

- **(1) Impermissible use or disclosure of individual's identifiable health information**
- **(2) Lack of adequate safeguards for protection**
- **(3) Refusal or failure to provide individual with access to or a copy of records**
- **(4) Disclosure of more than is minimally necessary to satisfy particular request for information**
- **(5) No valid authorization for disclosure**

Civil complaints are most often filed against: --

- **Private health care practices**
- **General hospitals**
- **Pharmacies**
- **Outpatient facilities**
- **Group health plans**

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**
- **Non-covered entity?**

National Association of Attorneys General

Bad HIPAA Conspiracy

- **Could a non-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 non-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 non-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[…."**

University of Colorado
Hospital Authority v. Denver Publishing Co

- **HIPAA AdSi does not allow Denver area hospital to sue to prevent newspaper from publishing peer review data, a federal court has ruled (8/2/04)**
- **Judge Walker Miller said HIPAA does not provide private right of action that would allow Hospital Authority to sue Rocky Mountain News over publication of information from peer review of a neurosurgeon at the hospital**

US vs. Richard W. Gibson

- **Employee of covered health care provider disclosed name, date of birth, & Social Security number of patient to AT&T Universal Card for personal gain**
- **Intended unlawfully to get credit card in name of patient**
- **Agreed to plead guilty to violation of HIPAA & likely to go to jail**
- **Mr. Gibson is NOT a covered entity or a business associate: he's a mere "person"**

Doctors vs. HIPAA

- ***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 – Case on Appeal

•Office for Civil Rights enforces final privacy rule

S E E A M E S S

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

- **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***

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 <u>NOT</u> 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

Sallie Mae

HIPAA Mae

Compliance in a box?

•

HIPAA BULL

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

FIRST HIPAARARIAN

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? Revoke it, amend it, replace it?

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?

I Practice Safe HIPAA!

And so should you!

That's All Folks!

goulston&storrs
counsellors at law

Alan Stuart Goldberg is a member of the bars of the District of Columbia, Massachusetts, New York, and Florida. Mr. Goldberg concentrates in the practice of business and administrative law including the delivery of health care and information technology. Goulston & Storrs provides creative solutions in the areas of real estate, taxation, estate planning, bankruptcy, health care, drugs and devices, litigation, technology, and complex business transactions nationally, and internationally via a London, UK office.

Mr. Goldberg's introduction to health law and information technology occurred during the dawning of the Medicare/Medicaid programs era as a staff judge advocate and a prosecutor in the United States Navy, and Mr. Goldberg was also involved in investigative actions relating to the USS Pueblo and the Sealab project. Mr. Goldberg joined Goulston & Storrs in 1967 upon graduation from Boston College Law School, where he was a member of the Law Review and received an academic scholarship, and as a Lecturer in Law presented a course in land finance. In 1978 Mr. Goldberg received an LL.M. (Taxation) from Boston University School of Law. Mr. Goldberg serves as an Adjunct Professor at the University of Maryland School of Law and at Boston's Suffolk University Law School. He is a Past President of National Health Lawyers Association (1991-1992) and served on the AHLA Board of Directors from 1981 to 1993; and served as an Internet advisor to the Health Lawyers Board. Mr. Goldberg received the National Health Lawyers Association David J. Greenburg Service Award in 1996.

Mr. Goldberg has published on many business, health law, and other legal issues and he has frequently lectured for the American Health Lawyers Association, and also for many bar and other associations including the Massachusetts, District of Columbia, Florida, Virginia and South Carolina bars; the Massachusetts Hospital Association, Dental Society, Medical Society, and Long Term Care Foundation; the American Telemedicine Association; the Workgroup For Electronic Data Interchange; the American Health Care Association; the Healthcare Information and Management Systems Society; the United States Navy; the Centers for Medicare and Medicaid Services; and for many other organizations, and he participates in many national conferences as a moderator and a lecturer.

Mr. Goldberg was the Editor of a law and computer technology column called “The Computer Wizard” published by the American Bar Association's Business Law Section magazine “Business Law Today”; and he is the founding moderator of the American Health Lawyers Association Health Information and Technology Internet listserv. Mr. Goldberg has presented loss prevention seminars relating to technology issues to the membership of Attorneys’ Liability Assurance Society. Among Mr. Goldberg’s current interests are national and international challenges and opportunities involving the application of technology to the practice of law and medicine and to the delivery of healthcare, including issues involving the Internet, security and encryption, privacy and confidentiality, software licensing and devices, corporate compliance programs and ethics, and telemedicine. Mr. Goldberg served as Vice Chair of the American Health Lawyers Association Health Information and Technology Practice Group, and Chair of the American Bar Association Health Law Section’s e-Health & Privacy Interest Group; and he cochairs The National HIPAA Summit series of events and is a Council Member of the ABA Health Law Section and its first Substantive Webmaster and he is a Steering Committee Member of the DC Bar Health Law Section.

Mr. Goldberg is the Webmaster of ***http://www.healthlawyer.com***; and agoldberg@goulstorrs.com is his electronic mail address. Mr. Goldberg is now resident in the Washington, DC office of Goulston & Storrs.

1717 Pennsylvania Av., NW, Suite 625, Washington, DC 20006, 202.721.1137, fax 617.574.7583