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**
  Univ. of Maryland School of Law
  Suffolk University Law School

It's all in the cards

San Diego 1968
CDR Rabb JAGC
LT Goldberg JAGC
Boston Lawyer
Inside the Beltway

Professor Goldberg's

Honest Lawyer Privacy Policy

- **Nothing I say in this room is private**
- **Everything you say in this room is public**

goulston&storrs
counsellors at law

Resume of Alan S. Goldberg, JD, LLM

Alan S. Goldberg is a member of the bars of the District of Columbia, Massachusetts 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 and medical devices, litigation, and complex business transactions nationally, and internationally via a London, UK office.

Mr. Goldberg's introduction to health law occurred in the 1960s, during the dawning of the Medicare and Medicaid programs era as a judge advocate and prosecuting attorney in the United States Navy, and Mr. Goldberg was also involved in investigative actions relating to the USS Pueblo and the Sea-lab 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 is an Adjunct Professor of Law at University of Maryland School of Law and Mr. Goldberg also taught at Boston's Suffolk University Law School. He is a a Past President of National Health Lawyers Association ('91-'92); served on its 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 extensively on a broad range of health law, and many other legal issues and has frequently lectured for American Health Lawyers Association and also for many bar and for other associations; the Massachusetts Hospital Association, Dental Society, Medical Society, and Long Term Care Foundation, the American Telemedicine Association, the Workgroup For Electronic Data Interchange, the Healthcare Information and Management Systems Society, and for governmental and other organizations and he participates in many national teleconferences as a moderator and a lecturer.

Mr. Goldberg was the moderator of the Health Law Forum computer on-line feature of CounselConnect; he is the Editor of a law and computer technology column entitled "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 telemedicine. Mr. Goldberg has 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 originated the HIPAA HERO® teaching methodology.

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

- **We have zero privacy in this room: get over it!**

We Have Lots of Law

- **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

What are the three biggest

HIPAA lies?

My Software Is HIPAA Compliant

My Hardware Is HIPAA Compliant

I Am HIPAA Compliant

HIPAA BULL

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

Medicare/Medicaid Program
Conditions of Participation
Conditions of Participation

?Right to personal privacy & confidentiality of personal & clinical records

<u>Not</u> 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.**

Zebras, Horses, HIPAAs

HIPAA from 40,000 feet up

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 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**

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

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 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

Gramm-Leach-Bliley

GLB: Not protected if public

HIPAA: Always protected

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 Creates
Obligations & Liabilities

•Operation Cure.All

National Association of Attorneys General
Unfair & Deceptive Trade Practices

Notice of Privacy Practices To Be Provided By Direct Covered Health Care Provider In First Patient Encounter

- **Acknowledgment required**
- **Writing or electronic**
- **Good faith efforts**
- **Layered notice on top is okay**

Patient Rights

- **To see patient health information**
- **To know about disclosures of patient health information**

Protected Health Information
Accounting for Disclosures

- **6 years (other than disclosures for payment, treatment, health care operations, or patient authorized, or by law)**

Incidental Use/Disclosure

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

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**

Agreement Terms

- **Amendment to comply with changes in law**
- **Interpretation in favor of compliance by CE**
- **No 3rd party beneficiaries**
- **Maintain lawyer/client privilege**
- **No agency or joint venture**
- **Reasonability to "help CE comply", not guarantee**
- **Force majeure**
- **BA compliance with state law nevertheless**
- **No indirect/consequential/peremptory damages**

Agreement Terms

- **Indemnification/hold harmless/exoneration**

- **Contract vs. tort vs. indemnity: no fault?**
- **Insurance protection NOT**
- **Notice**
- **Right to assume defense or participate in same**
- **No settlement without concurrence**
- **Subrogation**
- **Statute of limitations & termination of obligation**

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

Different Strokes for Different Folks

- *Organizing* - Organized Health Care Arrangement – NO ELECT?
- *Affiliating* - Affiliated Covered Entities - ELECT
- *Hybridizing* - Hybrid Entities - ELECT
- *Associating* - Business Associates vs. Workforce - ELECT

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's the Final HIPAA Security Rule?

- **In a lockbox?**

- **In a secure location?**

Privacy vs. Security

- ***Privacy:***
- **Individually identifiable health information in any format (paper, electronic, thought)**
- ***Security:*** **(change in final rule?)**
- **Electronic health information**

No HIPAA for Undertakers

No Business Associate Contract With Janitors

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**

***except small health plans**

Contracts Create Liabilities

HIPAA Documents

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

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

USA/Stewart vs. LA Clinic

- False claims act qui tam action naming MDs/clinic, 'Care/'Caid
- Defs. sought protective order for non-party patient records in order to avoid civil liability to patients under LA law

USA/Stewart vs. LA Clinic

- HIPAA does not preempt contrary state law that relates to privacy of individually identifiable health information & is more stringent than HIPAA

USA/Stewart vs. LA Clinic

- Defendants say LA law more

stringent because notice to patient required before provider can produce nonparty patient records without consent

USA/Stewart vs. LA Clinic

- **Quoting Judge Jones, and**
- **The HIPAA standards will require full compliance in a mere 4 months, when litigation will be ongoing with trial set for Oct. 2003**

US vs. Sutherland

- **USDC Northern VA**
- **Criminal prosecution of MD with patient records sought by the prosecution**

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[…."**

USA/Stewart vs. LA Clinic

- **HIPAA supercedes contrary state law, unless state law relates to privacy of IIHI & is more stringent than HIPAA**
- **But LA law does not address the form, substance, or need for express legal permission from an individual**

USA/Stewart vs. LA Clinic

- **Rather, LA law provides way of negating need for such permission**
- **Patient may attend hearing, but LA court "shall...order... disclosure (despite [no] consent) if court finds release is proper**

USA/Stewart vs. LA Clinic

- **Therefore court may order disclosure of**

nonparty patient information without state law hearing or consent

- **All parties agree (& court "strongly agree[s]") that good cause exists for protective order**

USA/Stewart vs. LA Clinic

- **Standard: disclosure for judicial & administrative proceedings**
- **Court to order disclosure to parties, parties' counsel of record, <= 2 paralegals & 1 expert per party**
- **All must sign affidavit agreeing to protective order**

Enforcers 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**

OCR: Privacy
CMS: Transactions

- **Enforcement rules from OCR & CMS coming**
- **No 2 yr./2 mo. delay**
- **Security by CMS?**

Chief Privacy Official
Chief Compliance Official

S E E A M E S S
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**

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"**

Status of Litigation

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

HIPAA BULL!!!!!

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**

False Claims Act (Civil)

- **"Knowing" or "Knowingly" is not solely specific intent, instead it means any of the following:**
  - **having actual knowledge of the information**
  - **acting in deliberate ignorance of the truth or falsity of the information; or**
  - **acting in reckless disregard of the truth or falsity of the information**

Nice HIPAA

"Reasonable Diligence"

- **Practicable**
- **Ordinary business care**
- **Normal prudence**

Nice HIPAA
"Willfully Neglectful"

- **Conscious intentional failure**
- **Reckless indifference**
- **In reckless disregard of truth**
- **No specific intent to violate HIPAA**
- **Not innocent mistake or negligence**

False Claims Act (Civil)

Eight Factors the DOJ/OIG Must Consider

1. **Notice of Rule or Policy**
2. **Clarity of Rule or Policy**

3. **Pervasiveness/ Magnitude of False Claims**
4. **Adherence to a Compliance Plan**
5. **Identification of/Response to Noncompliance**
6. **Guidance Sought from HCFA**
7. **Previous Audits for Same Issues**
8. **Any Other State of Mind Information**

False Claims Act (Civil)

Five Responses DOJ/OIG Must Consider

- **good faith reliance upon applicable statutory and regulatory provisions and interpretations**
- **misled by inconsistent and often contradictory guidance from the carrier**
- **provider's well-documented compliance and self-reporting procedures did not reveal the billing mistake**
- **error was immaterial**
- **"innocent" mistake/no intent to defraud**

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

Bad HIPAA Conspiracy

- **Could a business associate conspire with a covered entity to cause a violation of HIPAA for Crooks?**
- **Person charged with conspiracy to violate HIPAA need not be able to violate HIPAA**

Bad HIPAA Misprison of a Felony

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

Bad HIPAA Obstruction of Justice

- **Could a business associate obstruct justice by interfering with the enforcement of HIPAA?**

- **Person 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**

False Claims Act (Criminal)

"Whoever…knowingly and willfully makes or causes to be made any false statement or representation of a material fact in any application for any benefit or payment under a Federal health care program...."

HIPAA Corporate Compliance Program

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

Antifraud & Abuse Effective Compliance Plan

1. **Establish written standards & procedures**
2. **Designate responsible individuals**
3. **Regular & effective training**
4. **Effective means of communication**
5. **Audit & monitor compliance**
6. **Compliant hiring & discipline**
7. **Establish investigation protocols**

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**

Office for Civil Rights Compiled Privacy Rule

•34 reasonable

HHS Guidance 7/01

- **17 "reasonable(ly)"**
- **25 "professional(ly)"**
- **7 "judgment"**
- **23 "appropriate(ly)"**

OCR Guidance 12/02

- **58 "reasonable(ly)"**

- **34 “professional(ly)”**
- **17 “judgment”**
- **39 “child(ren)”**

Compliance in a box?

- **HIPAA BULL**

The HIPAA Clock
Is Ticking

- **What should**

a HIPAA
covered entity
or business
associate
do now?

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 of this presentation.

Why is this man smiling?

Practice Safe HIPAA!

www.healthlawyer.com

That's All Folks!