



HIPAA

*goulston&storr*s
think*results*

Washington, DC & Boston, Mass. & London, UK

Alan S. Goldberg, JD, LLM

www.healthlawyer.com

© Copyright 2002 Alan S. Goldberg All Rights Reserved

©www.hipaahero.com®



Who Am I

- **Goulston & Storrs since 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

CDR Rabb JAGC

LT Goldberg JAGC

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

**Federal
Law**

**Professional
Obligations**

**State
Law**

Privacy Before HIPAA

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 It's Powerful
And Awesome

*Privacy Added To End of
Employee Benefits Law*

AAdministrative SSimplification

Subtitle

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

- **Patient has right to personal privacy & confidentiality of personal & clinical records**

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.

The Book of HIPAA
Ministry of Spirit of HIPAA

HIPAA from 40,000 feet up

Hippapotamus

Name: *Hippapotamus Medicus*

Size: Ten data sets long plus unlimited attachments

Weight: More than you can carry

Lifespan: Infinite

Habitat: Hospital, HMO, nursing home, health plan, dentist, MD

Diet: Raw info. services staff

Gestation Period: Six years

Zebras, Horses, HIPAAs

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**

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 Standards

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

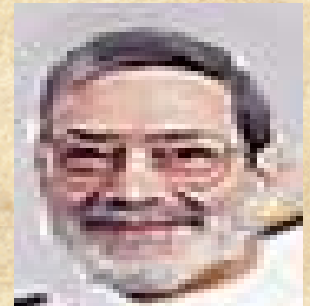
Loose Lips Sink Privacy

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**

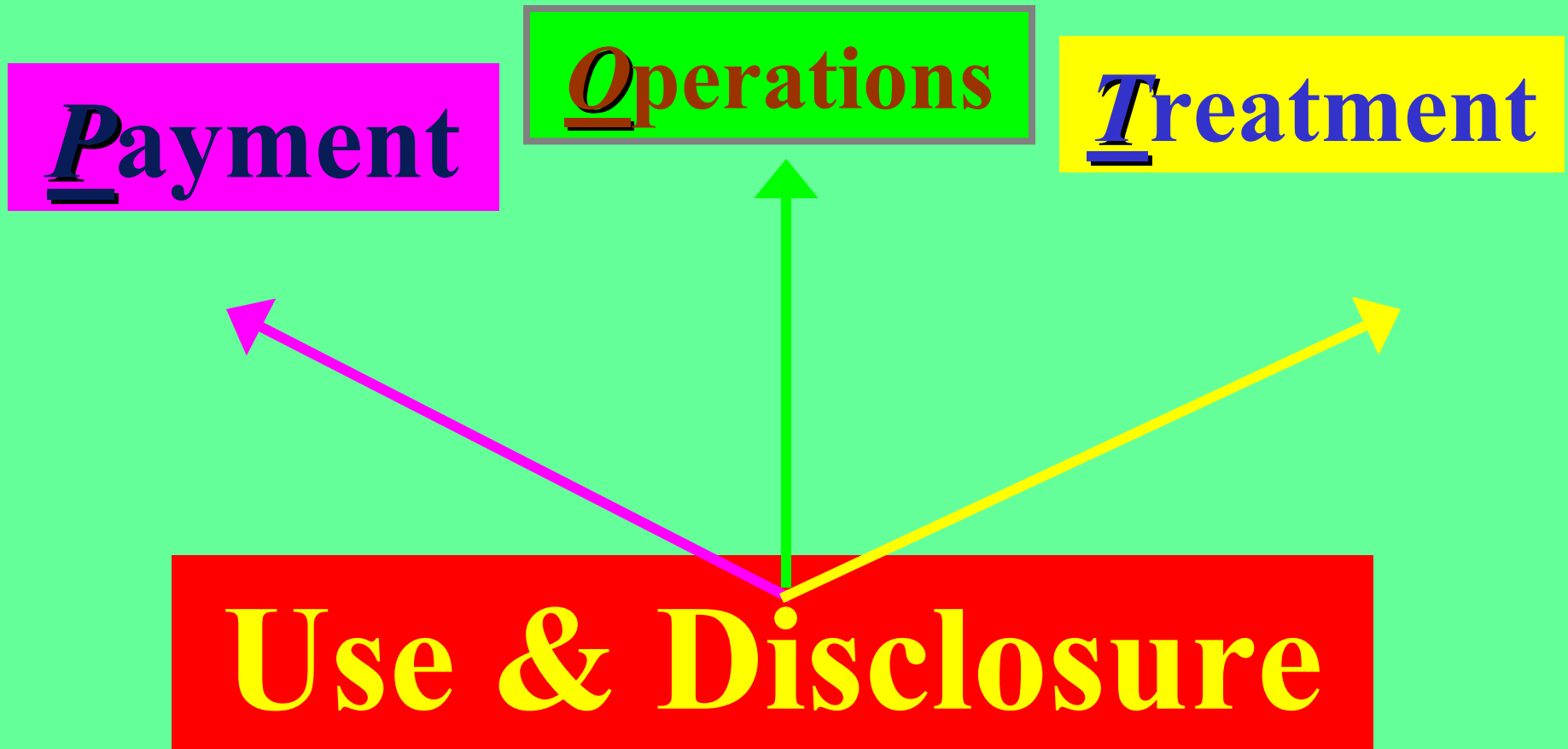
Only Two Required Disclosures

- **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**

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's the Final HIPAA Security Rule?

- **In a lockbox?**
- **In a secure location?**

First Technogarian

Privacy vs. Security

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

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**

***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 provisions**
- **Third party beneficiary**
- **Gap 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 to guard data integrity, confidentiality, & availability**

Trading Partner Agreement

- **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**

Certification/Testing

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

Administrative Simplification Compliance Act

- **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

- **\$44,200,000 appropriated, for--**
- **Technical assistance, education and outreach, & enforcement activities; &**
- **Adopting standards required to be adopted under HIPAA**

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 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**



OFFICE FOR CIVIL RIGHTS

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

HHS, Office of Inspector General

Michael Mangano, Acting Inspector General



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

Chief Privacy Official



Chief Compliance Officer



HIPAA BULL

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

Employees

Vendors

Patients

Corporate Compliance
Official

```
graph TD; CO[Corporate Compliance Official] --> E[Employees]; CO --> V[Vendors]; CO --> P[Patients];
```

Erin HIPAAvich

A Classy Action?

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!!!!!!

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 HIPAARIAN

Dial 1-800-RAT-FINK

FBI Likes HIPAA

National Association of Attorneys General

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



The Medicare,
Medicaid, and
SCHIP Agency

SEE A MESS



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**

***HIPAA: Largest Unfunded
Federal Mandate in Healthcare
\$\$\$\$\$Show Me the Money\$\$\$\$\$***

Fannie Mae

Freddie Mac

Sallie Mae

HIPAA Mae

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?**

*If you think you have
problems, talk to this guy*

Which Way Are We Going?

*What if this is
as good as it gets?*

Don't Get Behind HIPAA

BE A HIPAA HERO ^(R)



BE A HIPAA HEROINE *(sm)*



Learn the HIPAA HERO® Way

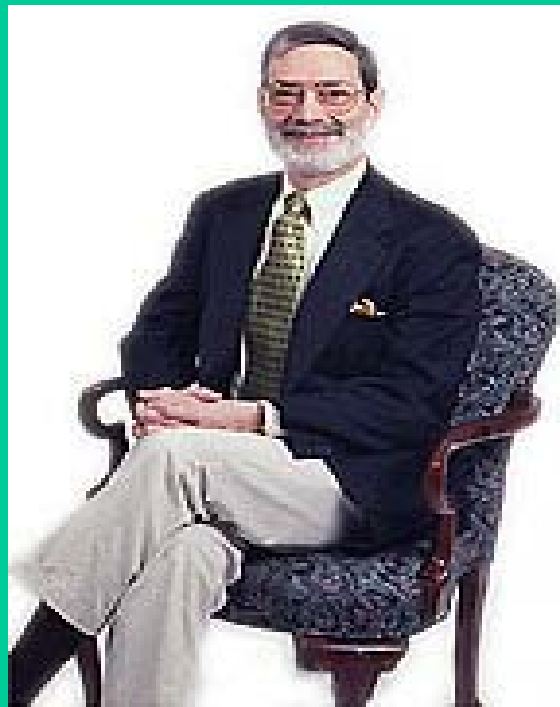


Professor Goldberg's

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 October 30, 2002.**

Why is this man smiling?
Practice Safe HIPAA!
www.healthlawyer.com



That's All Folks!

HIPAA

goulston&storrs
think*results*

Washington, DC & Boston & London, UK

Goulston & Storrs

www.healthlawyer.com

© Copyright 2002 All Rights Reserved

