

# ***Who Am I***

- **Goulston & Storrs 1967**
- **First computer Osborne**
- **Past Pres. Health Lawyers**
- **Moderator InfoTech listserv**
- **Adjunct Prof. Suffolk U. Law**

**[www.healthlawyer.com](http://www.healthlawyer.com)**

***Truth in Advertising***

***CDR Rabb JAGC***

***LT Goldberg JAGC***

***Alan S. Goldberg's***

***Honest Lawyer Privacy Policy***

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

***Healthcare Still Runs On***

***Dead Tree Media***

***HealthSouth & Oracle***

# *Hospital of Future*

- Will minimize paperwork
- Written information & medical images normally kept in big metal filing cabinets will be stored electronically and be accessible by computer

## *Say Good Bye*

*TV President Josiah Bartlet Has  
Health Care Secret In West Wing*

- H I P P A
- H I P A
- H I P P A A
- H I P A A It's Powerful  
And Awesome

*HIPAA Is About*

*Standards*

*Boston Bridge 1*

*Fire Engine 0*

***HIPAA Is About Security***  
***On internet nobody knows you're a dog***  
***Health Care & Privacy***  
***HCFA Internet Security***

- **1997 - HCFA to Internet: Drop Dead**
- **1998 - Internet Communications Security & Appropriate Use Policy**
- **An acceptable method of encryption**
- **Authentication or identification**
- **Temporary measure in anticipation of HIPAA implementation**

***Gramm-Leach-Bliley***  
***ESIGN LAW***  
**Electronic Signatures**  
**In Global & National**  
**Commerce Act**  
***European Union***  
***Directive on Data Protection***  
***Conditions of Participation***

- Resident 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

*Medicaid State Ops. Manual*

- MDS data are part of resident's clinical record
- Protected from improper disclosure
- Notice to resident

*Elevators vs. Escalators*

*If a HIPAA could talk,*

*what would a HIPAA say?*

**Aministrative Simplification Subtitle**

### ***HIPAA Applicability***

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

### ***Lost HIPAAginity***

### ***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.

## ***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 medical care

## ***Protected Health Information***

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

## ***Identifiable***

- Identifiers of patient, relatives, employers, household members
- (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

## ***Health Care Provider***

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

## ***What Is HIPAA Healthcare***

## ***Workforce***

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

## ***Business Associate***

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

# ***Business Associate Criteria***

- **What you do**

- **Not who you are**

***No HIPAA for Undertakers***

***Provider Needs Consent***

***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

## ***HIPAA NOTICE***

- “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 & Liability***

### ***Covered Entity Safeguards***

- Must have appropriate safeguards to protect privacy of protected health information
- Must reasonably safeguard information from any intentional/unintentional use/disclosure violations

### ***Security Tips***

- Delete is a lie
- Cache is not trash

- **Don't font around**
- **From: is not who**
- **To: might not be you**
- **Return: could be to all**

## *Security Tips*

- **Do you know where that floppy has been?**
- **Telephone broadcasting**
- **Phonemail messages**
- **Get your back up about backup**

## *Cookies*

- **iddb0480c4doubleclick.net/0146893875231583413233917568029322920\***
- **user\_typesubscribedwsj.com/0356700403230124358427668966429311616\*WSJIE\_LOGINihCYESCyELCaCTOwOnOdApALAYApAUDRBlBaDfDCDCDGHiw sj.com/0356700403230124358231940848029311745\***

## *Privacy:*

### *Office for Civil Rights*

- **Administer**
- **Interpret**
- **Implement**

- **Enforce**

*Office for Civil Rights*  
*Enforcer With a Heart*

## *Cooperation*

- HHS will, to extent practicable, seek cooperation of covered entities in obtaining compliance with requirements, standards, & implementation specifications

## *Here to Help You*

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

## *Format & Timing*

- Complaints to be in writing, on paper or electronic
- Identify alleged violator
- Describe acts/omissions believed to be violations
- File within 180 days (or later if good cause) of when knew or should have known occurred

## ***Must Mitigate***

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

## ***Investigations***

- HHS may investigate complaints including 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

## ***HIPAA Privacy Official***

## ***Access to Records***

- Covered entity must keep records & submit compliance reports as 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

## *Enforcement*

- HHS may seek to impose sanctions for violations
- Federal civil sanctions
- Federal criminal sanctions
- State sanctions
- Contractual sanctions
- Professional sanctions

## *HIPAA Corporate Compliance Program*

- DOJ Sentencing Guidelines
- Reduces costs & penalties

- Reduces likely enforcement
- Government strongly urges

# ***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 \$25K/year

## ***HIPAA RARIAN***

# ***BAD HIPAA***

## **VERY BAAAD HIPAA**

### ***HIPAA For Crooks***

#### **Unlawful use or disclosure of PHI**

- Under false pretenses: up to \$100K fine and/or five years in jail

- With ***intent*** to sell, transfer or use health information for commercial advantage, personal gain, or malicious harm: \$250K and/or ten years in jail

## ***National Association of Attorneys General***

### ***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”

### ***Congressional Testimony***

- HCFA lacks specially trained personnel to oversee HCFA’s & contractors’ activities
- In general, HCFA’s contractors are ***outright obstructive*** to providing sound security
- Compounding these errors was HCFA’s inability to catch or prevent them

## **But who will pay?**

*Privacy President says:*

*Use Tax Refund to Pay for HIPAA*

*The Fed Says:*

*Wait Until Rates Fall, Then Borrow*

## ***Mad Pharmacists***

- **HIPAA should not require consent from patients before pharmacists provide prescription services**
- **No state law requires pharmacies to obtain written consent from patients**

## ***Possible Changes***

- **Minimally necessary information**
- **Business associate agreements**
- **Stringency opinions**
- **Oral communications**
- **Consents**
- **External certifications**

## ***Calling Dr. Freud***



# *Which Way Are We Going? Don't Get Behind HIPAA*

## *Alan S. Goldberg's 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 June 8, 2001.

*We Practice Safe HIPAA  
Alan S. Goldberg & Steven J. Snyder*