Basic Legal Issues & Strategies in HIPAA Compliance

Alan S. Goldberg

Goulston & Storrs, Boston

The First National HIPAA Summit

October 16, 2000

www.healthlawyer.com

Who am I?

- LT US Navy JAGC: VietNam War
- Goulston & Storrs: 1967
- Piano: The Typhoons
- First computer: Osborne
- eHealth: Suffolk Univ. Law School
- Telemedicine: Emerging Issues
- Am. Bar As'n: eHealth & Privacy IG
- Past President Am. Health Lwyrs.
- Moderator: HIT listserv

Alan S. Goldberg's Privacy Policy

- **Nothing I say in this room is private**
- **Everything you say in this room is public**
- **You & I have zero privacy in this room: get over it.**
- **How's that for a simple privacy policy?**

Alan S. Goldberg's COPPA Disclaimer

- **This presentation is not for children.**
- **If you are under age 13, please go away.**
- **I do not give out cookies, Java, or milk.**
- **How's that for a simple COPPA policy?**

Law & Policy

- **Pres. Clinton ‘97 State Union:**
- **“Now we should connect every hospital to the Internet so that doctors can instantly share data about their patients with the best specialists in the field.”**
- **It depends on the meaning of “should” and “can”**

Internet Envy

- **"So far, the Internet seems to be largely amplifying the worst features of television's preoccupation with sex and violence, semi-literate chatter, shortened attention spans, and near-total subservience to commercial marketing...."**
- **The Librarian of Congress, James Billington**

The Ministry of the Spirit of HIPAA

Do we believe in privacy?

YES!

Are we all patients?

YES!

Will we take the HIPAA pledge?

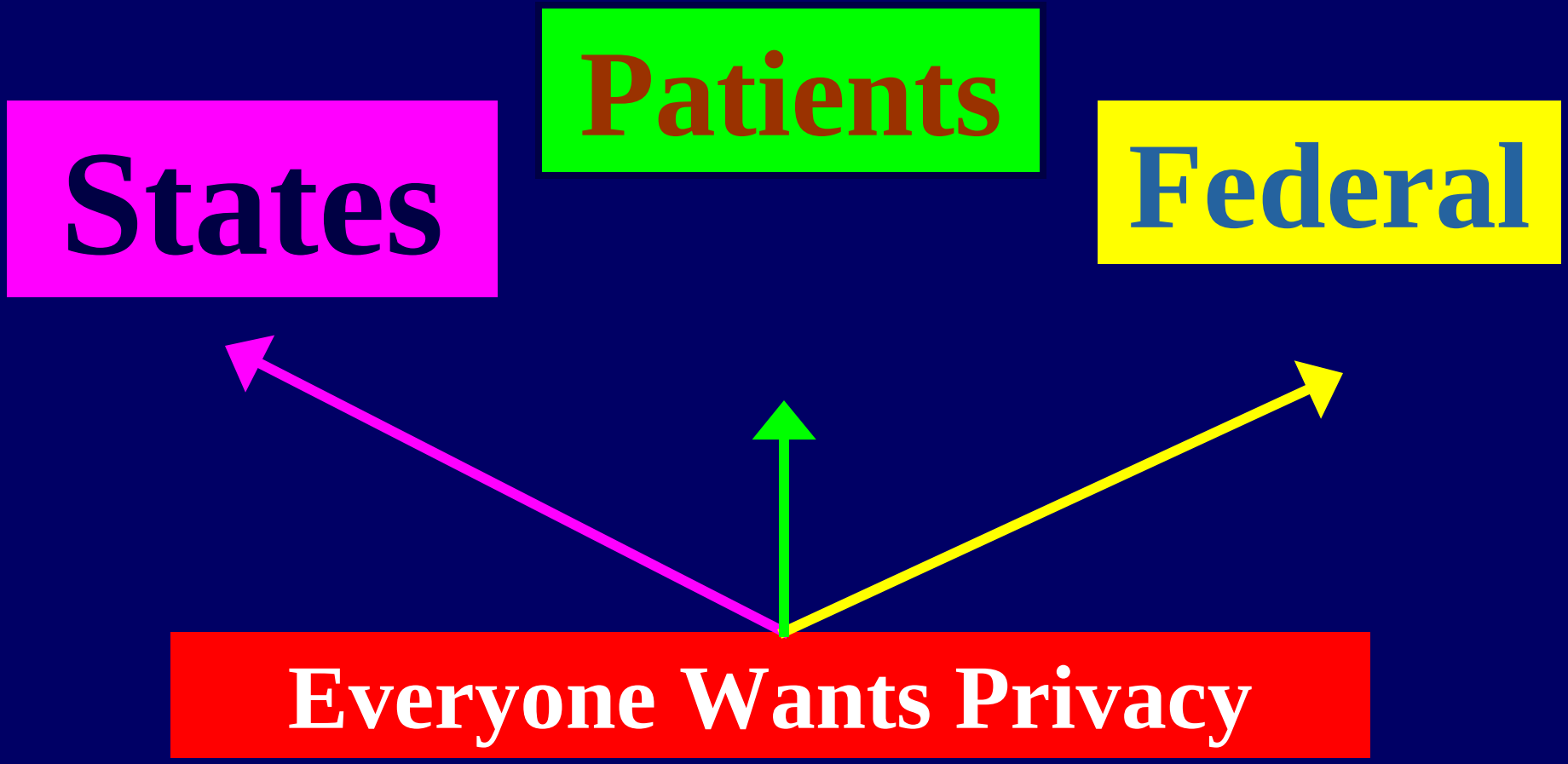
YES!

HALLELULA, PRAISE HIPAA, AMEN!

The HIPAA Pledge

“I pledge to preserve, protect, and defend the security, privacy & confidentiality of individually identifiable health information, to the best of my ability, and in furtherance of the best interests of more than 280,000,000 patients.”

But who will pay?

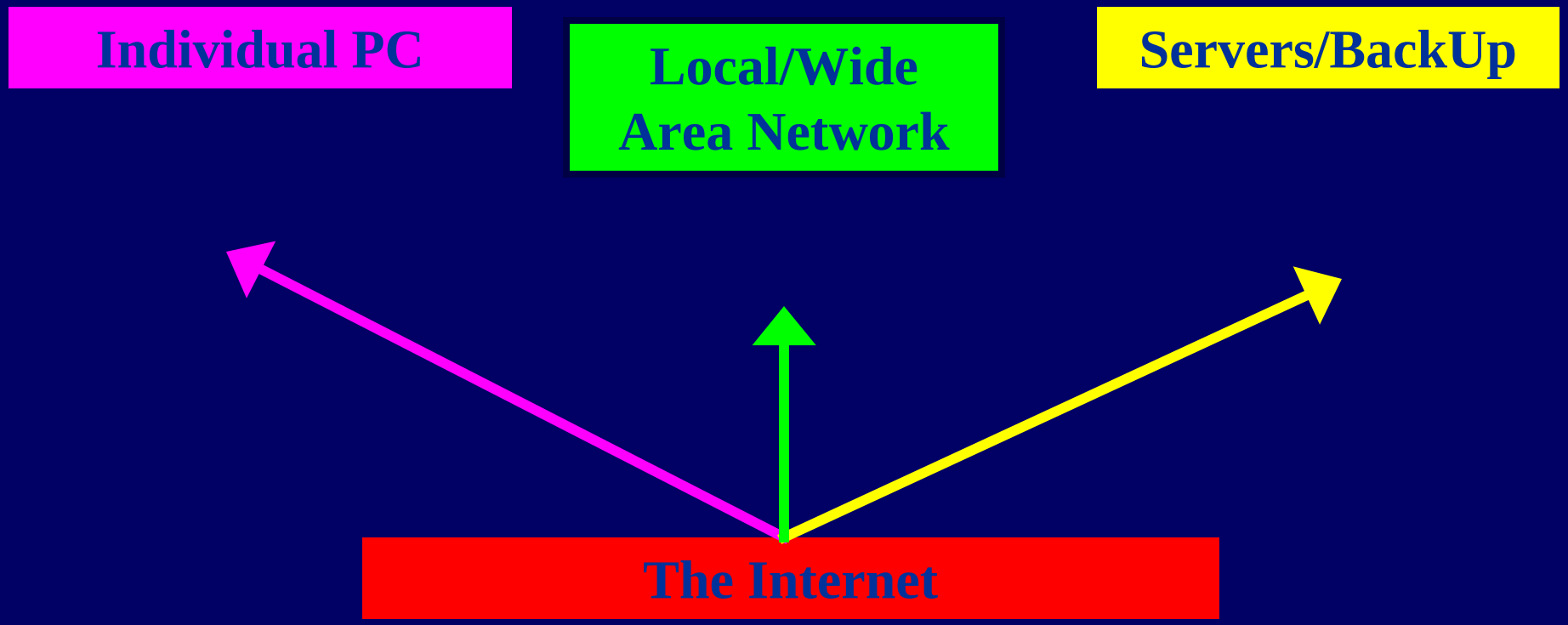


HIPAAs typically sleep during the day & maintain activity at night. HIPAAs are extremely graceful in the water, despite a clumsy appearance. HIPAAs sink to the bottom of rivers where they literally walk or run. The central core of HIPAA social groups is females with dependent offspring. Adult males vie for control of these herds. Aggression between HIPAA males is intense. Losing males are often relegated to a solitary HIPAA existence.

Confidentiality

- Technology vs. DTM (Dead Tree Media)
- Electronic medical records
- Store & forward vs. real time: back-up & purge
- Encryption, decryption & authentication
- Hospital elevators
- Internet

The Internet Is The Network



HCFA Internet Security

- **5 USC Sec. 552a "(e) Agency Requirements. - Each agency that maintains a system of records shall - (10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained...."**

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

HCFA Internet Security

- **A complete Internet communications implementation must include *adequate encryption*, employment of *authentication or identification* of communications partners, & a management scheme to incorporate *effective password/key management systems*.**
- **Acceptable *encryption* hardware & software approaches**
- **Acceptable *authentication/identification* approaches**

HIPAA Basics

- **Health Insurance Portability and Accountability Act of 1996**
- **“Administrative Simplification”**
- **Standards for electronic exchange of medical information**
- **Unique health identifiers for individuals, employers, health plans, & providers**

HIPAA Safeguards

- **Transmission of health information in electronic form**
- **Ensure integrity & confidentiality of information**
- **Protect against reasonably anticipated threats/hazards to security/integrity**
- **Prevent unauthorized use/disclosure of information**

HIPAA Applicability

- **Health plan**
- **Health care clearinghouse**
- **Health care provider**
- **Will affect all who deal with them**

Proposed HIPAA Privacy

- **Applies to protected health information**
- **Any individually identifiable health information that is or *has* been electronically transmitted or maintained by a covered entity**
- **Health plans, health care clearinghouses, health care providers, business partners (except for purposes of consultation or referral) via contracts**

Proposed HIPAA Privacy

- **Preemption**
- **Business partners**
- **Third party beneficiaries**
- **Privacy official**
- **Sanctions policy**
- **Surveys**
- **Record keeping**
- **Minimally necessary disclosure**

Cookies

- **iddb0480c4doubleclick.net/0146893875231583413233917568029322920***
- **user_typesubscribedwsj.com/0356700403230124358427668966429311616*WSJIE_LOGINihCYESCyELCaCTOwOnOdApALAYApAUDRBlBaDfDCDCDGHiwsj.com/0356700403230124358231940848029311745***

Single Security Standard

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

HIPAA Electronic Security Standards

- **AUG 12, 1998 proposed security rule**
- **Applicability**
- **Administrative**
- **Software**
- **Hardware**
- **Peopleware**

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?
- Conflicts inquiries
- Desktop views
- Phonemail messages
- Get your backup about backup

The Media Is The Message

- **Floppy disks**
- **Hard drives**
- **Cache**
- **Zip, Tape, Optical**
- **Cellular**
- **Fax**

Software Security

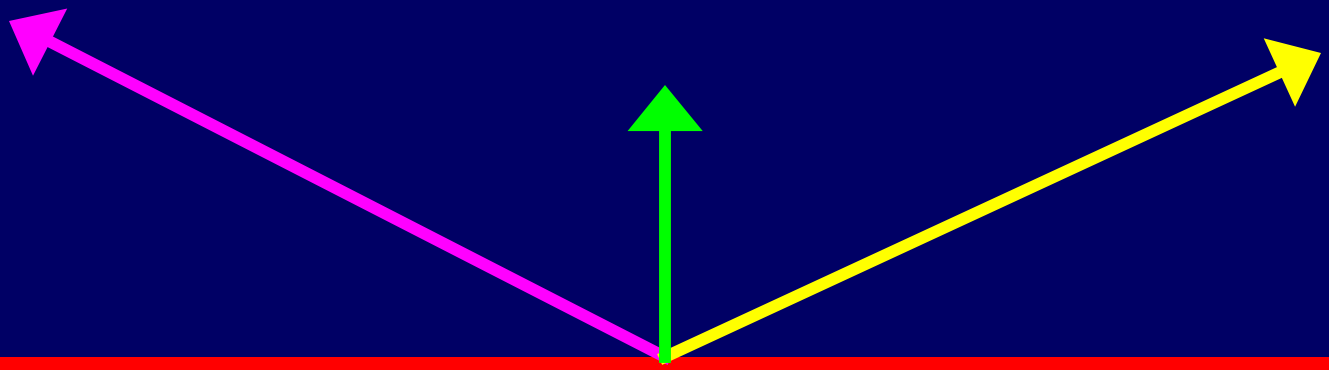
- Encryption & decryption
- eSign: electronic signature
- Authentication
- Public Key Infrastructure
- Rijndael [Rhine-doll] Data Encryption Standard
- Java & cookies & ice cream

Single Key Encryption

Encrypt Key

Same Key

Decrypt Key



Creator of eMail

Single Key Encryption

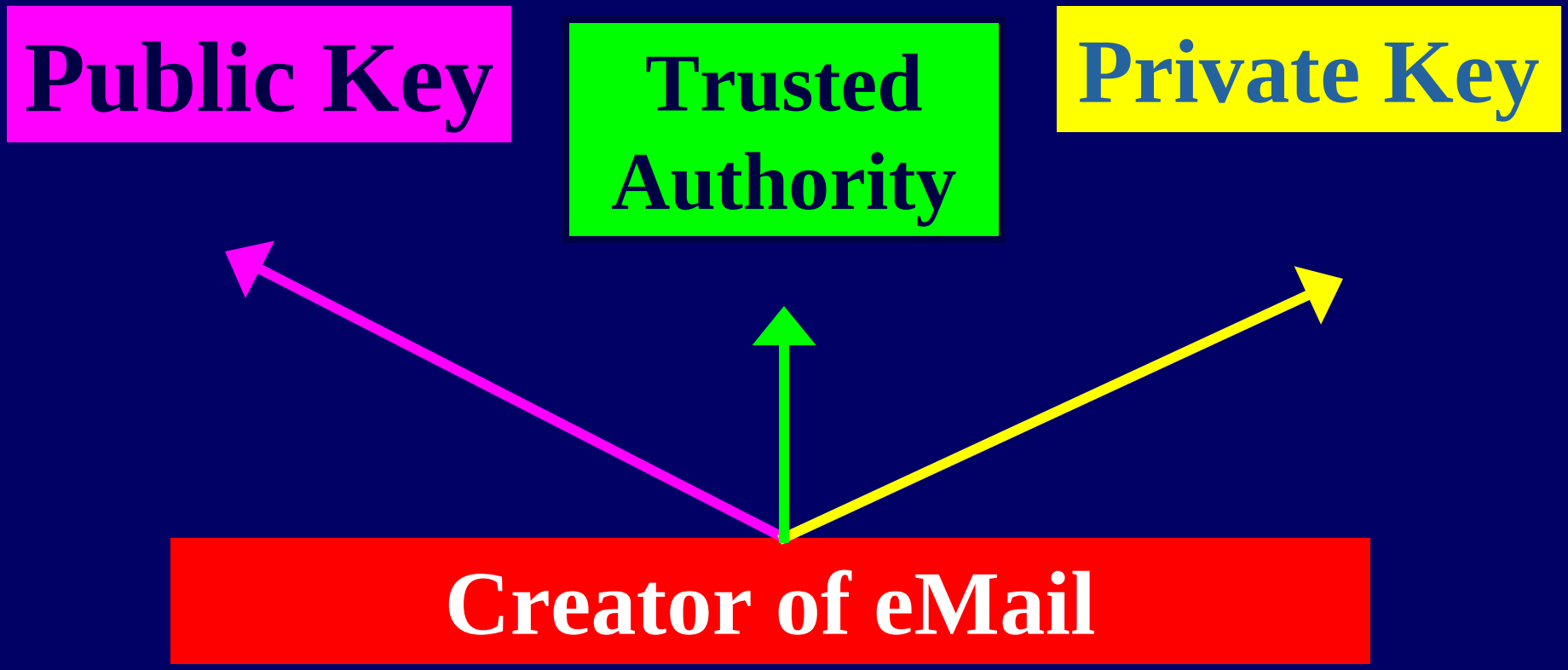
Encrypt eMail Using Single Key

Decrypt eMail Using Single Key

Result:

- **Sender must give key to Receiver**
- **Receiver must rely on Sender's key**
- **But who is the Sender**
- **And what if Sender's key is lost**

Public Key Encryption



PGP Public Key

- **-----BEGIN PGP PUBLIC KEY BLOCK-----**
  Version: PGPfreeware 6.5.8 for non-commercial use <*http://www.pgp.com*>

  mQGiBDnQduURBADbFeV4qX8oozzFS4LFq
  cx5s4zGKF+b+WghFVf3TenVHQ7MRoVl
  TFtFgjQAZtVk1ool6o9Wq7k3OezHBLdwBAi
  LZOJMF9a/O4qlbr5aDHPdYjL85bxP
  Fhm3eznJcpO50KD7kv7w72A55piQscbiWG0
  qCjvl6hTAH1D4NHULoZkL1wCg/zFs
  zWmTQaoZo9sj8Rw/93uWQSsD/1MtKhHino
  qw9zY9cq91fp8tyxtsGlDqqiCd2Xn0

Using PKI

Encrypt eMail Using Public Key

Decrypt eMail Using Private Key

Result:

- **Sender knows that only private key holder views**
- **Receiver know no one else knows but Sender**
- **But who is Sender**
- **And is Receiver really who purports so to be**

Using PKI

Encrypt eMail Using Private Key

Decrypt eMail Using Public Key

Result:

- **Sender knows that any public key holder views**
- **Receiver know no one but sender did send**
- **But is Sender who sender purports to be**
- **And is Sender's public key really Sender's**

Out Out Damn Bits

- **Delete**
- **Hide**
- **Overwrite**
- **Removing disks/drives**
- **Destroy**
- **Smash, burn and bury**

Corporate Compliance Program

- **Dept. of Justice Sentencing Guidelines**
- **Reduces Non-compliance Costs**
- **Reduces Potential Penalties**
- **Reduces Likelihood of Enforcement Action**

Penalty For Failure to Comply With Requirements & Standards

- **Not > $100 for each violation, total for violations of identical requirement or prohibition during a calendar year not > $25,000**
- **Except if *did not know*, and a person exercising *reasonable diligence* would not have known, that such person violated such provision**
- **Penalty may be waived if failure due to *reasonable cause* & not to *willful neglect***

HIPAA Wrongful Disclosure Fines & Imprisonment

- **Fine of not > $50,000 or imprisoned not > one year, or both**
- **If under false pretenses, fine not > $100,000 or imprisoned not > five years, or both**
- **If with intent to sell, transfer or use IIHI for commercial advantage, personal gain, or malicious harm, fine not > $250,000, imprisoned not > ten years, or both**

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 OCT 16, 2000.**

Be A HIPAA HERO

Words of Wisdom

- "Never make forecasts, especially about the future." Sam Goldwyn.
- "Long range planning does not deal with future decisions, but with the future of present decisions." Peter F. Drucker.
- "In the times of rapid change, learners inherit the Earth, while the learned find themselves beautifully equipped to deal with a world that no longer exists." Eric Hoffer.
- "When HIPAA is a metaphor, what will HIPAA mean?" Alan S. Goldberg.

Practice Safe Computing

- **Why is this man smiling?**

Basic Legal Issues & Strategies in HIPAA Compliance

Alan S. Goldberg

Goulston & Storrs, Boston

The First National HIPAA Summit

October 16, 2000

www.healthlawyer.com