Protecting the Confidentiality of Patient Data: Provider Perspective

Paul C. Tang, MD

Palo Alto Medical Foundation
Sutter Health

Outline

- Privacy and patient care
- Perspective on proposed privacy regulations
- Perspective on proposed security regulations
- Provider-patient electronic communication
- The HIPAA hole

Mandated Standards

- HHS Secretary must adopt standards for:
  - Electronic transactions
  - Code sets
  - Unique health identifiers
  - **Security and privacy**
  - Electronic signatures

NPRM Comments

- Transactions and codes → 17,000 comments
- Identifiers
  - Provider ID → 5,000 comments
  - Employer ID → 800 comments
- Security → 2,000 comments
- Privacy → 150,000 comments

Goals for Privacy Protection

- Patient-care decisions based on complete, accurate information
- Access to individually identifiable health information based on professional need to know
- Individually identifiable information used only for purposes under which it was acquired, unless otherwise authorized for appropriate, legal reasons
- Everyone accountable for handling confidential information properly

Privacy and Confidentiality

Penalties for Violating Patient Confidentiality *Civil and Criminal*

- Wrongful disclosure of individually identifiable health information information
  - Penalties of $50,000 to $250,000 and 1 to 10 years in jail
- Enforcement: NPRM 2001

Status of Confidentiality Legislation

- Congress was to have passed comprehensive confidentiality legislation by August 21, 1999
- Secretary issued NPRM Nov 3, 99
- Comment period closed Feb 17, 2000
- >50,000 submissions received
  - 40 reviewed in detail by GAO, including AMIA's
- Secretary hoping to issue final regs in 2000

http://aspe.os.dhhs.gov/admnsimp/nprm/pvclist.htm

Threats to Privacy

- Insider
  - Authorized access, casual (unauthorized) misuse
  - Authorized user, unauthorized “curious” access
  - Authorized user, unauthorized “for-profit” misuse
- Outsider
  - Unauthorized user (mountain climber)
  - Authorized user, unfettered use

Highlights of Privacy NPRM
Areas of Consensus

- Disclosures allowed for treatment, payment, and "health care operations"
- Patients have the right to examine and copy their records (with limited exceptions)
- Policies governing use and disclosure of confidential information should be in place
- Personal identifiers should be removed as soon as feasible, while maintaining usefulness of data
- Formal oversight should govern research use
- Health care organizations should implement security safeguards

"Health Care Operations"
Appropriateness Examples

- Allowable uses (without further authorization)
  - Quality assurance, quality management
  - Outcomes evaluation
  - Development of clinical guidelines
  - Peer review, credentialing
- Dis-allowed uses
  - Marketing; sale, rent, or barter of information
  - Sharing with non-healthcare sister division
  - Employment determinations
  - Fund raising

NPRM Issues
Electronic vs. Paper Media

- Confidentiality requirements apply to all information that was, is, or will be stored or transmitted electronically ("protected health information"); exempts paper-only documents
  - Rationale
    - Information vs. storage media
    - Close the loophole
    - But, paper-only information and fax were exempted

NPRM Issues
Electronic vs. Paper Media

- Concern
  - Information deserves protection, not the stored artifact
  - Impractical/impossible to segregate iswasorwillbe from paper-only information
- Recommendation
  - Apply regulations to all information regardless of storage media

NPRM Issues
Minimum Necessary Provision

- Only “minimal amount of information necessary” to be used and disclosed
  - Rationale
    - Professional need-to-know criteria
    - Potential for internal abuse
  - Concern
    - Challenging in a paper world
  - Recommendation
    - Encourage routine use of CPR and its security features

NPRM Issues
Business Partner Contracts

- Privacy protections should follow the data; contracts with all business partners listing patients as “third party beneficiaries”
  - Rationale
    - HIPAA-derived regs only apply to covered entities
  - Concern
    - Practicality of monitoring partners and assumed liability
    - Private right of action
  - Recommendations:
    - Pass federal legislation
    - Delete 3rd party beneficiary requirement

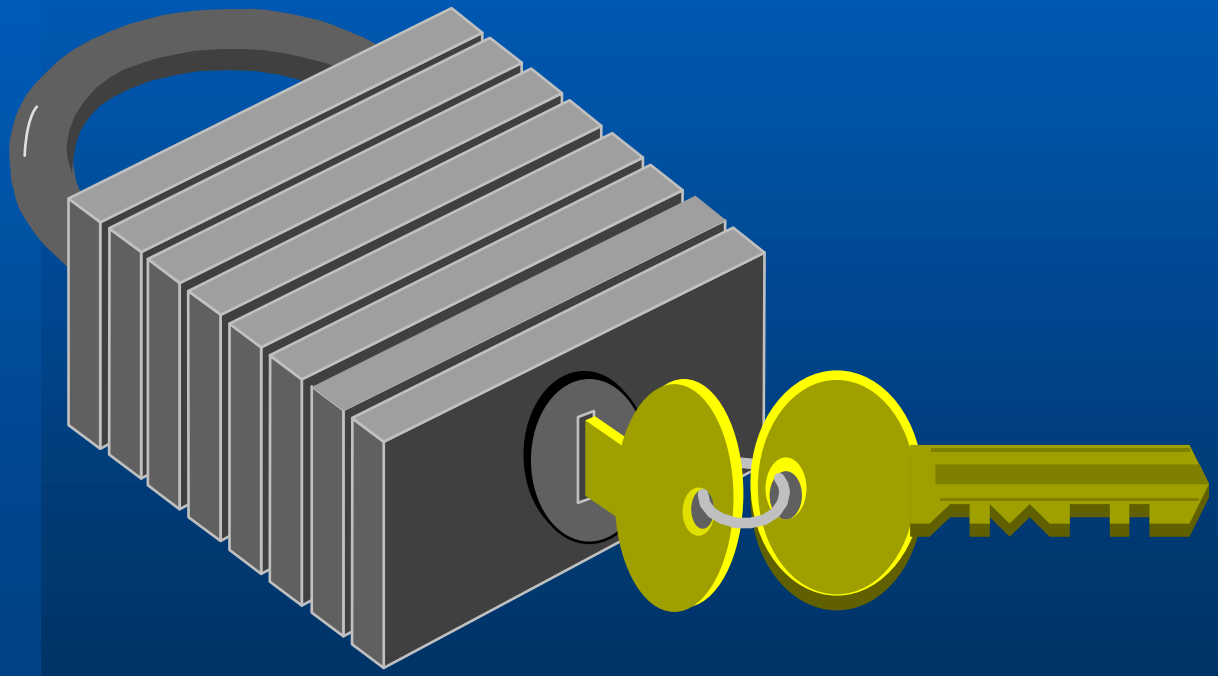
NPRM Issues
"Opting Out"

- Patients offered opportunity to further restrict access; providers do not have to comply
  - Concern
    - Perpetuate un-informed decision making
    - Impractical for restrictions to follow information
    - Potential conflict between patient and provider
  - Recommendation
    - Uniform high level protections without "opt out" provisions

NPRM Issues
Federal Preemption

- "More restrictive" state laws are not preempted
  - Concern
    - Definition of "more restrictive"
    - Inter-state nature of health care delivery
    - Complex patchwork of laws and regulations
    - May result in failure to disclose or blanket releases
  - Recommendation
    - Preemptive federal legislation

Security



Status of Security Regulations

- Secretary issued NPRM for security regulations Aug, 98
- Secretary expected to issue regulations governing system security in 2000
  - Awaiting reconciliation with privacy regs
- Applies to all electronic data – transmitted or stored

http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm

Security Standards

Controlling Access, Integrity, and Disclosure

- Policy
- Physical controls
- Software controls

Security: Policies and Procedures
Establishing Guidelines and Requirements

Topic	PAMF
Security officer	→HIM manager
Security management	→HIM Security Comm/IS/HIM
Information access policies	→HIM Security Comm/IS/HIM
User access privileges	→HIM Security Comm/IS/HIM
Annual confidentiality agreements	→Manager
Training	→EMR training/HR orient

Security: Policies and Procedures
Establishing Guidelines and Requirements

Topic	PAMF
Security incident procedures	→HIM Security Comm/IS/HIM
Termination procedures	→HR/IS
Chain of trust partner agreements	→Legal/IS
Contingency plans	→IS
Internal audit	→HIM Security Comm/IS
Certification of compliance	→HIM Security Comm/IS

Security: Physical Controls

- Restricted access to sensitive areas
  - Data center (e.g., servers)
  - Networks (e.g., routers, network closets)
  - Workstations (e.g., public areas vs. private offices)
- Media control and disposal
- Uninterruptible power supply
- Backup systems

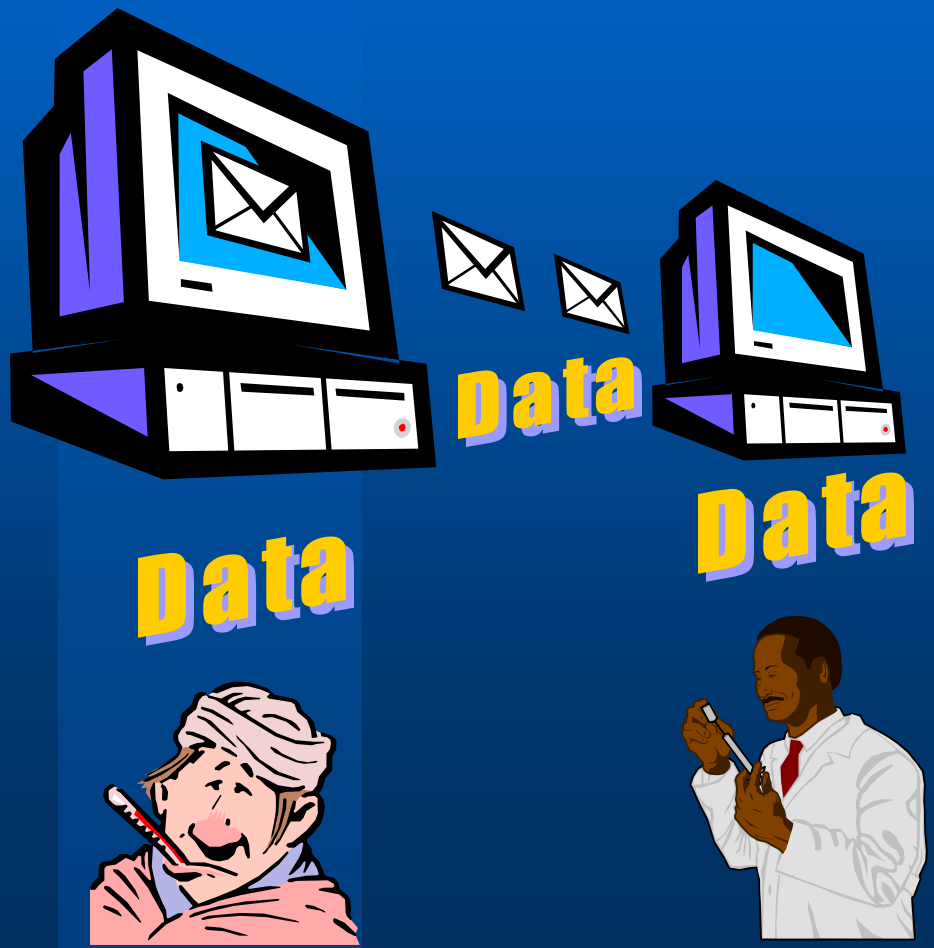
Security: Software Controls

- Authorization control (e.g., who has access)
- Authentication control (e.g., who they are)
- Password controls (e.g., expiration, nonrepeating, suspension)
- Access privileges (e.g., what can they see)
  - Role-based, user-based accesses
  - Emergency access
- Audit controls
  - Retrospective
  - Warnings (e.g., break-the-glass)
- Data integrity
- Workstation timeout
- Automatic backup
- Virus protection

A Word about Email

Electronic Patient-Physician Communication

Email



- Confidential patient data
  - Employer's PC or server
  - Internet in clear text
  - Physician's PC
- No record in chart or EMR (x "cut & paste")
- No acknowledgement of patient receipt

Some Other Issues with Email

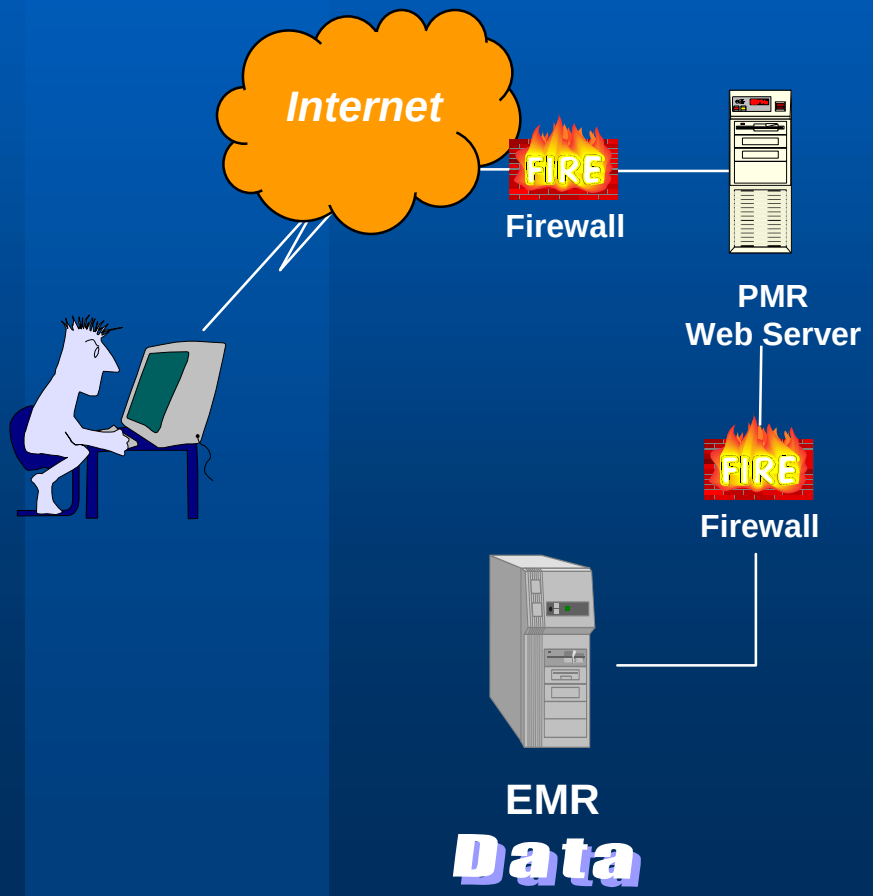
- No disclaimer prior to initiation of email
  - Caution about ‘sensitive` information
  - Notice of timeliness expectation
  - Appropriate topics for electronic communication
- Ownership of data on PCs
- Deletion policies
- Identity verification
- No triage pool function
- Lack of explicit HIPAA protection

Email Policies
Interim Practices

- Patient must agree to email policies before use (document in chart)
- Name and MRN in all email
- Appropriate topics
  - Non-urgent
  - Non-sensitive
  - Topic in subject field
- Print and file in medical record

Electronic Patient-Physician Communication

EMR-Based Communication



- Confidential patient data in EMR governed by privacy laws (and HIPAA)
- Encrypted transmission
- Cache purged
- No data stored on PCs
- Streamlined workflow
- Encounter documented in EMR

The HIPAA Hole: eHealth Sites

"There oughta be a law"

eHealth Privacy Policies
California HealthCare Foundation Study

- Study of 21 eHealth sites
- Visitors to eHealth sites not anonymous
- Many sites violate their own privacy policies
- Some sites transfer patient-identifiable information to third parties

California Health Care Foundation, 2000

Misleading Privacy Policies

- Example privacy policy:

  "The only information drkoop.com obtains about visitors to its Web site is information supplied voluntarily by visitors."

  - "Voluntarily:"
    - "Free" registration
    - Health risk assessment
  - Terms of Use: Use of cookies "relate your use of the site to information that you have `specifically and knowingly' provided to the site."

California Health Care Foundation, 2000

DoubleClick Case Study
DoubleStandard for Privacy

- Most commonly used banner ad services
- Banner ad cookies track user behavior over all web sites that use its banner ads
- DoubleClick had 100 M files on users in Jan, 2000

California Health Care Foundation, 2000

Giving Away Your Privacy
Contract with DoubleClick

"… [the web site] Company hereby grants to DoubleClick an irrevocable, perpetual, and royalty-free license to use such user data in connection with business provided…"

"…any information by which individual users …can be identified… shall not be disclosed to any third party…without written consent."

California Health Care Foundation, 2000

DoubleClick's Use of Information

Were you warned?

"…DoubleClick combines the non-personally-identifiable data collected by DoubleClick from a user's computer with the log-in name and demographic data about users collected by the Web publisher and furnished to DoubleClick…"
"DoubleClick has requested that this information be disclosed on the web site's privacy statement."

California Health Care Foundation, 2000

DoubleClick Privacy Policy

"… as described in 'Abacus Alliance' and 'Information Collected by DoubleClick's Web Sites' below, non-personally identifiable information collected by DoubleClick in the course of ad delivery *can be associated with a user's personally identifiable information* if that user has agreed to receive personally-tailored ads."

DoubleClick Privacy Policy, 9/17/00

The Pledge

OnHealth: “We will never release your name, street address, telephone number or e-mail address without your consent.”

The Transfer …to a Third Party

OnHealth's Wellness Test Done by 3rd Party

```
<form name="HRAuth" method="post"
action="http://www.wellmed.com/onhealth/connect.asp">
<input type=hidden name="Start" value="HQ"><br>
<input type=hidden name="ID"
value="896d2a210ab2012d02a184a949034a3f"><br>
<input type=hidden name="FirstName" value="John"><br>
<input type=hidden name="LastName" value="Doe"><br>
<input type=hidden name="Sex" value="male"><br>
<input type=hidden name="EMail"
value="doe@mail.net"><br>
<input type=hidden name="BirthDate"
value="11/12/57"><br>
</form>
```

California Health Care Foundation, 2000

Federal Legislation Needed

- HIPAA limits scope of regulations:
  - Covered entities (provider, plan, clearinghouse)
  - Electronically transmitted
- Reuse and redisclosure not covered for non-covered entities
- eHealth sites were not included in HIPAA
- Preemption of state laws needed to establish uniform protection

Organizing for HIPAA Implementation

Getting Started

It’s here; we need to deal with it.

Preparation Steps
Organize, Educate, Assess Preparedness

- Organize coordinated approach
  - HIPAA compliance steering committee (e.g., Executive admin, security officer, CMO, CIO, HIM dir, legal, HR)
    - Work groups (e.g., HIM, IT, policies, training)
- Educate Board and senior management
- Allocate budget and time
- Monitor laws, regulations, standards
- Assess preparedness
  - Policies, confidentiality forms, contracts
  - Procedures
  - IT system compliance, including source data systems

Execution Steps
Update, Upgrade, Train

- Update policies, procedures, business contracts
- Upgrade information systems and processes
- Communication and training
- Models like:
  - Corporate compliance (policies and training)
  - Y2K (IT and $$)
  - JACHO (fear and widespread impact, and accreditation)
  - All of the above!

Summary
Do No Harm to Patient Data

- Patients first: balance goals of care with protection of information
- Compliance and implementation starts at the top
- Establish policies and user accountabilities
- Review system security features and procedures
- Implement security functionality as needed
- Communicate, educate, and set clear examples
- Federal legislation essential to adequate protection of information

Contact Information:

Paul C. Tang, MD
Chief Medical Information Officer
Palo Alto Medical Foundation
tangp@pamf.org