# HIPAA Privacy:
## Separating Common Sense from Myth

Paul C. Tang, MD
*Palo Alto Medical Foundation*
*Sutter Health*

## Outline

- The case for patient care
- Key provisions and implications of privacy rule
  - Patient rights
  - Provider responsibilities
- The HIPAA hole

## The Case for Patient Care
*Common Sense*

- Patient-care decisions based on complete, accurate information; requires patient trust
- 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

## HIPAA Mandated Standards

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

## Privacy

Privacy is the individual's right to keep certain information to him or herself, with the understanding that the information will only be used or disclosed with his or her permission, or as permitted by law

## Confidentiality

Confidentiality is the practice of permitting only certain authorized individuals to access information, with the understanding that they will only disclose it to other authorized individuals who have a need to know

## Provider Definitions

- Direct treatment relationship – direct relationship between provider and individual
- Indirect treatment relationship – provide care under orders of another provider (e.g., radiologist, pathologist)
- Use – employment, application, utilization, examination, or analysis of information within entity
- Disclosure – release, transfer, provision of access to, divulging of information outside of entity (including disclosure to business associate)

## Protected Health Information

*Individually Identifiable Health Information*

- "All individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity." Includes:
  - Electronic records
  - Paper records
  - Oral communication
    - NYDHT:
      - Build soundproof private rooms
    - YYC:
      - Call patient names in waiting rooms
      - Use sign-in sheets

## Designated Record Set
*Covered Records*

- "…records maintained by or for a covered entity that are always part of a covered entity's designated record sets and to include other records that are used to make decisions about individuals."
- Provider: medical record and billing record (including those held by business associate)
- Does not include oral communication or QA recordings
  - NYDHT: record and transcribe all oral utterances

## Individual Access to PHI
*Providing Access*

- Rights to summary and/or underlying information
- Provide in format requested (e.g., electronic), if readily producible
- Act within 30 days (60 days if off-site)
- Fees for labor and supply (e.g., paper or disk) for copying or summarizing, but not retrieving and handling information
- Fees for explanation OK

## Individual Access to PHI
### *Grounds for Denial*

- Grounds for denial of access:
  - Physical harm to self or other (reviewable)
  - About another and likely cause harm to the other (reviewable)
  - Obtained under promise of confidentiality to another
  - Obtained in course of clinical trial
- Denial may be reviewed by licensed professional

## Right to Request Amendment
### *To the Medical Record*

- If agree, must act on request within 60 days, and:
  - Notify persons identified by individual who received PHI
  - Notify persons known to have relied on unamended information to detriment of individual
- May decline amendment if:
  - Did not create information
  - Information is accurate and complete
  - Not part of a designated record
- If denied, must inform individual of right to disagree, complain to Secretary, and include request/denial with future disclosures

## Consent Requirements
### *Use and Disclosure of PHI*

- Health care providers with direct treatment relationship must obtain consent to use or disclose PHI for treatment, payment, or "health care operations"
- Valid indefinitely unless revoked
- Providers may condition treatment on consent
- Must refer to separate notice of privacy practices
- Consent not required for providers with indirect treatment relationship

## Consent Requirements, II
### *Use and Disclosure of PHI*

- Must inform individual of right to restrict use and disclosure, and that covered entity does not have to agree. However, agreement is binding.
- Conflicting agreements yield to more restrictive permission
- Revocable at any time, but covered for acts in reliance on prior consent
- May be brief (less than 1 page)
- YYC: have friend or family pick up prescription
- Anticipated changes to rule:
  - Pharmacists may fill phoned-in prescriptions
  - Referred patients may be scheduled for visit, surgery, procedures

## Exceptions to Consent and Authorizations
*Parents and Minors*

- Person's right to control PHI is based on right to control health care
  - State laws apply
  - Generally parent is a personal representative of children
  - When state law does not require parental consent for treatment (e.g., bcp), parent is not the personal representative for child and may not access PHI without permission

## "Health Care Operations"
*Allowable Examples*

- Quality assurance, quality management
- Quality improvement (if purpose is not creation of generalizable knowledge)
- Population-based activities
  - Development of clinical guidelines
  - Disease management
- Peer review, credentialing
- Preparing legal proceedings
- Business planning (e.g., formulary development)
- Business management (e.g., fundraising)

## "Health Care Operations"
### *Allowable "Marketing"*

- Covered entity describing services or products (incl, 3rd party) face-to-face
- Treatment-related communication (tailored by PHI)
- Providing products or services of nominal value (e.g., pens)
- Promote products and services (incl 3rd party) if:
  - Identify covered entity
  - Explain why individual targeted and how benefit health
  - Disclose any direct or indirect remuneration
  - Describe how to opt out (except for general communication)

## "Health Care Operations"
### *Fundraising*

- Fundraising for self
  - Limited information: demographics and dates of service
  - Must describe how to opt out of future communications
  - May disclose to business associate and institutionally related foundation

## "Health Care Operations"
*Dis-allowed Examples*

- Marketing, other than for self
- Sale, rent, or barter of information
- Sharing with non-healthcare sister division
- Employment determinations
- Fund raising other than for own purposes

## Notice of Privacy Practices
*Uses and Disclosures*

- Describe all uses and disclosures permitted by law
  - With at least one example
  - If plan to use PHI, must disclose:
    - Providing appointment reminders
    - Describing treatment alternatives
    - Providing information about benefits and services
    - Soliciting funds
- All other uses and disclosures require revocable authorization

## Notice of Privacy Practices
*NYDHT*

- Wait for the patient to read the notice first
- Explain each item to the patient before the patient signs
- Verify the signature on the consent form if patient not present when he/she signs it

## Authorizations
*Use and Disclosure of PHI*

- Required for all uses or disclosures not otherwise permitted for treatment, payment or health care ops
- Required for psychotherapy notes
- Required to access the medical record of another covered entity (ie., Release of Information)
- May not condition treatment on signing
- Revocable

## Authorizations
*Core Elements Required*

- Name of entity authorized to use or disclose
- Description of information
- Name or types of recipients
- Statement of financial remuneration, if applicable
- Expiration date or event
- Signatures
- Notice of right to revoke in writing

## Accounting of Disclosures

- Right to accounting of disclosures for preceding 6 years by covered entity or its business associates for purposes other than treatment, payment, or health care operations (60 days to fulfill request)
- Accounting includes:
  - Date, name/address
  - Description of information
  - Purpose (unless requested by individual)
  - Summary of recurrent disclosures permitted
- One free accounting per 12 months

## Minimum Necessary Provision
### *Implementing "Need-to-Know"*

- Must establish policies and procedures for routine uses and disclosures and make reasonable efforts to:
  - Restrict access and use based on role
  - Limit disclosures to what is reasonably necessary for intended purpose
  - YYC use: sign-up sheets, X-ray lightboards, bedside charts
- Must develop criteria for non-routine disclosure
- Disclosures to individuals and to providers for treatment are exempt from minimum necessary rule (YYC!)
- Request for entire record without documented justification violates rule
- NYDHT:
  - Purchase new computer systems
  - Redesign facility office space

## Business Associates
### *Extend Privacy Policies*

- Privacy protections should follow the data; contracts required for all business associates
  - Definition:
    - Business association occurs when PHI is used or disclosed by a 3rd party acting on behalf of the covered entity or rendering service to or for a covered entity
  - Accountability:
    - Actions relating to PHI undertaken by business associate considered to be actions of the covered entity
    - Sanctions applied only if covered entity had knowledge of wrongful activity and failed to take required action

## Business Associates
*Examples*

- Business associate examples: legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, financial services
- Non-business associate examples: covered entity members of an "organized health care arrangement" (e.g., hospital and medical staff, IPA), medical staff member (e.g., unless hospital provides billing services to physician), ISP, postal service, financial institution

## Business Associates
*Responsibilities of Covered Entities*

- Must have contractual "satisfactory assurances" from business associate that information will be protected
- Must investigate complaints and either cure a breach or terminate contract
  - If not feasible to terminate, must report to Secretary
- Not required to monitor compliance

## Research Uses and Disclosures

- All research covered regardless of funding
- Privacy review by IRB or privacy board for waivers
  - Minimal privacy risk
  - Waiver not adversely affect privacy rights and welfare of subjects
  - Research not practically conducted without waiver
  - Research not practically conducted without PHI
  - Research importance outweighs privacy risk
  - Adequate plan to destroy the identifiers as soon as possible (unless health or research justification)

## Use of Aggregate De-identified Data *Methods*

- Apply generally accepted statistical and scientific principles to render information not identifiable
  - Document analysis and results
- Safe harbor method

## De-Identifying Data

*Safe Harbor List of Identifiers to Remove*

- Name
- Address (except 3-digit zip unless <20K people)
- All dates (except year) and aggregate 90+ year olds
- Telephone numbers
- Fax numbers
- Email addresses
- Social security number
- Medical record number
- Health plan number
- Account numbers
- Certificate/license numbers
- Vehicle numbers
- Device identifiers
- URLs
- IP addresses
- Biometric identifiers
- Full-face photos
- Any other unique identifying number, characteristic, or code

## Administrative Requirements

- Designate privacy official
- Train all workforce by compliance date
- Safeguard PHI from inappropriate use or disclosure
- Provide internal complaint process and sanctions
- Mitigate harmful effects of violations

## Federal Preemption of State Laws
*Floor*

- "More stringent" state laws are not preempted
  - Concern
    - Definition of "more stringent"
    - 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

## Penalties for Violating Patient Confidentiality
*Civil and Criminal*

- Wrongful disclosure of individually identifiable health information information
  - Civil: $100/person/violation, max $25K/person/standard/yr
  - Penalties of $50,000 to $250,000 and 1 to 10 years in jail
- Enforcement: NPRM 2002
- Responsibility of HHS Office for Civil Rights

# The HIPAA Hole: eHealth Sites

## 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

## DoubleClick DoubleStandard
*Case Study*

- 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

## 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
- Communicate, educate, and set clear examples
- Apply common sense and reasonableness test