Second National HIPAA Summit
Overview and Compliance to Final Privacy Regulations

Tom Hanks

Practice Director, Enterprise Security

1-800-4-BEACON

tom.hanks@beaconpartners.com

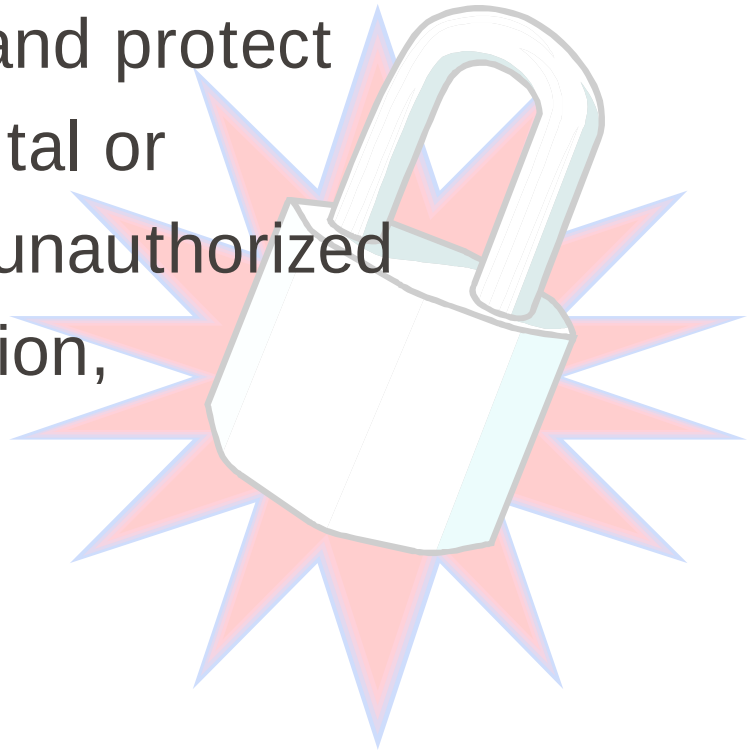
www.beaconpartners.com

HIPAA Regulations

- Two years + 60 days from pub date
- Formats & codes - final 8/17/00
- Identifiers – 1Q-3Q 2001 (except patient)
- Security – 1Q-2Q 2001
- Privacy – final 12/28/00

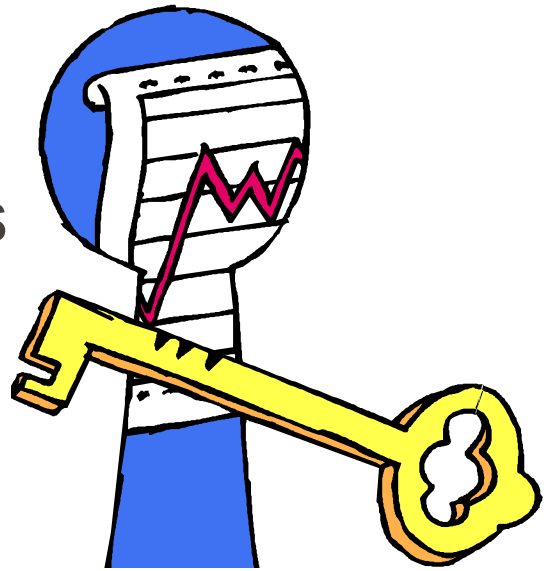
Security vs. Privacy... Definitions

- Security
  - ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss



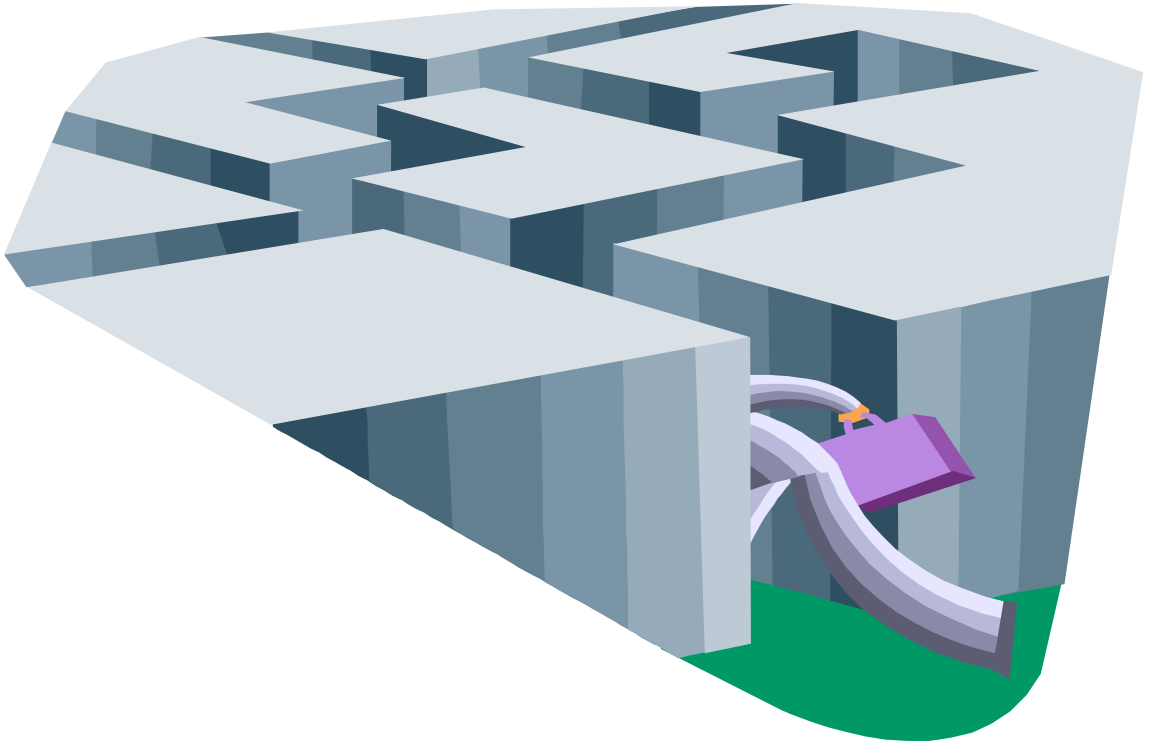
Security vs. Privacy... Definitions

- Privacy
  - defines who is authorized to access information (the right of individuals to keep information about themselves from being disclosed)



HIPAA Privacy Regulations

- Lots of twists & turns



Privacy Rule
Law & Enforcement

- No preemption of state law
  - Privacy rule establishes a regulatory floor
  - state law that is contrary & provides more protection retains primacy

Privacy Rule
Law & Enforcement

- Enforcement provisions
  - enforcement NPRM in 2001
  - Office of Civil Rights to enforce
  - covered entities provide compliant process
  - any person may complain to DHHS
  - whistleblower provision
  - does not apply to workforce

Privacy Rule
Law & Enforcement

- Civil penalties - $25,000 per incident – could add up to significant dollars
- Enforcement by Office of Civil Rights could be embarrassing

Privacy Rule
Law & Enforcement

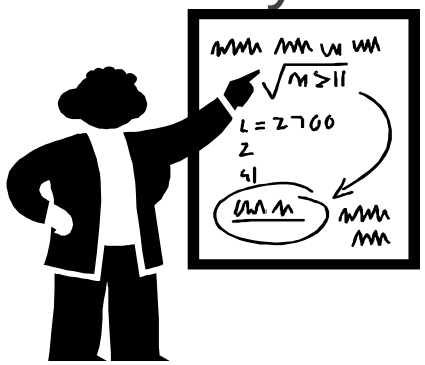
- And... significant penalties associated with non-compliance
- Criminal penalties
  - 1 - 10 years
  - $50,000 - $250,000 fines

DHHS Privacy Regulations

- Boundaries
- Security
- Consumer control
- Public responsibility
- Administrative

Boundaries–What's Covered
Protected Health Information

- Protected Health Information
  - ☞ all individually identifiable health information in ANY form or media
- De-identified data defined by removing list of elements
- Statistical determination that the risk of re-identification is very small



Boundaries–Who's Covered
Covered Entities

- Health care providers that transmit covered transactions
- Health plans
  - generally any individual or group health plan that provides or pays for the cost of medical care (TPA not a health plan)
- Clearinghouses
  - receives or produces non-standard data or format

Boundaries–Who's Covered
Entity Variations

- Multi-function
  - multiple covered entity components
- Hybrid Entities
  - health care and non-health care components
- Affiliated Entities
  - single control or ownership (5%)
- Organized Health Care Arrangement
  - expect that activities are integrated

Boundaries–Who's Covered
Business Associates (BA)

- Business Associate Contract (BAC) required with any entity that performs services to, or on behalf of, a covered entity that uses or discloses PHI belonging to the covered entity
- Relationship of the entities governs applicability
  - ☞ covered may also be BA to another covered entity

Boundaries–Who's Covered BAC Exceptions

- Disclosures for purpose of treatment
- Financial institutions processing credit cards, checks, funds transfers
- Group health plans with plan sponsors
- Certain jointly administered government programs
- Conduits are not BA's – ISP & phone
- Participation in joint activities

Boundaries–Who's Covered BAC Enforcement

- Direct knowledge of material violation
- Take reasonable steps to cure
- If no cure – then requires termination, except when termination is not feasible
  - no other viable alternatives to the BA
  - cost or convenience are not determining factors

Boundaries–Who's Covered
Business Associates (BA)

- BAC are required for:
  - legal, actuarial, accounting, consulting, management, accreditation, data aggregation, financial services
- BAC not required for:
  - employees (workforce), including some contractors, are not BA's
  - staff physicians not usually BA's to hospitals

Boundaries–Who's Covered BAC Overview

- Laundry list of terms, including:
  - HHS right to audit, use appropriate safeguards, ensure vendors comply, termination for violation, only disclose per BAC, BA may provide access & amendment

Security – Protection of PHI
Safeguards

- Not required to guarantee the safety of PHI against all threats
- Theft of PHI may not be a violation if reasonable policies in place
- Appropriate administrative, technical and physical safeguards to protect the privacy of PHI

Security – Protection of PHI
Safeguards

- Reasonably required to protect from intentional or unintentional violation
- No proscribed implementation
- Vary according to size and type of entity

Security – Protection of PHI
Safeguards

- Privacy rule gives us a peek at potential final security provisions
  - audit trails anticipated for alterations
- Minimum disclosure
- Role based access

Consumer Control
Controlling Disclosures

- “Use” defined as internal use by a covered entity
- “Disclosure” defined as release, access or transfer of PHI outside the entity

Consumer Control
Controlling Definitions

- Treatment
- Payment
- Health care operations

Consumer Control
Treatment

- Provision, coordination or management of health care and related services by health care providers – including with a third party, consultation and referral
  - health care providers only

Consumer Control Payment

- Health plan
  - any activity undertaken by a health plan to obtain premiums or coverage
- Provider
  - any activity undertaken to obtain reimbursement for health care

Consumer Control
Health Care Operations

- Quality assessment & improvement – not generalized
- Reviewing competence, qualifications or performance
- Underwriting, premium rating, etc.
- Medical review, legal services, auditing, fraud and abuse, and compliance

Consumer Control
Health Care Operations

- Business planning and development
- Business management and general administrative functions

Consumer Control
Minimum Disclosure Provision

- Except for treatment, payment and health care operations...
  - disclosure of any patient information is limited to the minimum amount necessary to accomplish the purpose of the disclosure
  - internal & external

Consumer Control
Controlling Disclosures

Three Tiered Approach

- Provide notice of privacy practices
- Seek permission to use or disclose PHI – lots of exceptions
- Right of individual to access, copy and amend their medical record

Consumer Control
Notice of Privacy Practices

- Notice to individuals must inform them of their rights, disclose privacy practices, and procedur for patients to obtain access and amend their information

Consumer Control
Notice of Privacy Practices

- Different notices for different states
- General explanation of privacy practices
- Written in plain language
- Specific header wording
- State all the uses and disclosures
- Right to revoke & process for revocation
- Entities requirements under law

Consumer Control
Notice requirements

- Separate statements required & opt out provision
  - providing appointment reminder, treatment alternatives or other related benefits & services
  - fund raising for the covered entity
  - Group health plan may disclose PHI to the employer (plan sponsor)

Consumer Control
Notice requirements

- Statement of individual rights
- Notice should contain reservation of right to revise
- Complaint process to entity & HHS
- Effective date not earlier than pub
- Joint notices

Consumer Control
Permission to Disclose

- Consent required for treatment, payment and health care operations
- Individual given opportunity to agree or object to informal disclosures
- Authorization required for all other purposes except public protection

Consumer Control
Consent

- Providers delivering direct treatment must obtain consent
- Providers delivering in-direct treatment are not required to obtain consent
- Optional for health plans & clearinghouses

Consumer Control
Consent Requirements

- Must refer to notice
- Right to review notice prior to signing
- State that notice may be revised (if notice reserves such right)
- May be combined with other forms of legal permission
  - ☞ visually and organizationally separate with separate signatures and dates

Consumer Control
Consent Requirements

- State the uses and disclosures
- Cannot combine with authorization
- State right to request restrictions and entity's right to refuse request
- Any element missing – not valid
- Valid until revoked in writing

Consumer Control
Right to Agree or Object

- Anticipates informal settings where agreements are made orally, without written authorization

Consumer Control
Specifics of Agree or Object

- Facility directories
- Disclosure to clergy
- Disclosures to persons involved in the individual's care
- Notification of relatives
- Agreement to disclosure does not persist

Consumer Control
Authorization

- For every other use or disclosure of PHI except those exceptions – e.g. public responsibility
- Including internal use not for treatment, payment or health care operations

Consumer Control
Authorization Requirements

- Provider must state treatment not conditioned on authorization
- Description for each purpose for use or disclosure of PHI
- Health plan must state eligibility or enrollment not conditioned, except...

Consumer Control
Authorization Requirements

- Individual may revoke in writing at any time
- Identify the name or class of persons to whom PHI will be disclosed
- Contain an expiration date or event which must be related to the purpose
- If applicable, disclose that the covered entity receives remuneration

Consumer Control
Authorization - Marketing

- Defined as a communication about a product or service to encourage recipients to purchase or use the product or service
- Authorization must be obtained for any marketing activities, except...

Consumer Control
Authorization - Marketing

- Any activity related to treatment, payment or health care operations
- Provider for the purpose of furthering treatment
  - discussion of providers or others products or services
  - prescribe, recommend or sell products and services as part of treatment

Consumer Control
Authorization - Marketing

- referrals, prescriptions, communications that describe how a product or service may relate to the health of the individual

Consumer Control
Authorization - Marketing

- Health plan or provider communications, tailored to an individual, made in the course of managing treatment
  - recommending alternative treatments, therapies, providers or settings of care

Consumer Control
Auth. – Psychotherapy Notes

- Health plans may not request for determination of benefits, underwriting, issuing insurance or payment of claims
- May not be combined with any other authorization or consent

Consumer Control
Right to Request Restrictions

- Individual can request from any covered entity, except a covered entity operating under a BAC, specific restrictions on use or disclosure
- Covered entity has right to refuse

Consumer Control
Right to Request Restrictions

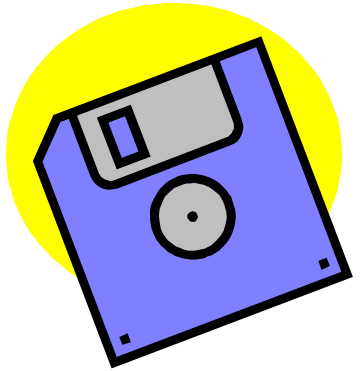
- Individual can request covered entities to provide confidential communications
  - sealed envelopes – no postcards
  - phone individual at a designated phone number
  - send mail to designated address – e.g. mail EOB to an address other than the members

Consumer Control
Right of Access / Amendment

- Right to access and request amendment of any PHI maintained in their designated record set
  - PHI maintained by the covered entity or their BA and used to make a decision on that individual

Consumer Control
Right of Access / Amendment

- If able, must provide information in the format requested
- Must respond within 60 days
  - one time extension of 30 days
- Could provide summary if individual agrees



Consumer Control
Right of Access

- Reasonable charge for copying
  - does not include retrieval
  - supercede state law that provides retrieval fee

Consumer Control
Right of Access - Exceptions

- Psychotherapy notes
- Information compiled for use in civil, criminal or administrative actions
- Certain PHI maintained by entities subject to or exempted from CLIA
- Copying for inmates – access ok
- Endanger life or physical safety

Consumer Control
Right of Amendment - Denial

- If the entity did not create the information
  - ☞ if the creator is no longer available then entity must address the request
- If the PHI is not part of the designated record set
- If the information is accurate and complete

Consumer Control
Right to Access - Denial

- Denial in writing
- Included the basis of denial
- How the individual may file a written statement disagreeing
- How to file a complaint with the entity and HHS

Consumer Control
Right of Amendment - Denial

- Individual may request that the request for amendment and the denial be included with any future disclosures
- In the event of written disagreement, entity must identify the record and append or link...

Consumer Control
Right of Amendment - Accept

- Identify the affected records in the designated record set and append or link to the location of the amendment
- Obtain authorization to share
- Provide copy of the amendments
  - persons the individual names
  - persons, including BAs that relied on the information
- Same issues for receipt

Consumer Control
Right of Accounting

- Right to request and receive accounting of any disclosures made for purposes other than treatment, payment and health care operations
  - respond within 60 days – one time 30 day extension
  - free accounting every 12 months

Consumer Control
Accounting - Requirements

- Date of each disclosure
- Name and address, if known, of person or entity receiving the PHI
- Brief description of information disclosed
- Purpose for disclosure or copy of individual's authorization
- May summarize

Consumer Control
Accounting - Exceptions

- Facility directories
- Persons involved in the individual's care
- Allowed in the right to object or agree
- National security or intelligence
- Correctional institutions or law enforcement
- Made prior to Privacy rule compliance date

Public Responsibility

Use & Disclosures

- Covered entities are not required to obtain any form of individual permission for disclosures
- Laundry list of exceptions & exceptions to exceptions

Public Responsibility
Use & Disclosures

- Mandated by law
- Public health activities
- Workman's compensation
- Law enforcement
- Research controlled by IRB
- Serious threat to health and safety
- National security

Administrative Requirements

- Privacy officer and privacy contact person
- Policies and procedures
  - reasonably designed and developed to comply with rule - taking into account size and nature of the activities

Administrative Requirements

- Provide training to workforce
- Sanctions – measure compliance
- Complaint process
  - whistleblower
- Policy and procedures to mitigate
  - includes workforce and BA

Resources

- HIPAA Comply web site
  - www.HIPAAcomply.com
- WEDI web site
  - www.wedi.org
- AFEHCT web site
  - www.afehct.org
- EHNAC web site
  - www.ehnac.org

Resources

- DHHS Administrative Simplification
  - aspe.dhhs.gov/admnsimp/index.htm
- DHHS Data Council Web Site
  - aspe.dhhs.gov/datacncl/
- NCVHS Web Site
  - ncvhs.hhs.gov

Thank you!

Tom Hanks

Practice Director, Enterprise Security

1-800-4-BEACON

tom.hanks@beaconpartners.com

www.beaconpartners.com