goulston&storrs
thinkresults

Alan S. Goldberg, JD, LLM

Third National HIPAA Summit

Basic HIPAA for the Rest of Us

www.healthlawyer.com

Who Am I

- **Rt. Rev of Ministry Spirit of HIPAA**
- **Massachusetts bar, 1967**
- **Florida bar, 1984**
- **DC bar, sooner rather than later**
- **Past Pres. American Health Lawyers**
- **American Bar Association e-Health**
- **Adjunct Professor of Law**

  Suffolk University Law School

It's all in the cards

CDR Rabb JAGC

LT Goldberg JAGC

Iron Man Award

Professor Goldberg's

Honest Lawyer Privacy Policy

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

Healthcare Still Runs On Vertical 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**

Good Bye VDTM, Hello Bits & Bytes

Privacy & Security Are Part of Health Care

Never Tell a HIPAA Lie

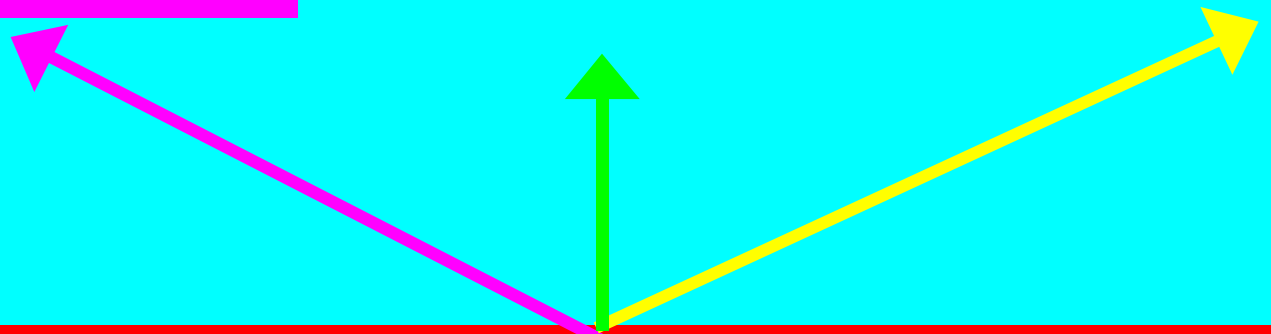
HIPAA BULL!!!!!

We Have Lots of Law

Federal Law

Professional Obligations

State Law



Privacy *Before* HIPAA

HCFA (CMS) Internet Security Policy

- **1997 – Drop Dead Internet**
- **1998 - Internet Communications Security & Appropriate Use Policy**
- **Encryption, authentication**
- **Temporary pre-HIPAA**

First Technologarian

Conditions of Participation

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 of facility**

Conditions of Participation

- **Resident right to access all records pertaining to resident including current clinical records within 24 hours (excluding weekends & holidays)**
- **May buy, at cost not to exceed community standard, photocopies of records or any portions of them upon request**

Conditions of Participation

- **Resident has right to be fully informed in language that resident can understand resident's total health status, including resident's medical condition**

Conditions of Participation

- **Privacy includes accommodations, medical treatment, written & telephone communications, personal care, visits, & meetings of family & resident groups**
- **Does not require facility to provide a private room for each resident**

Conditions of Participation

- **Resident may approve or refuse release of personal & clinical records to any individual outside facility**

Conditions of Participation

- **But resident's right to refuse release of personal & clinical records does *not* apply when resident transferred to another health care institution record or release required by law**

Medicare State Ops. Manual

- MDS data are part of resident's clinical record
- Protected from improper disclosure by facilities

MDS Privacy Resident's Rights

- **Nursing homes must inform each resident about electronic transmission of MDS to State & HCFA**

National Association of Attorneys General

- State consumer protection laws
- State health care privacy laws

HIPAA Is Tippa Privacy & Security Iceberg

TV President Josiah Bartlet Has Health Care Secret In West Wing

The HIPAA Monologues

If a HIPAA could talk, what would it want to say?

- **281,000,000+ patients**
- **Tell us your medical history please (fat chance)**
- **Wake up & smell the HIPAA**

- **H I P P A**
- **H I P A**
- **H I P P A A**
- ***H*** **I P A A** ***I*****t's** ***P*****owerful** ***A*****nd** ***A*****wesome**

Privacy Added To Rear of Employee Benefits Law

Administrative Simplification Subtitle

Ministry of Spirit of HIPAA

Embrace the Church of What's HIPAA'IN Now

Do we believe in privacy?

YES!

Are we all patients?

YES!

Will we take the HIPAA pledge?

YES!

HALLELULA, PRAISE HIPAA, AMEN!

HIPAA Pledge

"I pledge to preserve, protect, and defend the privacy and security of individually identifiable health information, to the best of my ability, and in furtherance of the best interests of more than 281,000,000 patients."

HIPAA Applicability

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

Lost HIPAAginity

HIPAA BULL!!!!!

HIPAA Is About

Standards

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.

HIPAA IS ABOUT PRIVACY

HIPAA Is About Security

On internet nobody knows you're a dog

Health Care Provider

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

What Is Health Care?

HIPAA BULL!!!!!

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**

- **<u>Not</u> who you are**

Protected Health Information

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

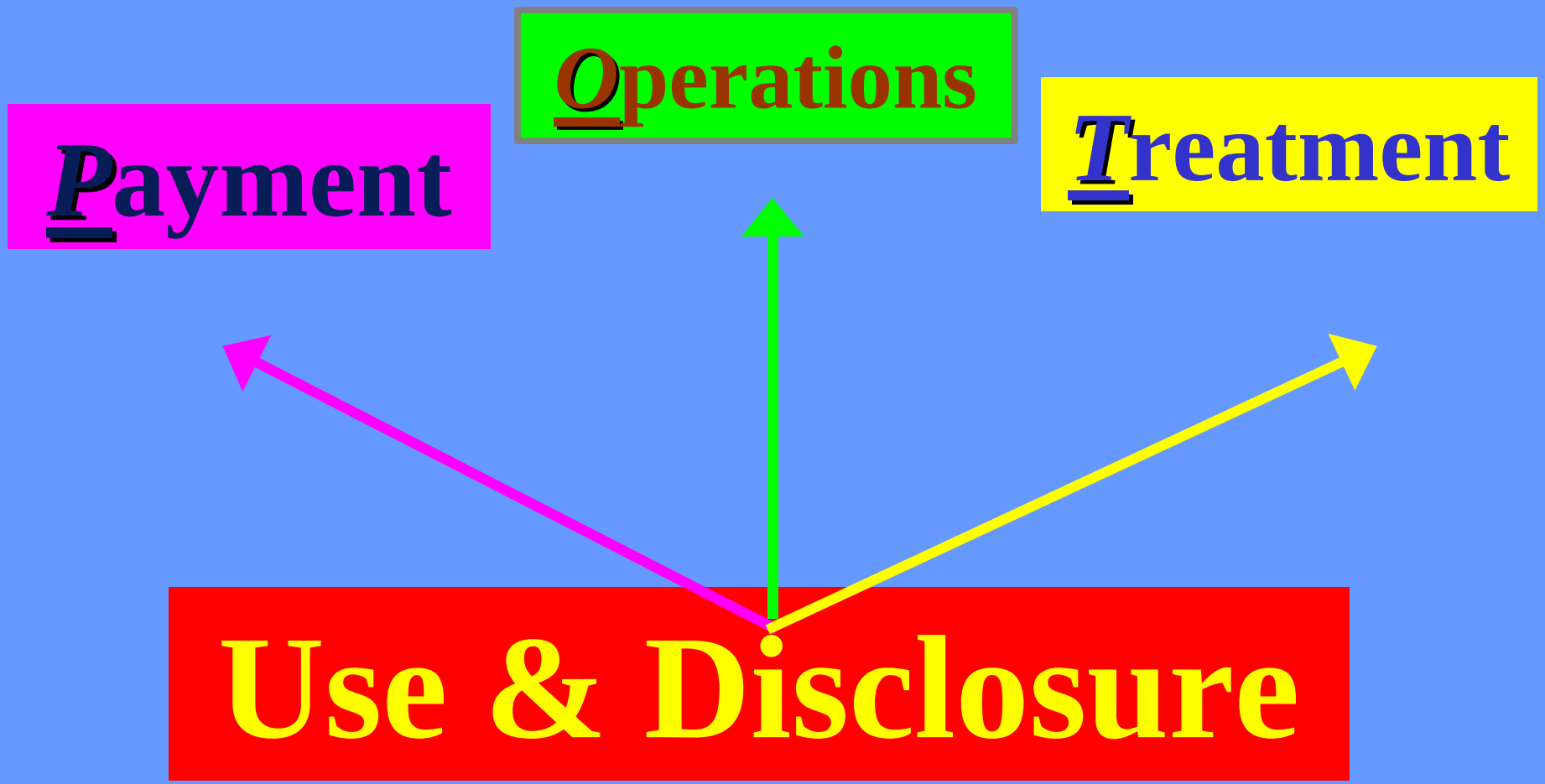
Individually Identifiable

- **ID of patient, relatives, employers, household**
- **(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**

HIPAA Privacy

- ***Protected health information*: individually identifiable health information transmitted by or maintained in electronic media or in any other form or medium**
- ***Consent*: use/disclose for payment, treatment, healthcare operations**
- ***Authorization*: outside use or disclosure**

Direct Provider Needs Consent



Use

- **Sharing, employment, application, utilization, examination, or analysis of individually identifiable health information *within* an entity that maintains such information**

Disclosure

- **Release, transfer, provision of access to, or divulging in any other manner of information *outside* the entity holding the information**

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 BULL!!!!!

Psychotherapy Is Special under HIPAA

Psychotherapy Notes

- **Notes recorded (in any medium) by health care provider who is a mental health professional documenting or analyzing contents of conversation during a private counseling session or a group, joint, or family counseling session and *that are separated from the rest of the individual's medical record***

***NOT* Psych. Notes**

- **Prescription & monitoring, counseling session start & stop times, modalities & frequencies of treatment furnished, results of clinical tests**
- **Summary of diagnosis, functional status, treatment plan, symptoms, prognosis, & progress to date**

Psychotherapy Consent

- **Covered entity (other than covered health care provider) is permitted to use or disclose protected health information without consent, if consent is not otherwise required under HIPAA, to carry out treatment, payment, or health care operations**

- ***EXCEPT*** **with respect to psych. notes**

Authorization Required for Covered Entity Use/Discl. of Psych. Notes EXCEPT:

- **To carry out the following treatment, payment, or health care operations, consistent with consent requirements:**
- **By originator of psych. notes for treatment**
- **By covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling**

Authorization Required for Covered Entity Use/Discl. of Psych. Notes EXCEPT:

- **By covered entity to defend legal action or other proceeding brought by the individual**
- **As required to investigate or determine covered entity's compliance with HIPAA**
- **As required by law or health oversight agency for oversight activities or with respect to the oversight of the originator of psych. notes; or by coroners or medical examiners; or to prevent/lessen a serious & imminent threat to health/safety of a person or the public**

No Access to Psych. Notes

- **Individual has right of access to inspect & obtain protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, *except for psychotherapy notes***
- **Covered entity *may* deny an individual access to psychotherapy notes without providing an opportunity for review**

Consent Required for Covered Health Care Provider Use or Disclosure of T/P/O EXCEPT:

- **If covered health care provider has an indirect treatment relationship with the individual**
- **If covered health care provider created or received protected health information in course of providing health care to an inmate**
- **In emergency treatment situations, if covered health care provider attempts to obtain consent as soon as reasonably practicable after delivery of such treatment**

Consent Required for Covered Health Care Provider Use or Disclosure of T/P/O EXCEPT:

- **If covered health care provider required by law to treat & tries but cannot obtain consent**
- **If covered health care provider tries but cannot obtain consent due to substantial barriers to communicating & makes professional judgment that consent to receive treatment is clearly inferred from the circumstances**
- **Absence of consent must be documented including reason why consent was not obtained**

Authorization & Consent

- **Covered entities need authorization to use or disclose psych. notes to carry out treatment, payment, or health care operations**
- **Consent, but *not* authorization, needed *for person who created psych. notes to use notes to carry out treatment* & for covered entity to use or disclose psych. notes for supervised training of students or practitioners in mental health under to practice or improve their skills in group, joint, family or individual counseling**

Get it in writing?

HIPAA BULL!!!!!

Verbal Agreement

- **Covered entities *must* obtain individual's verbal "agreement" before using or disclosing protected health information for facility directories & to persons assisting in the individual's care**

Verbal Agreement

- **Unlike "consent" and "authorization," verbal agreement may be informal & implied from the circumstances**

Verbal Agreement

- Verbal agreements are intended to accommodate situations where it is neither appropriate to remove from the individual the ability to control protected health information nor appropriate to require formal, written permission to share such information

Use of Psychotherapy Notes

- **Covered entity may, pursuant to a consent & without an authorization, use psych. notes to defend legal action or other proceeding brought by individual**
- **Disclosure allowed to covered entity's attorney to defend against action or proceeding & to others during judicial or administrative proceeding**

Authorization Not Required for Covered Entity Disclosure of Psych. Notes to Defend

- **Because authorization is required for disclosure of psych. notes for "health care operations," exception needed to allow covered entities to use protected health information about individual to defend against an action threatened or brought by that individual without asking individual for authorization to do so**
- **Otherwise, a consent is not sufficient for the use or disclosure of psych. notes to carry out treatment, payment, or health care operations -- *authorization is required***

Authorization Required for Covered Entity Use/Discl. of Psych. Notes for T/P/O

- **These authorizations will rarely be necessary, since psych. notes do not include information that covered entities typically need for treatment, payment, or other types of health care operations**
- **Authorization not required for use or disclosure of psych. notes when required for enforcement purposes, or when mandated by law, or when needed for oversight of the health care provider who created psych. notes, or by a coroner or medical examiner, or when needed to avert a serious and imminent threat to health or safety**

No Right of Access Unless Covered Entity Says Yes

- **Psychotherapy notes**
- **Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding**
- **Certain protected health information maintained by a covered entity that is subject to or exempted from Clinical Laboratory Improvements Amendments of 1988**

Health Plans & Psych. Notes

- **Health plans may *not* condition payment, eligibility, or enrollment on the receipt of an authorization for the use or disclosure of psychotherapy notes, even if the health plan intends to use the information for underwriting or payment purposes**

HIPAA BULL!!!!!

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**

Disclosures to Sponsor

- Plan documents restrict use/disclosure
- May disclose summary health info.
- To obtain premium bids & modify, amend, terminate plan
- Amend plan to establish permitted & required uses/disclosures
- Ensure agents/subs. getting PHI agree to same restrictions/conditions as plan sponsor

Sponsor Requirements

- Don’t use information for employment-related actions/decisions or other benefit plans
- Report inconsistent disclosures
- Show internal practices/books/records on PHI use/disclosure to HHS for compliance

Sponsor Requirements

- Destroy/return PHI when no longer needed
- Provide for adequate separation from plan
- Restrict employee access/use
- Lawyer/client privilege

Sponsor vs. Plan

- Fiduciary responsibilities
- Cost allocations
- Insurance
- Personnel additions
- Two entities, not one

Disclosures to Sponsor

- To carry out administration
- Restrict insurer/HMO disclosures
- No disclosure for employment-related actions/decisions or in connection with other benefit plan of sponsor
- Sponsor ***not*** covered entity or business associate or workforce

Enrollee Rights

- **Notice from plan *OR***
- **Notice from insurer/HMO**
- **But plan must maintain/provide limited notice**
- **"This notice describes how medical information about you may be used & disclosed & how you can get access to this information…."**

Special Plan Notice

- On compliance date to all covered individuals
- Thereafter at time of enrollment
- Within 60 days of material revisions to notice
- At least every three years tell them how to get notice of rights

Exceptions for Plans

- **Benefits solely thru insurer/HMO**
- **Do not create/receive PHI other than summary or participation information**

Not Covered Entities

- Employers (but note info.)
- TPAs
- Property/casualty/disability/auto plans event if pay for health care
- Workers compensation
- Stop-loss carriers & reinsurers

HIPAA BULL!!!!!

No HIPAA for Undertakers

The New Way: eSign

Electronic Signatures In Global & National Commerce Act

eSign Law & Beyond

- US: eSign Law Effective October 1, 2000
- German: Digital Signature Law
- European Union: Electronic Signature Directive

Security & Technology

Purpose of eSign Law

- To regulate interstate commerce by electronic means by permitting & encouraging continued expansion of electronic commerce through operation of free market forces

Purpose of HIPAA

- To improve Medicare & Medicaid programs, & efficiency & effectiveness of health care system, by encouraging development of health information system through establishment of standards & requirements for & electronic transmission of *certain* health information

eSign & Standards

- eSign law does *not* limit, alter, or otherwise affect any requirement of law relating to rights & obligations
- *Except* any requirement that contracts or other records be written, signed, or not electronic

HIPAA & Standards

- HIPAA is first, foremost, & uppermost about *standards*
- HIPAA is first, foremost, & uppermost about *standards*
- HIPAA is first, foremost, & uppermost about *standards*

eSign General Validity

- **Signature, contract, or other record relating to a transaction may *not* be denied legal effect, validity, or enforceability *solely* because it is in electronic form**

eSign General Validity

- Contract relating to such transaction may *not* be denied legal effect, validity, or enforceability *solely* because an electronic signature or record used in its formation

eSign Transaction Coverage

- Action(s) relating to the conduct of business, consumer, or commercial affairs between 2+ persons
- In or affecting interstate or foreign commerce

HIPAA Coverage

- Covered entities & transactions
- Fifty states
- DC, Guam, Puerto Rico, US Virgin Islands (but not American Samoa)

eSign Electronic

- Technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities

HIPAA Electronic Media

- Internet, Extranet, leased & dial-up lines, private networks, transmissions using magnetic tape, disk, or compact disk

eSign Record

- Information inscribed on a tangible medium
- Or stored in an electronic or other medium & is retrievable in

eSign Electronic Record

- Contract or other record created, generated, sent, communicated, received, or stored by electronic means

eSign Electronic Signature

- Electronic sound, symbol, or process, attached to or logically associated with a contract or other record
- And executed or adopted by a person

HIPAA Electronic Signature

- The attribute affixed to an electronic document to bind it to a particular entity
- The HIPAA

eSign Does *Not* Make You Use or Accept Electronic

- You do *not* have to agree to use *or* accept electronic records or signatures
- But government agency *must* accept a record "other than a contract to

HIPAA Electronic Signature

- **Covered entities are *not* yet required to use electronic signature -- but can be**
- **But if electronic signature *is* used in a covered transaction, HIPAA electronic signature standard *would* be required to be applied**

HIPAA Digital Signature

- Electronic signature based upon cryptographic methods of originator authentication, computed by using set of rules & parameters so that identity of signer & integrity of

HIPAA Use of Electronic Signature

- Use of electronic signature refers to act of attaching signature by electronic means
- Authentication of signatory
- Binding of signature to document & non-alterability after affixation

Computer Security

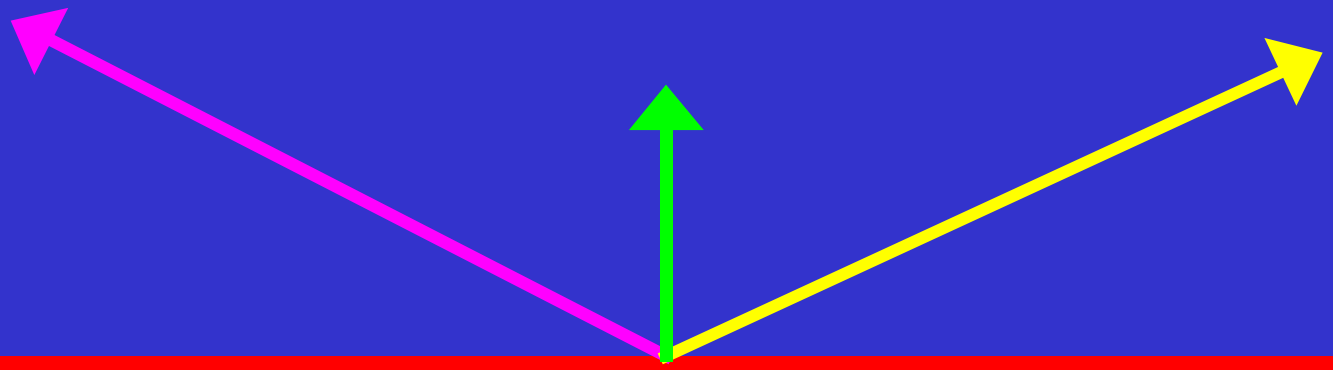
- Encryption & decryption
- Authentication/indentification
- *P*ublic *K*ey *I*nfrastructure
- Department of Commerce *Rijndael* [Rhine-doll] Data Encryption Standard

Single Key Encryption

Encrypt Key

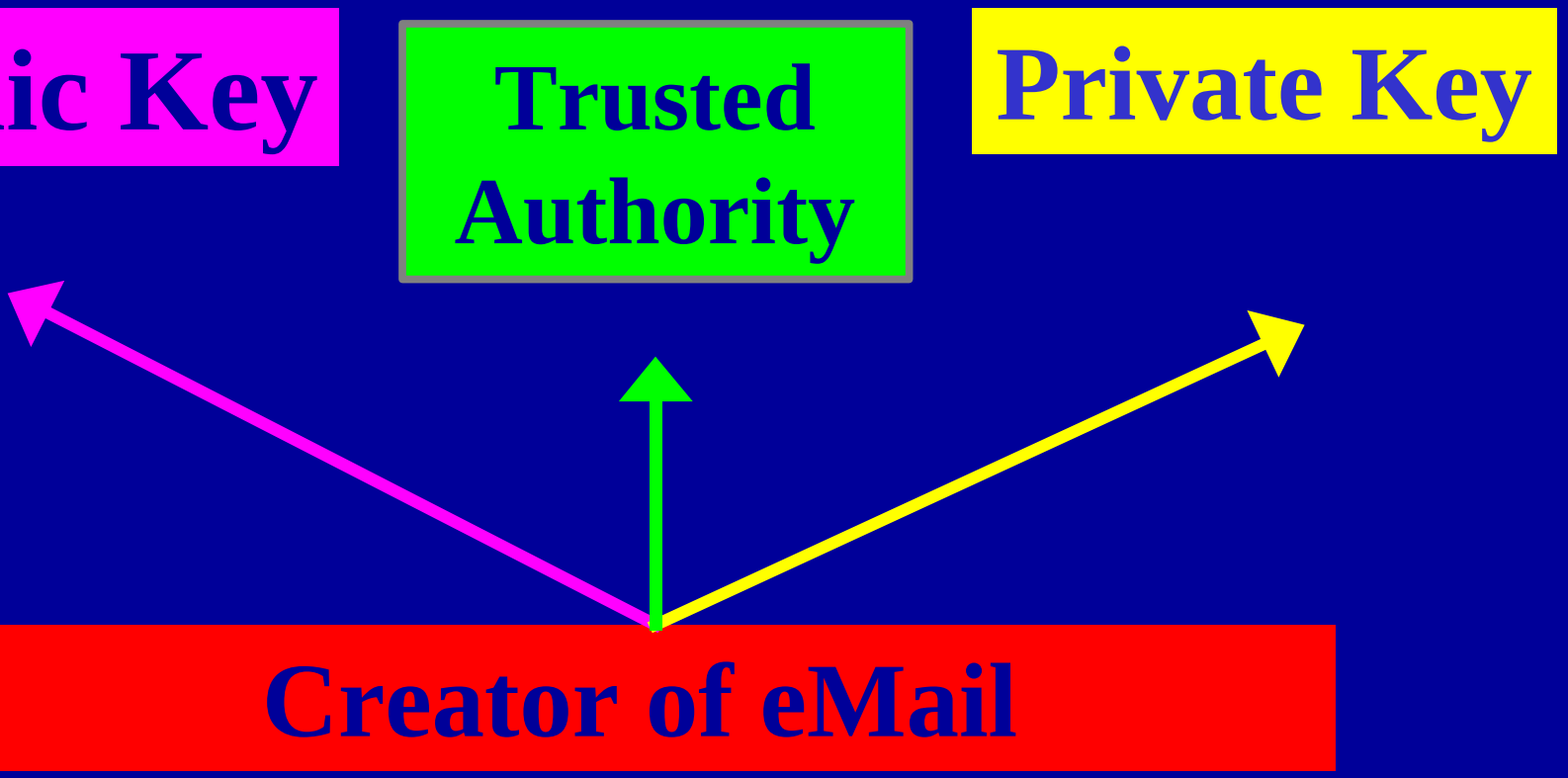
Same Key

Decrypt Key



Creator of eMail

Public Key Encryption



eSign Electronic Agent

- A computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response

Use of Electronic Agent

- **Contract/record relating to transaction in or affecting interstate/foreign commerce may *not* be denied legal effect, validity, or enforceability *solely* because its formation, creation, or delivery involved the action of one or more electronic agents so long as action is legally attributable to person to be bound**

eSign Law Does *Not* Cover:

- Laws about wills/trust & family law
- Consumer notices unless consented to
- Uniform Commercial Code
- Federal & state court orders & pleadings
- Utility services cancellation/termination
- Default & other primary home notices

Federal/State eSign Standards

- eSign does *not* limit or supercede Federal or state regulatory agency requirement that *records* be filed in specified *standards* or *formats*

eSign Preemption

- State law *may* preempt eSign with Uniform Electronic Transactions Act of National Conference of Commissions on Uniform State Laws (UETA)

eSign Preemption

- But any exception to scope of UETA *is* preempted by eSign
- If such exception is *inconsistent* with eSign or requires or gives greater legal status or effect to, specific technology for electronic records or

HIPAA Preemption

- Proposed security rule preempts state law
- Final privacy rule does *not* preempt more stringent state law
- Final standards/data sets rule preempts state law

Federal/State eSign Rules/Interpretation

- Federal/state regulatory agency with statutory rulemaking authority may *interpret* eSign Law
- HHS to interpret eSign?

eSign Enforcement

- ***No*** **specific delegation under eSign for enforcement or sanctions for failure to honor eSign**
- **Remedy: sue**

Office for Civil Rights

Enforcer With a Heart

HIPAA Office for Civil Rights Enforcement

- **HHS delegates – with authority to redelegate – authority under HIPAA to *administer* regulations & to *make decisions* regarding *interpretation*, *implementation* & *enforcement* of standards & administrative requirements**

HIPAA BULL!!!!!

Cooperation

- **HHS will, to extent practicable, seek cooperation of covered entities in obtaining compliance**

We're Here to Help You

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

Complaints

- **Person who believes covered entity is not complying with HIPAA may file complaint within 180 days +**

Must Mitigate

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

Investigations

- **HHS may investigate complaints & review policies, procedures, & practices of covered entity & circumstances regarding alleged compliance acts & omissions**

Access to Records

- **Covered entity must keep records & submit compliance reports, as, when & how 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**

Investigations

- **HHS may investigate complaints**
- **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**

Enforcement

- HHS sanctions for violations
- Federal civil sanctions
- Federal criminal sanctions
- State sanctions
- Contractual sanctions
- Professional sanctions

HIPAA Corporate Compliance Program

- **DOJ Sentencing Guidelines**
- **Can abate costs/penalties & enforcement actions**

False Claims Act

"Whoever…knowingly and willfully makes or causes to be made any false statement or representation of a material fact in any application for any benefit or payment under a Federal health care program...."

Max. Penalty: $25,000/

5 years in jail

False Claims Act

- Qui Tam
- “honest mistakes”
- “mere negligence”
- Quality of care cases
- Violation of HIPAA rules
- Poor HIPAA = poor care?

Why Have Compliance Plan

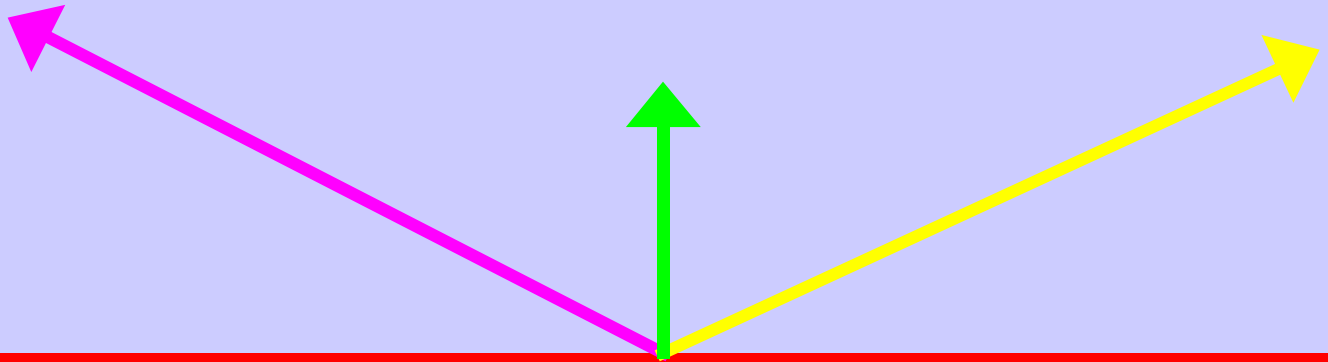
- **Reduces Non-compliance Costs**
  - **Sanctions**
  - **Survey compliance issues**
- **Reduces Potential Penalties**
  - **US DOJ sentencing guidelines**
  - **Criminal and civil fines & penalties**
  - **Program exclusion**
- **Reduces Likelihood of Enforcement Action**
- **Government strongly recommends**

Risk Assessment

Employees

Vendors

Patients



Corporate Compliance Official

Compliance in a Nutshell

- **<u>What you cannot do</u>: violate the law by, among other things, not using the data sets and standard transactions; or violating the prohibitions against disseminating protected health information or have bad security**
- **<u>What you must do</u>: institute a QA-type process to monitor, track, correct and prevent non-compliance**

What Are the Laws?

- False Claims Act (Civil/Criminal/State)
- Anti-Kickback Statute
- Federal Health Care Offense
- Health Care Fraud
- Theft or Embezzlement
- False Statements
- Obstruction of Investigations
- Wire Fraud/Mail Fraud
- General (consumer protection)
- HIPAA

False Claims Act (Criminal)

"Whoever…knowingly and willfully makes or causes to be made any false statement or representation of a material fact in any application for any benefit or payment under a Federal health care program...."

Max. Penalty: $25,000/5 years in jail

False Claims Act (Criminal)

- **Criminalizes Billing For Services:**
  - **never delivered**
  - **never documented**
  - **different than delivered**
  - **doubly billed to two payors**
  - **not medically necessary**
  - **not accurately coded**
  - **violation of Conditions/Participation**
  - ***in violation of HIPAA rules???***

False Claims Act (Criminal)

Whoever ... having knowledge of the occurrence of any event affecting (A) his initial or continued right to any such benefit/payment, or (B) the initial/continued right to any such benefit/payment of any other individual in whose behalf he has applied for or is receiving such benefit/payment, *conceals or fails to disclose such event with an intent fraudulently to secure such benefit/payment* either in a greater amount or quantity than is due or when no such benefit or payment is authorized

False Claims Act (Civil)

- Civil War era statute
- Prohibits “knowingly” submitting a claim to the federal government for payment of a false or fraudulent claim, or using a false record to support a claim for payment.
- Penalties: up to $10,000 plus double or treble damages

False Claims Act (Civil)

- **"Knowing" or "Knowingly" is not solely specific intent, instead it means any of the following:**
  - **having actual knowledge of the information**
  - **acting in deliberate ignorance of the truth or falsity of the information; or**
  - **acting in reckless disregard of the truth or falsity of the information.**

False Claims Act (Civil)

Eight Factors the DOJ/OIG Must Consider

1. **Notice of Rule or Policy**
2. **Clarity of Rule or Policy**
3. **Pervasiveness/ Magnitude of False Claims**
4. **Adherence to a Compliance Plan**
5. **Identification of/Response to Noncompliance**
6. **Guidance Sought from HCFA**
7. **Previous Audits for Same Issues**
8. **Any Other State of Mind Information**

False Claims Act (Civil)

Five Responses DOJ/OIG Must Consider

- good faith reliance upon applicable statutory and regulatory provisions and interpretations
- misled by inconsistent and often contradictory guidance from the carrier
- provider's well-documented compliance and self-reporting procedures did not reveal the billing mistake
- error was immaterial
- "innocent" mistake/no intent to defraud

Anti-Kickback Statute

illegal to knowingly and willfully solicit, receive, offer or pay remuneration in cash or in kind to induce or in return for referring, recommending or arranging for the furnishing of any item or service payable by Medicare or Medicaid programs

$25,000/5 years in jail

civil penalties and program exclusion

Effective Compliance Plan

1. Establish written standards & procedures
2. Designate responsible individuals
3. Regular & effective training
4. Effective means of communication
5. Audit & monitor compliance
6. Compliant hiring & discipline
7. Establish investigation protocols

Organizational Structure

- **Designation of a Privacy/Compliance Official**
  - **who**
  - **reporting obligations**
  - **oversight & monitoring**
  - **develop training programs**
  - **coordinate personnel & contractors**
  - **oversee audits**
  - **conduct investigations**

Organizational Structure

- **Form HIPAA Compliance Committee**
  - **Composition**
  - **Function**
  - ***"high integrity, good judgment, assertiveness and an approachable demeanor"***
  - **develop standards of conduct**
  - **resources for compliance official**

Chief Privacy Official

Your Compliance Team: Where Everyone Knows Your Name

- **Cheers!**

Written Standards: Code of Conduct

- Brief statement of general principles
- Expectations of employees
- Summary of basic laws
- Basic instructions for reporting & response
- Management involvement
- Readable (translated if necessary)
- Posted & distributed
- Attestations of receipt & understanding

Written Standards: Risk Areas

- Baseline audit recommended
- Written data
- Electronic data
- Access to information
- Document, document, document
- Minimally necessary information

Employee Screening

- **Pre-employment screening**
- ***"a…facility also should seriously consider whether to employ individuals who have been convicted of crimes of neglect, violence, theft or dishonesty, or financial misconduct"***
- **avoid excluded individuals & contractors**
- **OIG Exclusions List: http//exclusions.oig.hhs.gov/epls**

Excluded Individuals

- **Examples of Excluded Providers**
  - **nurses, nurse aides & others**
  - **pharmacists**
  - **ambulance drivers**
  - **contractors, suppliers and manufacturers**
  - **billing agents and claims processors**
- **$10,000 CMP for each excluded item or service**

Your Privacy Official's Job:

To Worry, Worry, Worry

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 & Liabilities

- **Operation Cure.All**

Erin HIPAAvich

A Classy Action?

HIPAA BULL!!!!!

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”

More Litigation

- ***Sutherland*** **case in VA**
- ***South Carolina Med'l Association et al.***
- ***As'n of Amer. Physicians & Surgeons*** **Houston, TX**

So. Carolina Med'l As'n

- HIPAA law & rules defective
- Unconstitutional delegation
- Preemption is vague
- Save stringency?
- Rule expands > electronic

Amer. Phys. & Surgeons

- Unconstitutional delegation
- Gov't intrusion w/o warrant
- Should not affect intrastate
- Rule expands > electric
- Houston, Texas, y'all

HIPAA BULL!!!!!

Judge Jones says:

- ***[I]n light of the strong federal policy in favor of protecting the privacy of medical records…”***

Judge Jones says:

- ***"In accord with the [HIPAA privacy] Standards issued by [HHS[…"***

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 $25,000/year**

BAD HIPAA

VERY BAAAD HIPAA

HIPAA For Crooks

- ***Unlawful use or disclosure***
- **$250,000 + 10 years in jail if with *intent* to sell, transfer or use health information for commercial advantage, personal gain, or malicious harm**

FIRST HIPAARARIAN

Dial 1-800-RAT-FINK

FBI Likes HIPAA

HIPAA: Largest Unfunded Federal Mandate in Healthcare

I Gave You CMS Because I Feel Your Pain
and I "See A Mess"

Congressional Testimony

- **HCFA [CMS] lacks specially trained personnel to oversee security**
- **HCFA's contractors are *outright obstructive* to providing sound security**
- **Compounding these errors was HCFA's inability to catch or prevent errors**

Guidance Overview

- 17 “reasonable(ly)” steps, criteria, reliance, efforts, safeguards, precautions
- 18 “professional(ly)”
- 7 “professional judgment”
- 23 “appropriate(ly)”

Clarifications

- **HHS & most parties agree that privacy protections must *not* interfere with a patient's access to or the quality of health care delivery**

Clarifications

- ***Phoned-in Prescriptions* – permit pharmacists to fill prescriptions phoned**
- ***Referral Appointments* – permit direct treatment providers receiving first time referral to schedule procedures before obtaining consent**

Clarifications

- ***Allowable Communications*** **– okay to have whatever communications required for quick, effective, high quality health care, including routine oral communications**
- ***Minimum Necessary Scope*** **– common practices, such as use of sign-up sheets & X-ray lightboards, & maintenance of patient medical charts at bedside, are okay**

Clarifications

- **HIPAA does NOT require:**
- **Private rooms**
- **Soundproofing of rooms**
- **Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners**
- **Encryption of telephone systems**

Clarifications

- **The Privacy Rule does not "pass through" its requirements to business associates**
- **Set of contractual obligations far narrower than the provisions of the rule**
- **Covered entities do not need to ask their business associates to agree to appoint a privacy officer [sic], or develop policies & procedures for use & disclosure of PHI**

Clarifications

- **Covered entity *not* liable for privacy violations of business associates**
- **Covered entities *not* required to actively monitor or oversee how business associate carries out safeguards or extent to which business associate abides by requirements of contract**

Americans Wants HIPAA

HIPAA IN A BOX?

-

HIPAA BULL!!!!!

ARE *YOU* THE WEAKEST LINK?

Which Way Are We Going?

What if this is

as good as it gets?

Don’t Get Behind HIPAA

BE A HIPAA HERO (sm)

BE A HIPAA HEROINE (sm)

Professor 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 October 24, 2001.**

Why is this man smiling?

We practice safe HIPAA!

www.healthlawyer.com

That's All Folks!

www.healthlawyer.com

- For additional materials including the HIPAA law, rules, & other materials relating to health care and information technology, please visit http://www.healthlawyer.com

goulston&storrs
thinkresults

Alan S. Goldberg, JD, LLM

Third National HIPAA Summit

Basic HIPAA for the Rest of Us

www.healthlawyer.com