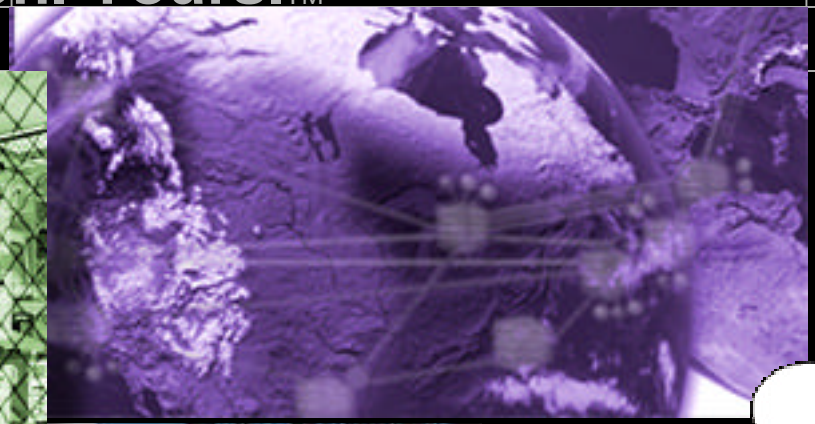
We’re on a mission. Yours.™



EXODUS

Agenda

- **Background**
  - Culture of HC
  - Difficulties
  - Drivers
  - Stance of Government
  - Viewpoint of HC Community
- **HIPAA and Administrative Simplification**
  - History
  - Definitions
  - Relevant Regulations that flow from HIPAA
  - Covered Entities
- **Compliance**
- **HC Provider Roles and Responsibilities**
- **Security Vendors - How can we help?**

Cultural Background

"Their powers for change lie in the hands of those who have the imagination and insight to see that the new invention has offered them new liberties of action ... and that they can act in new ways."

Ithiel Sola De Pool - The Social impact of the telephone (MIT Press, Cambridge, MA, 1977)

intersect associates
a limited liability company

Cultural Background

" New social behavior patterns and new social institutions are created which in turn become the commonplace experience of future generations."

Ithiel Sola De Pool - The Social impact of the telephone (MIT Press, Cambridge, MA, 1977)

intersect associates
a limited liability company

Cultural Background

"Where .. foresight has still failed, a common .. reason has been a lack of imagination about .. change and perseverance in an established way of doing things."

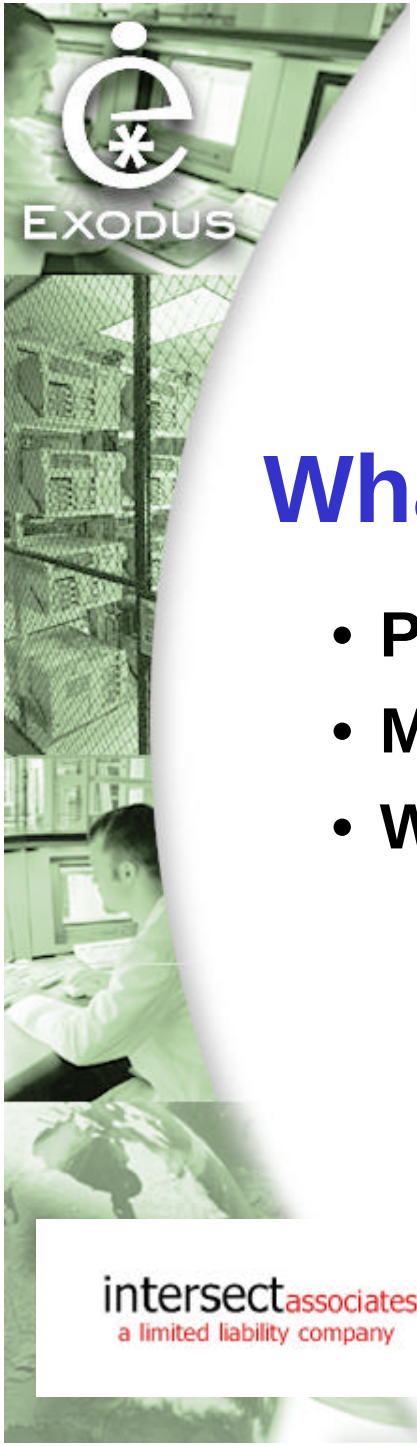
Ithiel Sola De Pool - The Social impact of the telephone (MIT Press, Cambridge, MA, 1977)

intersect associates
a limited liability company

Is the healthcare environment different from other industries?

Yes, but not for the reasons you might think!

intersect associates
a limited liability company



What are the drivers for doctors?

- **Providing care**
- **Meeting their ethical and professional obligation**
- **Working within their environment successfully**

intersect associates
a limited liability company

Where does the security of the healthcare data fit?

intersect associates
a limited liability company

Privacy has been a concern since the Hippocratic Oath

Integrity of the data is as important as confidentiality

Professional ethics, business practices, and state laws overwhelm privacy

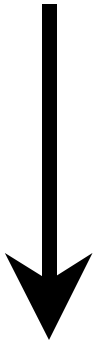
intersect associates
a limited liability company

Health care security has been lax

intersectassociates
a limited liability company

New uses of data

Electronic exchange of data



Heightened consumer concerns

Who are the Players?

- **Public**
- **Government**
- **Healthcare Industry**
  - **traditional health care enterprise**
  - **web-based health care enterprises**

- 10% are purists
- 10% don't care
- 80% are somewhere in the middle

The percentages change

The public changes their stance

intersect associates
a limited liability company

- Who are they?
- What are they like?
- What are they trying to accomplish?

- **the traditional healthcare enterprise**
- **the web-based healthcare enterprise**

The drivers and concerns are different

intersectassociates
a limited liability company

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA) -**

  aka - Kennedy-Kassebaum

  - **Enacted August 21, 1996 (104th Congress)**
  - **Provides continuity of healthcare coverage**
    - **Limits preexisting condition exclusions**
    - **Prohibits discrimination based on health status**

- **Purpose: to improve the health care system with standards for electronic transfer of information**
  - **Encourages development of a health information system to promote system effectiveness and efficiency**
  - **Establishes standards and requirements for electronic transmission of certain health information**

- A specific proposal for a rule (regulation) for implementing the requirements of Administrative Simplification subtitle of HIPAA
- Common elements:
  - Definitions
  - Implementation
  - Penalties for Violations

- **Notice of Proposed Rule Making (NPRM)**
  - **Process for creating standards for implementing the requirements of Administrative Simplification subtitle of HIPAA**
  - **The NPRM is an announcement of a specific proposal for a rule (regulation)**

Steps to Publication

1. **Drafting by HHS Implementation Teams with extensive outreach to:**
   - **National Committee on Vital & Health Statistics (NCVHS)**
   - **ADA, NUBC, NUCC, WEDI**
   - **ANSI HISB, CPRI, and many others**
2. **Government approval (Data Council, advisors, other agencies, OMB)**
3. **Publication in *Federal Register***
4. **Analysis of extensive comments**
5. **Reconciliation among NPRMs and implementation planning**

Timetable for Standards Adoption and Compliance

- **18 months after its enactment for HHS to adopt standards (i.e. write regulations), except**
  - **30 months to adopt claims attachment standards**
- **24 months after effective date of final rule for compliance (effective date is 60 days after publication), except**
  - **36 months for small health plans**

Schedule for Publication

Rule	Status
Standards for Electronic Transactions and Code Sets	NPRM published May 7, 1998 Comment period ended July 6, 1998 Expected Final Rule publication 6/2000 Expected Date Compliance Req'd 8/2002
National Standard Health Care Provider Identifier	NPRM published May 7, 1998 Comment period ended July 6, 1998 System of Records Notice published July 28, 1998
National Standard Employer Identifier	NPRM published June 16, 1998 Comment period ended August 17, 1998
Security and Electronic Signature Standards	NPRM published August 12, 1998 Comment period ended October 13, 1998
Standards for Privacy of Individually Identifiable Health Information	NPRM published November 3, 1999 12/15/99 Federal Register notice of extension of comment period. 1/5/2000 Federal Register notice of NPRM technical corrections. Comment period ended February 17, 2000
National Standard for Health Claim Attachments	not yet available
National Standard Identifiers for Health Plans	not yet available

- **Security and Electronic Signature Standards - developed to protect the confidentiality, integrity, and availability of individual health information**
  - **The Security Standard will provide a standard level of protection in an environment where health information pertaining to an individual is housed electronically and/or is transmitted over telecommunications systems/networks**
  - **The Electronic Signature Standard will provide a reliable method of assuring message integrity, user authentication, and non-repudiation**

- **Standards for Privacy of Individually Identifiable Health Information** - standards to protect the privacy of individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions

- **Standards for Electronic Transactions and Code Sets** - standard for Electronic data interchange (EDI), or electronic transfer of information, such as electronic media health care claims, in a standard format between trading partners

intersect associates
a limited liability company

- **Covered entities - Definitions**
  - **Providers - entities that:**
    - **transmit health information in electronic form in connection with a standard transaction**
    - **use another entity to transmit health information in electronic form with a standard transaction on its behalf**
  - **Clearinghouses - a public or private entity that possesses or facilitates the processing of health information**
  - **Health Plans - entity that provides, or pays the cost of, medical care**

HIPAA Applies to...

- **Covered Entities - Examples**
  - **All health care providers**
    - Hospitals
    - Clinics
    - Nursing homes
    - Physicians
    - Dentists
    - Suppliers
- **All health care clearinghouses**
  - Billing services
  - Re-pricing companies
  - "Value added" networks
- **All health plans**
  - Group health plans
  - Health insurance issuers
  - HMOs
  - Medicare and Medicaid
  - Governmental health care programs

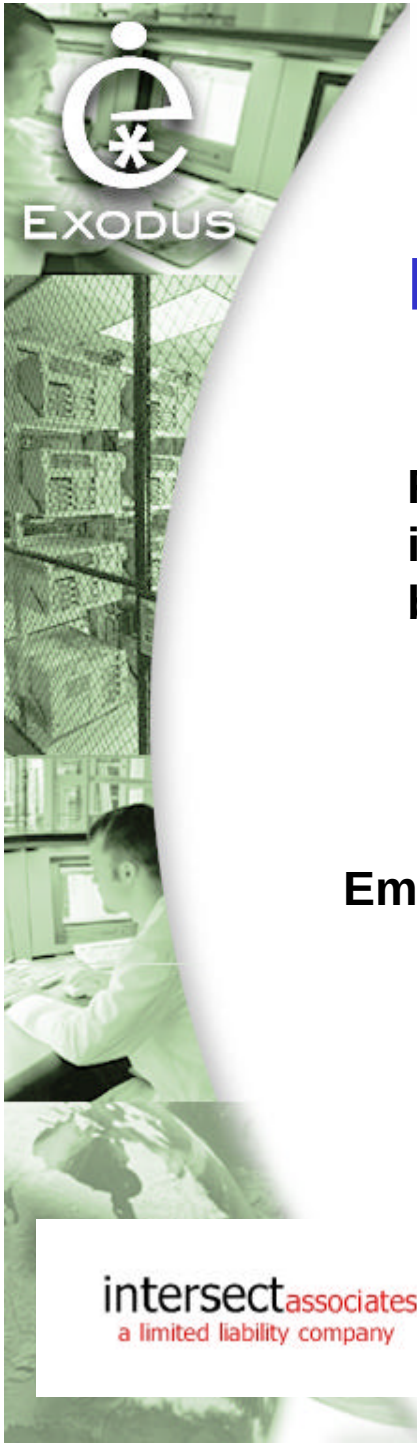
- **Business partners of covered entities -** **such as Vendors and Contractors,**
  - **must sign a contract with the covered entity that binds the business partner to the same use and disclosure rules as the covered entity - “Chain of Trust Partner Agreement”**

- **Individually identifiable health information**
  - ***Any information*, whether oral or recorded in any form or medium, that**
  - **is *created or received* by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and**
  - **relates to the past, present, or future *physical or mental health* or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and**
  - ***identifies the individual*, or**
  - **with respect to which there is reasonable basis to believe that the information *can be used to identify the individual***

intersect associates
a limited liability company

- **Individuals**
  - many options considered
  - congress has put this on hold
  - many privacy concerns
- **Health Plans**
  - proposed rule delayed while health plan was defined and identifier solution found
- **Employers**
  - Federal Employer Identification Number (EIN)
  - used by health plans to identify the employer of the participant in the health plan

- **Providers**
  - **Health plans have routinely and independently assigned identifiers to providers**
  - **National Provider Identifier created by HCFA was chosen and will initially be assigned to providers who participate in the electronic transactions**
  - **A National Provider System will be created to maintain a National Provider File and assign numbers**



Privacy

Right of an individual to be left alone

Private information shared in confidence

Security

Guards:

- integrity
- confidentiality
- availability

Embodied in:

- Law
- Professional codes of conduct
- Accrediting and licensing standards
- Business practices mechanisms
- Consumer influence

Provided through:

- Policies
- Procedures
- Technical services
- Technical mechanisms

intersect associates
a limited liability company

Security Standard

- **Requirements**
- **Implementation features**
- **Standards**

Security Standard

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms

Administrative Security Standards

- Certification
- Chain of trust partner agreement
- Contingency plan
- Formal mechanism for processing records
- Information access control policies and procedures
- Internal audit
- Personnel security
- Security configuration management
- Security incident procedures
- Security management process
- Termination procedures
- Training

Physical Security Standards

- Assigned security responsibility
- Media controls
- Physical access controls
- Policy and guidelines on work station use
- Secure work station location
- Security awareness training

Technical Security Standards

- Access control
- Alarm, event reporting, and audit trail
- Authorization control
- Data authentication
- Encryption
- Entity authentication

- **Because of constraints imposed by scope of HIPAA, privacy *regulation* is applicable only to:**
  - **"Covered" entities - health care providers, plans, and clearinghouses**
  - **"Protected" information - electronic information (and its antecedents and descendents)**
  - **"Floor" of provisions - does not preempt more stringent state laws, potentially requiring some dual systems**

Regulation intended to be flexible and scalable, in which each covered entity assesses its own needs and implements policies appropriate to its information practices and business requirements

intersect associates
a limited liability company

Privacy Rule - Key Provisions

- **Use**
- **Disclosure**
- **Minimum necessary**
- **De-identification**
- **Reasonable**

Privacy Rule - Individual Rights

- ***Permit*** **versus** ***require***
- **Individuals must be *informed* of how their information is used and disclosed**
- **Individuals have the right to *inspect* and copy information about themselves (with reasonable, cost-based copying fees)**
- **Individuals have the right to have an *accounting* for all disclosures of protected health information for purposes other than treatment, payment, and healthcare operations**
- **Individuals have the right to request *restrictions* on further disclosures (although covered entity is not required to comply unless agreed upon)**
- **Individuals have the right to request *amendment* to correct their information (although covered entity is not required to comply)**

Impact of HIPAA on Healthcare Organizations

- **Business Processes** - affects:
  - how information is processed
  - how information is exchanged with business partners (chain of trust partner agreement)
  - personnel security procedures
  - security configuration management
  - security incident response/management
  - termination procedures
  - security awareness training
  - physical access to systems
  - contingency planning
  - media controls
- **IT Operations** - imposes additional IT requirements:
  - audit
  - authentication of users/entities
  - access control
  - protect/determine data integrity
  - protect/secure communications

Compliance is required, but ...

- **No Current Compliance Regulation/Mechanism**
  - No details provided by regs other than possibility of either periodic reviews of policies, practices, procedures
  - Self compliance is the working assumption
  - Compliance through accreditation reviews?
- **HC Orgs need to worry about due diligence**
  - Need to sign Chain of Trust Partner Agreement
  - Are they doing enough to instill confidence in their patients/clients/business partners?
  - Can they be sued?
- **Enforcement will be addressed**
  - Complaints made by individuals will be addressed
- **Organizations already addressing compliance**

intersect associates
a limited liability company

- **Non-compliance**
  - $100 for each violation, total for each requirement in calendar year not more than $25,000
- **Wrongful disclosure of individually identifiable health information**
  - Uses or causes to be used a unique health identifier
  - Obtains individually identifiable health information
  - Discloses individually identifiable health information
- **Penalties**
  - $50,000 and/or 1 yr imprisonment
  - $100,000 and/or 5 yrs imprisonment for false pretenses
  - $250,000 and/or 10 yrs imprisonment for intent to sell

Healthcare Provider Responsibilities

- Create corporate culture of sensitivity
- Mandate compliance
- Create security and privacy policies for use and disclosure
  - clear
  - concise
- Require same of business partners
- Provide consumer education

Healthcare Provider Implementation

- Awareness, education, top management commitment
- Develop strategic approach
- Current state inventory (leverage Y2K)
- Risk assessment
- Standards selection
- Resource and cost estimation
- Business partner negotiation
- Operational policy and procedure development
- Implementation and testing
- Ongoing monitoring and compliance

Security Vendor Niches

- **Knowledge sources**
- **Trainers**
- **Suppliers**
  - **Standards**
  - **Implementation Guides**
  - **Conformance Testing**
  - **Compliance Certifications**
- **Business partners**
- **Good citizens**

- **Key Security Vendor Roles**
  - **become knowledgeable**
  - **guide provider understanding**
  - **provide knowledge that is missing**

Lead rather than respond

What can we do?

- **security implementations**
  - **not impede the providing of care**
  - **guard against loss, destruction, or unwarranted changes or release of data**
  - **ensure compliance with regulation**
  - **provide ‘safe harbor’ against litigation**
- **security engineers *must know healthcare* to have any chance of success**

intersect associates
a limited liability company

Summary

- the primary concern of healthcare practitioners is to *provide care*
- security engineers must know and do their job within the context of the most complicated industry environment
- security engineers must walk a narrow path - balancing the primary concerns of the industry yet meeting regulatory requirements

intersect associates
a limited liability company