The Health Insurance Portability and Accountability Act (HIPAA) and Strategies for Implementation in a Government Healthcare Organization
Agenda

- Overview of HIPAA
  - ETCS
  - ASCA
  - Identifiers
  - Privacy
  - Security

- Implementation Strategies
  - Challenges
  - Impacts of HIPAA on VHA
  - Implementation Organizational Structure
  - Successes

- Questions
Overview of HIPAA: VHA’s Focus

HIPAA
Health Insurance Portability and Accountability Act of 1996

Title I
- Insurance Portability

Title II
- Fraud and Abuse
- Medical Liability Reform
- Administrative Simplification

Title III
- Tax Related Health Provision

Title IV
- Group Health Plan Requirements

Title V
- Revenue Off-sets

Privacy

Security

EDI

Identifiers

Transactions

Code Sets
## Status of HIPAA in Rulemaking Process

<table>
<thead>
<tr>
<th>Electronic Transactions and Code Sets Standards</th>
<th>Proposed</th>
<th>Final</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider ID</td>
<td>Released 5/1998</td>
<td>Not yet published</td>
</tr>
<tr>
<td>Payer ID</td>
<td>Not yet released</td>
<td>Not yet published</td>
</tr>
<tr>
<td>Patient ID</td>
<td>Not yet released</td>
<td>On-hold</td>
</tr>
</tbody>
</table>


Who Complies With HIPAA?

- **Covered Entity**
  - Providers
  - Plans
  - Clearinghouses

- **Requirements**
  - **Scope** – All of Health Care
  - **Specific to Structure of entity**
  - Different for each covered entity
  - Different for each area of HIPAA
  - Includes Business Associates

- **Deadlines**
  - Different for each area of HIPAA
  - **Privacy** – April 14, 2003
HIPAA EDI Standards
HIPAA: The EDI Standards

- Transaction standards:
  - Enrollment/Dis-enrollment: ASC X12N 834
  - Eligibility request and response: ASC X12N 270/271
  - Claims Institutional ASC X12N 837
    - Professional
    - Dental
  - Claims – Pharmacy ASC NCPDP v 5.1
  - Claim status: ASC X12N 276/277
  - Referral and authorization: ASC X12N 278
  - Payment and remittance advice: ASC X12N 835
  - Premium payment: ASC X12N 820

- Though a standard for Claims Attachments has not yet been announced, it is expected to be: ASC X12N 277+275 + HL7
Clinical Data Code Sets Standards:

- ICD-9 for diseases (CMS formerly HCFA)
- CPT-4 for services and procedures (AMA)
- HCPCS for medical equipment, injectable drugs, and transportation services (AMA)
- CDT-3 for dental services (ADA)
- NDC for prescription drugs (For retail only)

These apply only to the administrative and financial electronic transactions
ASCA: The 6-Months Extension

Congress has approved through the Administrative Simplification Compliance Act, an extension to the HIPAA ETCS deadline for organizations who need additional time to comply with HIPAA.

- The organization must submit a request for the extension prior to October 15, 2002; VHA filed timely.
- To file, the organization must have a plan in place to become compliant with HIPAA by October 2003.
- Must begin testing by April 2003 . . . translates to a 6-mos extension.
- The extension does not affect the deadline for other areas of the legislation (i.e., Privacy).
- ASCA prohibits payment of Medicare claims not submitted electronically.
Key EDI Initiatives

- **Payor ETCS for payor functions**
  - Ability to receive all required transactions

- **Provider ETCS for VA medical centers**
  - e-Claims transactions
  - e-Payment transactions
  - e-Insurance Identification & Verification
  - e-Status Messaging
  - e-Medicare Remittance Advice

- **Special Government Agency Issues**
  - Other laws dictates how VA does business
  - Relationship with Department of Treasury
HIPAA Standard Identifiers
HIPAA: Standard Identifiers

Universal Identifier Standards:

- Health Care Providers (NPI - National Provider Identifier)
  - Originally proposed to be an 10 digit numeric identifier with a check digit, though some modifications already expected
- Employers (EIN - Employer Identification Number) – Final Rule designates the nine digit IRS Taxpayer Identification Number
- Health Plans (HealthPlanID) - Identifier yet to be announced
- Individuals (UHID) - Currently on hold; hotly debated

Use of these identifiers technically applies only to the administrative and financial electronic transactions
HIPAA Privacy Rule
HIPAA: The Privacy Rule

The Privacy Rule:

- Extends coverage to electronic, paper-based and orally communicated information
- Allows health information to be used and shared for treatment, payment and health care operations
- Supports disclosure under defined circumstances for certain national priority purposes such as research, public health, law enforcement and oversight
- Requires patient authorization for use and disclosure of health information for purposes other than treatment, payment or health care operations
- Gives consumers greater access to and control over their health information
- Requires organizations to establish and maintain safeguards for protecting the confidentiality and integrity of health information and protect against unauthorized access of this information
HIPAA: The Privacy Rule

The Bottom Line:

- Compliance will be required by April 14, 2003
- Civil monetary and criminal penalties apply:
  - If knowingly providing information
    - $50,000 and/or up to 1 year imprisonment
  - Under false pretenses
    - $100,000 and/or up to 5 years imprisonment
  - Intent to sell, transfer, or use health information for commercial advantage, personal gain, or malicious harm
    - $250,000 and/or up to 10 years imprisonment
- At the present time there is no indication of when enforcement will be effective and how enforcement will be conducted
  - A separate Enforcement Rule is being drafted
- Office of Civil Rights has been given responsibility for enforcement
# HIPAA: The Privacy Rule

<table>
<thead>
<tr>
<th>General Rules &amp; Information</th>
<th>§164.502</th>
<th>Uses and disclosures of protected health information General Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>§164.504</td>
<td>Uses and disclosures: Organizational Requirements</td>
</tr>
<tr>
<td>Uses and Disclosures Requirements</td>
<td>§164.506</td>
<td>Uses and disclosures to carry out treatment, payment or health care operations</td>
</tr>
<tr>
<td></td>
<td>§164.508</td>
<td>Uses and disclosures to which an authorization is required</td>
</tr>
<tr>
<td></td>
<td>§164.510</td>
<td>Uses and disclosures requiring an opportunity for the individual to agree or object</td>
</tr>
<tr>
<td></td>
<td>§164.512</td>
<td>Uses and disclosures for an authorization or opportunity to agree or object is not required</td>
</tr>
<tr>
<td></td>
<td>§164.514</td>
<td>Uses and disclosures of protected health information: Other requirements</td>
</tr>
<tr>
<td>Notice</td>
<td>§164.520</td>
<td>Notice of privacy practices for protected health information</td>
</tr>
<tr>
<td>Patient’s Rights</td>
<td>§164.522</td>
<td>Patient’s Rights: Right to request privacy protection for protected health information</td>
</tr>
<tr>
<td></td>
<td>§164.524</td>
<td>Patient’s Rights: Access of individuals to protected health information</td>
</tr>
<tr>
<td></td>
<td>§164.526</td>
<td>Patient’s Rights: Amendment of protected health information</td>
</tr>
<tr>
<td></td>
<td>§164.528</td>
<td>Patient’s Rights: Accounting of disclosures of protected health information</td>
</tr>
<tr>
<td>Administration</td>
<td>§164.530</td>
<td>Administrative Requirements</td>
</tr>
</tbody>
</table>
Key Privacy Initiatives

- Policy Review and Re-write
- Privacy Policy Training
- Notice of Privacy Practices
- Minimum Necessary
- Directory Opt-out
- Business Associates
- Security Safeguards
- Special Government Issues
  - Privacy Act, FOIA and other Government-specific laws governing privacy
  - Sharing relationship with other Government agencies (i.e., DoD)
HIPAA Security Rule
HIPAA: The Security Rule

Intent of HIPAA Security Rule:

- Maintain reasonable and appropriate operational, technical, and physical safeguards that:
  - Ensure confidentiality and integrity of information provided to authorized staff
  - Prevent unauthorized use or disclosure
  - Protect against external threats and physical hazards
- Standards are intended to protect against both external and internal threats
- Technical measures alone will be insufficient; security tools by themselves won’t make an organization compliant
- A successful privacy/security program requires a solid “confidentiality culture”
- Good documentation will is essential to compliance with the Security standards and development of a Security Program
Implementation Strategies
Challenges

- VHA is one covered entity with 162 hospitals and over 600 CBOCs
- Legislative mandate on program structures
- Classification in HIPAA inconsistent with major business models
- Complexities of a Governmental Agency
Strategies: Immediate Impacts

- Classification of Organization
- Privacy (by April 2003)
  - Development /documentation of policies & procedures
  - Broadening responsibilities of VHA Privacy Officers
  - Identifying /contracting with business associates
  - De-identifying patient information where necessary
  - Producing notice of privacy practices, authorization forms
  - Capturing, providing patients access to, the uses and disclosures of their health information for purposes other than treatment, payment or health care operations
  - Training workforce members who have access to IIHI
  - Altering information usage culture & security awareness of the organization
  - Processing & reviewing individual complaints

- Electronic Transactions and Code Sets—ETCS
  (Testing by April 2002 and Implementation by October 2003)
  - Multiple IT initiatives to upgrade core systems for ETCS
  - Establish a new system -or- outsource HP2 payment activities
  - Multiple IT initiatives to upgrade HP1 systems for ETCS
  - Implementing code set updates in a more timely manner

- Resources
Strategies: Future Impacts

• Resources

• Identifiers (multiple implementation dates)
  - Health Care Provider ID
    • NPRM Published May 1998
    • Awaiting Final Rule
  - Employer ID
    • NPRM Published June 1998
    • Final Rule Published May 2002
  - Health Plan ID
    • Controversial & Debated within the Industry
    • Awaiting NPRM
  - Individual ID
    • Controversial
    • Placed on hold by Congress

• Additional Transaction Sets, e.g. Claims Attachments

• Dynamic Nature of Evolving Electronic Business Solutions
• Ongoing Maintenance of Requirements
Strategies: Roles and Responsibilities

- Role of the PMO
- Role of the HIPAA Implementation Advisory Council (HIAC)
- Role of the Office Liaisons
- HIPAA Implementation Teams (HITs)
HIPAA Organizational Structure

Under Secretary for Health Business Office

VHA HIPAA-AS PMO

Admin Support

PO Director

PMO STAFF

SECURITY STANDARDS
VHA HIPAA-AS COMPONENT
Liaison

PRIVACY STANDARDS
VHA HIPAA-AS COMPONENT
Liaison

ETCS STANDARDS
VHA HIPAA-AS COMPONENT
Liaison

STANDARD IDENTIFIERS STANDARDS
VHA HIPAA-AS COMPONENT
Liaison

BUSINESS ASSOCIATE RELATIONS
Assistant PMO Director

OIC Office Liaison

EES Office Liaison

Revenue Office Liaison

HAC Office Liaison

Mgmt. Support Office Liaison

Prosthetics Office Liaison

HAS Office Liaison

Pharmacy Office Liaison

AAC Office Liaison

cyber Security Office Liaison

OGC Office Liaison

HSR&D Office Liaison

HEC Office Liaison

VA OAMM Office Liaison

VISN/Network Office Liaison

HIS Office Liaison

Compliance Office Liaison

Dental Office Liaison

VA HRM Office Liaison

SD&D Office Liaison

VAMC

HIT Teams X162
Role of the HIPAA-AS PMO:

The PMO will serve as:

- The major communications & information forum for HIPAA. Coordinate VHA’s efforts with the Department.

- Clearinghouse for ideas, best practices, solutions to problems

- Champion for overall vision, providing program guidance

- Catalyst for ensuring that HIPAA compliance strategies are implemented within the identified time frames.

- Reporting entity that collects & aggregates monthly progress reports from Office Liaisons
Role of the VHA HIPAA Implementation Advisory Council (HIAC)

- The HIAC provides overall guidance to the PMO with subject matter expertise, rule interpretation, legal and general support.

- Representatives from all critical VHA and VA Departments fulfill these HIAC roles.

- Strategic individuals from the former OI HIPAA Workgroup were transitioned onto the HIAC to ensure consistency.

- HIAC members may assist with the development of projects, strategy, and implementation planning of the HIPAA requirements.
Role of the Office Liaisons

- The Office Liaison responsible for managing/monitoring individual initiatives within their Program Office and ensuring that their Office complies.
- The PMO works with Office Liaisons to define tasks/offer guidance & support.
- Specific responsibilities of the Office Liaison are to:
  - Facilitate Office-wide efforts and promote overall HIPAA implementation;
  - Provide direction to their HIPAA Team Members;
  - Communicate overall status to PMO on a monthly basis;
  - Escalate issues to the PMO;
  - Facilitate tactical development to address new HIPAA requirements;
  - Communicate Best Practices, Issues and Resolutions to the PMO.
Role of the HITs

- The HIT is responsible for implementing within their Facility and ensuring that their Facility complies with HIPAA.
- The PMO and Program Offices will assist HITs in understanding requirements.
- Specific responsibilities of the HIT are to:
  - Interact with HIPAA PMO, the Privacy Office and other Program Offices to implement HIPAA solutions created by Program Offices.
  - Conduct local surveys/inventories & initiatives to prepare facility for HIPAA implementation
  - Assist Program Offices & HIPAA PMO in educating their facility on HIPAA requirements
  - Monitor and report their facility’s implementation progress as required by the HIPAA PMO
Successes

- Compliance with Privacy Rule by April 2003
  - Notice released to Veterans
  - Training completed by workforce
  - P&P Re-write complete and implemented
  - Minimum Necessary assignments completed
  - Business Associate Agreements in place
  - Confidential communications and directory-opt out capabilities in place
  - Release of Information Software in place
  - Research forms, policies and procedures in place
  - Complaint tracking process in place

- Compliance with ETCS Rule by October 2003
  - Testing on a number of projects
  - On target for all major ETCS initiatives for payor and provider functions
Questions?