HIPAA Training is Forever

Presented by Samuel P. Jenkins, Privacy Officer

Military Health System – TRICARE Management Activity

March 29, 2007

Agenda

- Background
- Changing Policy Landscape
- HIPAA Training - Accountability and Consequences
- Look Ahead – Training Trends

Background

Speaker Introduction – Samuel P. Jenkins, Privacy Officer

- Joined TRICARE Management Activity (TMA) in July 2001 and was appointed the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Privacy Implementation Officer
- Appointed TMA Privacy Officer in August 2003, responsibilities include:
  - HIPAA
  - Freedom of Information Act (FOIA)
  - Privacy Act
  - Information Technology/Automated Data Processing Personnel Security
  - Data Use Agreements
  - Records Management
  - Privacy Impact Assessments (PIAs)
  - Privacy and Security Compliance

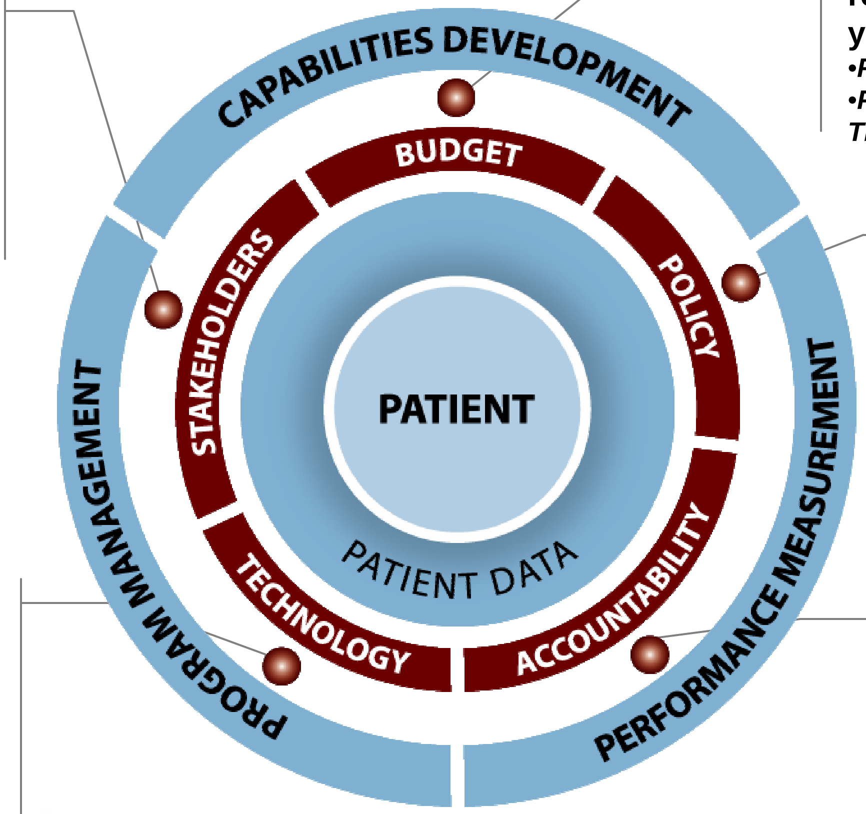
Learning Objectives

- Obtain a holistic understanding about the environment and landscape for HIPAA training and why training is required – “forever”
- Understand the key considerations for designing and implementing an enterprise-wide HIPAA awareness, education and training program
- Share techniques to ensure that all staff have the awareness, capabilities, skills, attitudes, understanding, sensitivity and education to create a culture of privacy and security
- Discuss consequences for not providing adequate training – accountability
- Look ahead to examine the issues and drivers that may impact privacy training in the future

What Makes the Military Health System (MHS) Unique?

Characteristics	Unique Training challenges
Size of staff	Support staff of 132,500+ individuals (more for HIPAA training)
Mobile and relocating	Reach a highly mobile workforce with frequent changes in work location
Global locations	Serve facilities and beneficiaries stationed in many countries and the battlefield
Distinct Branches of Service	Integrate large organizational units with distinct business processes (Army, Navy, Air Force and Coast Guard)
Multiple time zones	Conduct business in almost every time zone
Diverse patient and employee population	Require knowledge of many diverse cultures
Foreign language requirements	Perform work in multiple languages

Specific management activities are required to ensure proper alignment of patient centered care and its many considerations



Those who deliver, consume and monitor healthcare.

- *Agents and Caregivers*
- *Military Treatment Facilities (MTF)*
- *Regulators*
- *Standards Development Organizations (SDO)*

Foundation for advancement and innovation to improve healthcare.

- *Standards*
- *New Technological Developments*
- *Interoperability*
- *Certification & Accreditation (C&A)*
- *Security – Availability, Confidentiality, Integrity*

The processes for ensuring you have the capital to act on your requirements and achieve your mission.

- *Funding*
- *Portfolio Management and Transition Planning*

Rules and requirements to regulate the activities of healthcare stakeholders.

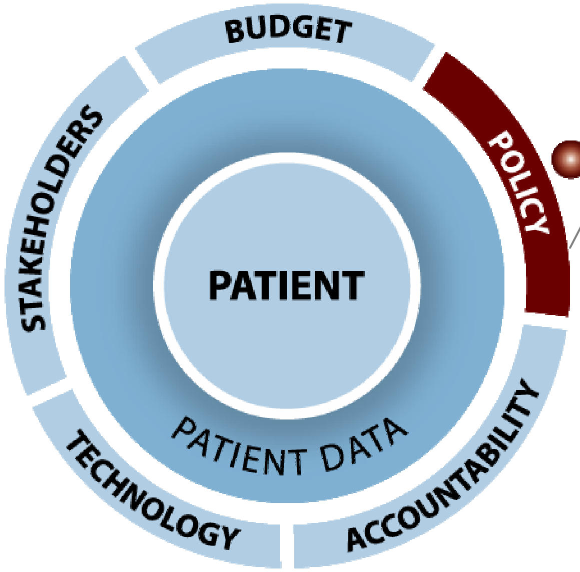
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Department of Defense (DoD) Policy*
- ***Department of Health and Human Services HHS Privacy and Security Standards***

Pressures from consumers that force us to ensure effective healthcare delivery.

- *Privacy*
- ***Awareness, Education and Training***
- *Contingency Planning*
- *Safety and Quality*
- *Trust*

Changing Policy Landscape

The changing policy landscape is one crucial factor creating the need for continuous HIPAA training

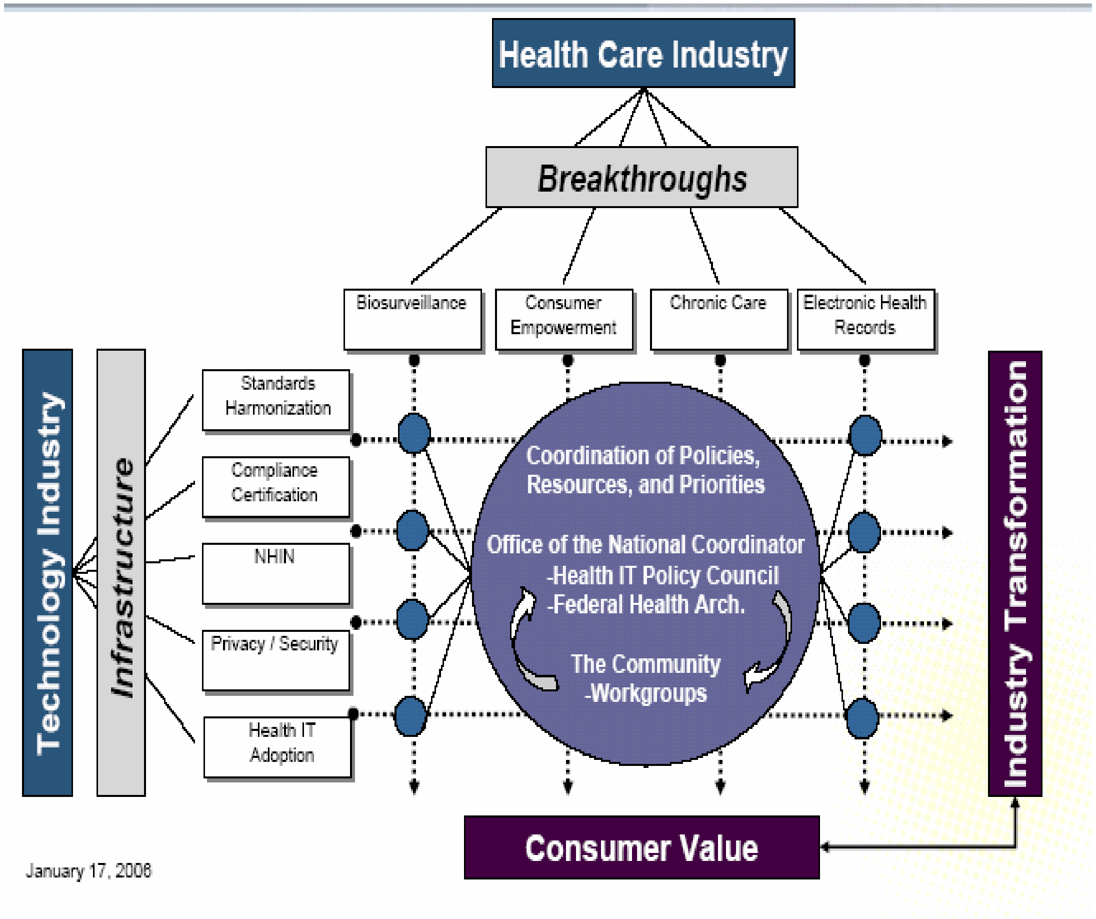


Rules and requirements to regulate the activities of healthcare stakeholders.

•Health Insurance Portability and Accountability Act (HIPAA)
•Federal Requirements
•Department of Defense (DoD) Policy
•State and Federal Laws
•Department of Health and Human Services HHS Privacy and Security Standards

New policy standards and best practices will impact business process and training requirements across the Military Health System (MHS)

- Executive Orders require MHS to increase the use of Health Information Exchange (HIE) to promote cost and efficiency improvement, transparency of health information, quality of care and patient safety in compliance with the HHS Office of the National Coordinator for Health Information Technology (ONC) standards as they are developed
- TRICARE Management Activity (TMA) Privacy Office is supporting standard setting efforts with HHS and compliance efforts with TMA divisions through the investment review process and collaboration with the MHS Chief Information Officers (CIOs)



Health Care Industry

Breakthroughs

Biosurveillance

Consumer Empowerment

Chronic Care

Electronic Health Records

Technology Industry

Infrastructure

Standards Harmonization

Compliance Certification

NHIN

Privacy / Security

Health IT Adoption

Coordination of Policies, Resources, and Priorities

Office of the National Coordinator
-Health IT Policy Council
-Federal Health Arch.

The Community
-Workgroups

Industry Transformation

Consumer Value

January 17, 2006

The HHS Office of the National Coordinator (ONC) on Health IT (HIT), promotes increasing interoperability and protection of health information

- **Health Information Standards Technology Panel (HITSP)**
  - Harmonizes workgroup recommendations with existing standards to refine and release IT standards
- **Certification Commission for Health Information Technology (CCHIT)**
  - Develops certification criteria and processes for healthcare IT products based on HITSP standards
- **National Health Information Network (NHIN)**
  - Produces pilot implementations of interoperable health information exchanges (HIE), consisting of four consortia led by Accenture, CSC, IBM and Northrop Grumman
- **Health Information Security and Privacy Collaborative (HISPC)**
  - Researching variations in business policy and state law that affect privacy and security
- **American Health Information Community (AHIC) Workgroups**
  - Federal Advisory panels make recommendations regarding potential standards and research initiatives

AHIC Confidentiality, Privacy and Security (CPS) Workgroup charges are designed to promote increased use of HIE by ensuring protection of health information

- Identity Proofing
- User Authentication
- Means to ensure data integrity
- Methods for controlling access to personal health information
- Policies for breaches of personal health information confidentiality
- Guidelines & processes to determine appropriate secondary uses of data
- A scope of work for a long-term independent advisory body on privacy and security policies

The CPS Workgroup made an initial set of recommendations to the HHS Secretary in January 2007

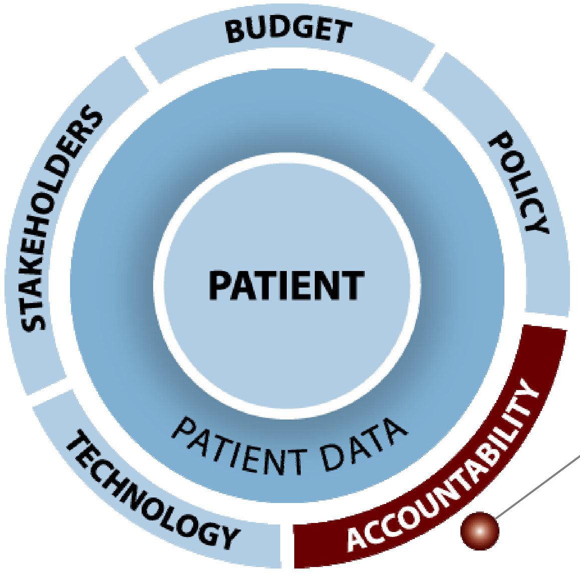
- Establishment of in-person identity proofing as the preferred method for new patient-provider relationships
- Documentation used for identity proofing should be maintained separate from health records and personally identifiable information (PII)
- Guidelines for non-in-person identity proofing when a standing, durable relationship exists between the patient and provider
- Approval for provider organizations to convert existing paper-based records into electronic format to promote adoption of HIT and transition to HIE
- CCHIT should develop software certification criteria, where applicable, to the above recommendations

Priorities for the coming year including collaboration with other groups/organizations and complementary research

- Patient Participation - Determine thresholds for mandatory and voluntary patient participation in Electronic Health Record (EHR) systems and recommend the appropriateness of various “Opt in vs. Opt out” models
- Access Control – define minimum necessary requirements for consumer control over their health information and extent to which its shared
- Privacy Policy Best Practices - Develop principles for interoperable consumer Personal Health Records (PHRs)
- Recommend essential privacy protections for non-covered entities under HIPAA (e.g., commercial PHRs vendors, HIEs, Regional Health Information Exchanges (RHIO))

HIPAA Training - Accountability and Consequences

A culture of privacy can be created through a robust awareness, education and training program to ensure compliance with privacy policy requirements



Pressures from consumers that force us to ensure effective healthcare delivery.

- ***Privacy***
- ***Awareness, Education and Training***
- ***Contingency Planning***
- ***Safety and Quality***
- ***Trust***

Key HIPAA Privacy Training Program Activities – Six Steps

Step 1: Conduct a training needs assessment and document the stakeholders’ training needs

Step 2: Create a training strategy and a plan to address the needs identified

Step 3: Develop the appropriate awareness, education and training content/materials; and determine the most effective delivery methods to meet the training needs

Step 4: Implement the training

Step 5: Monitor, evaluate and document compliance with the training strategy/plan

Step 6: Establish security and privacy reminders (Ongoing communications plan)

Step 1: Conduct a training needs assessment

- Complete baseline assessments at each facility
  - Deploy an appropriate gap analysis tool web application
  - Provide a standardized way for asking everyone the same questions and ensure that facilities are looking at the same things
  - Allow for trending across the enterprise and enable common solutions
- Complete a crosswalk analysis between HIPAA and various federal regulations; and compare with existing privacy and security programs to determine exact training content needs
- Identify and coordinate HIPAA training with other privacy training mandates (i.e. privacy impact assessments), if practical

Step 2: Create a training strategy and a plan

- Create a comprehensive plan
  - Go beyond checklist compliance
  - Integrate the selected tools into business processes
  - Measure the management processes of the organization
- Institute reporting methodology
  - Detail at the Facility level
  - Dashboard for Senior Leadership Level
- Build a professional workforce
  - Certifications
- Refresh and assess accomplishments

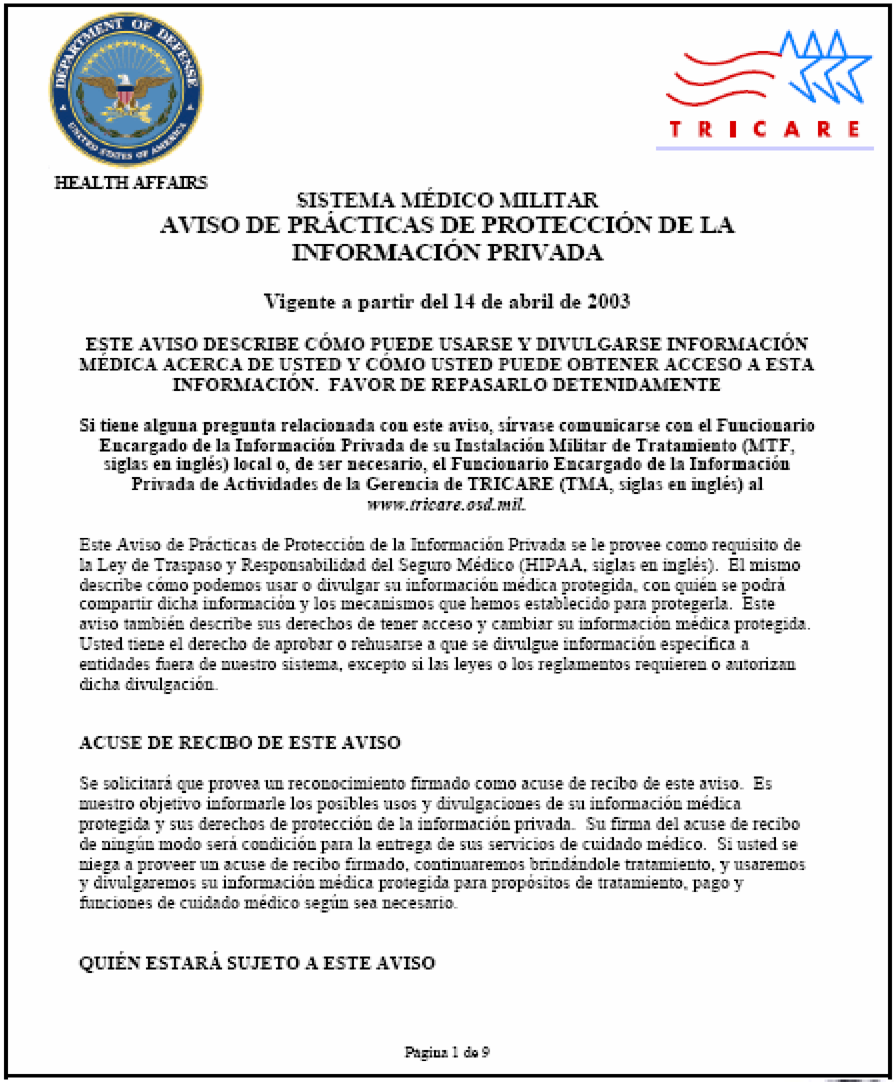
Step 3: Develop the appropriate awareness, education and training content/materials; and determine the most effective delivery methods to meet the training needs

- Use web cast training to augment the in-person conference and the selected Learning Management System courses
  - Real-time multimedia communication product
  - Enables instructors to deliver presentations, conduct live demonstrations, facilitate questions and answers, and lead discussions for participants around the world

Step 3: Develop the content/materials

Consider foreign language requirements

- Notices of Privacy Practices (NoPPs) are available in many languages
  - TRICARE Management Activity (TMA) NoPP is available in several alternative formats which include NoPPs in languages such as Tagalog, French, German, Italian, Japanese, Korean, Portuguese, Spanish, Chinese and Turkish.



HEALTH AFFAIRS

TRICARE

SISTEMA MÉDICO MILITAR
AVISO DE PRÁCTICAS DE PROTECCIÓN DE LA INFORMACIÓN PRIVADA

Vigente a partir del 14 de abril de 2003

ESTE AVISO DESCRIBE CÓMO PUEDE USARSE Y DIVULGARSE INFORMACIÓN MÉDICA ACERCA DE USTED Y CÓMO USTED PUEDE OBTENER ACCESO A ESTA INFORMACIÓN. FAVOR DE REPASARLO DETENIDAMENTE

Si tiene alguna pregunta relacionada con este aviso, sírvase comunicarse con el Funcionario Encargado de la Información Privada de su Instalación Militar de Tratamiento (MTF, siglas en inglés) local o, de ser necesario, el Funcionario Encargado de la Información Privada de Actividades de la Gerencia de TRICARE (TMA, siglas en inglés) al *www.tricare.osd.mil.*

Este Aviso de Prácticas de Protección de la Información Privada se le provee como requisito de la Ley de Traspaso y Responsabilidad del Seguro Médico (HIPAA, siglas en inglés). El mismo describe cómo podemos usar o divulgar su información médica protegida, con quién se podrá compartir dicha información y los mecanismos que hemos establecido para protegerla. Este aviso también describe sus derechos de tener acceso y cambiar su información médica protegida. Usted tiene el derecho de aprobar o rehusarse a que se divulgue información específica a entidades fuera de nuestro sistema, excepto si las leyes o los reglamentos requieren o autorizan dicha divulgación.

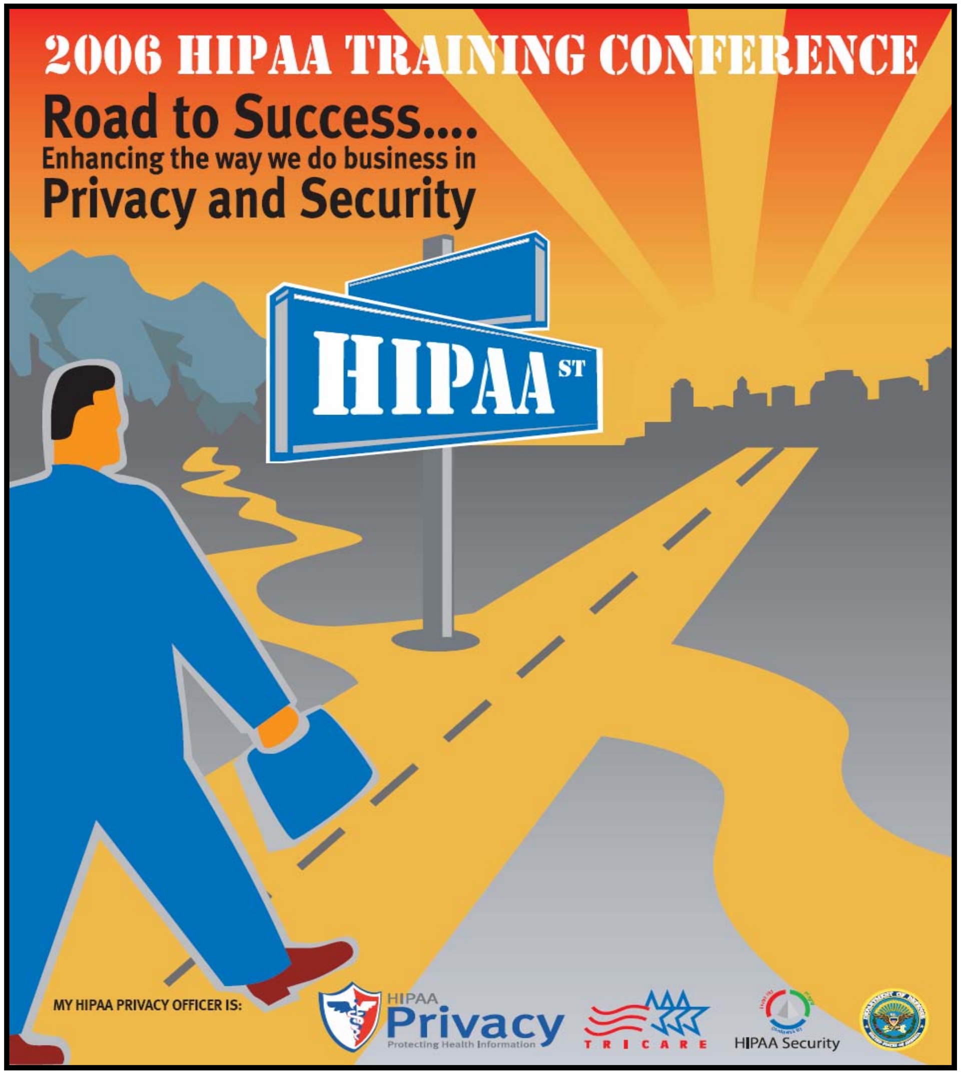
ACUSE DE RECIBO DE ESTE AVISO

Se solicitará que provea un reconocimiento firmado como acuse de recibo de este aviso. Es nuestro objetivo informarle los posibles usos y divulgaciones de su información médica protegida y sus derechos de protección de la información privada. Su firma del acuse de recibo de ningún modo será condición para la entrega de sus servicios de cuidado médico. Si usted se niega a proveer un acuse de recibo firmado, continuaremos brindándole tratamiento, y usaremos y divulgaremos su información médica protegida para propósitos de tratamiento, pago y funciones de cuidado médico según sea necesario.

QUIÉN ESTARÁ SUJETO A ESTE AVISO

Pagina 1 de 9

Step 4: Implement the training


2006 HIPAA TRAINING CONFERENCE
Road to Success....
Enhancing the way we do business in
Privacy and Security
HIPAA ST
MY HIPAA PRIVACY OFFICER IS:
HIPAA Privacy
Protecting Health Information
TRICARE
HIPAA Security

- Web cast training – homework
- Classroom lessons – theory
- War game exercise - practice

Step 4: Implement the training

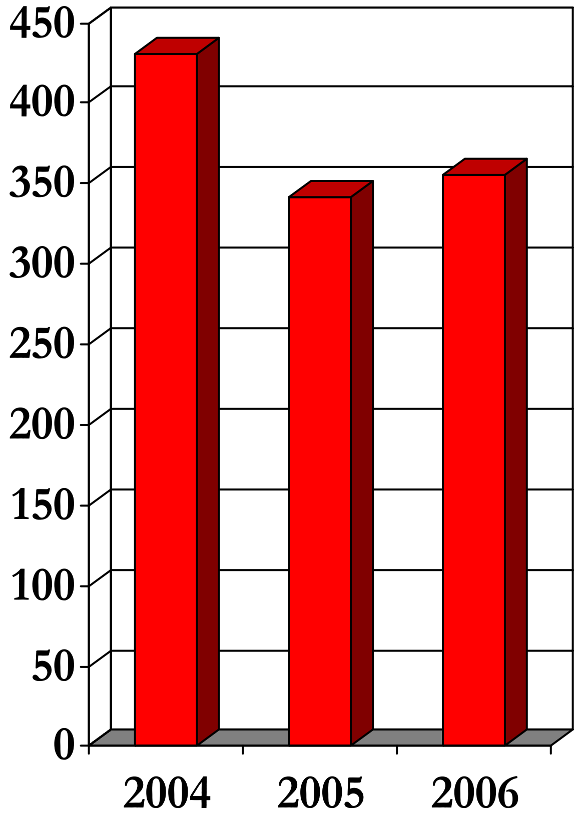
Military Health System (MHS) Stakeholders' Trained

- Deployed the first MHS global enterprise-wide Learning Management System (LMS)
  - Prior training initiatives were mostly Service specific or even command specific
- Successful deployment and robust business processes resulted in:
  - Data migration to an MHS-wide LMS that goes beyond HIPAA training
  - Enabled rapid world-wide accountable training response for major issues such as the Department of Veterans Affairs (VA) data breach

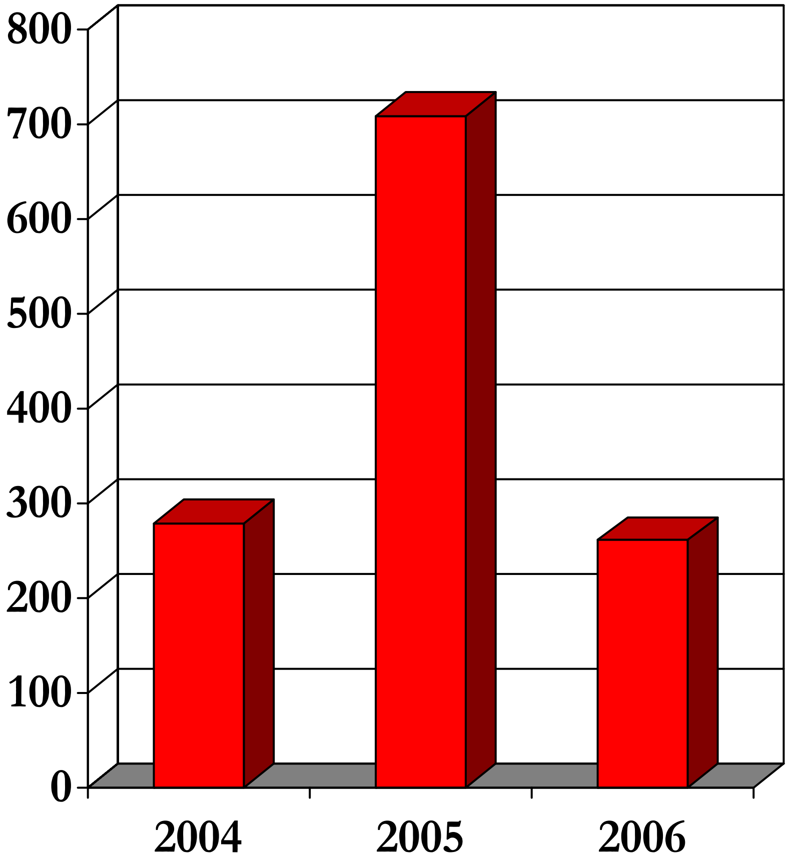
Training Methodology	Number of participants (2002-present)
Learning Management System (LMS)	160,000 plus (annually)
Training Conferences	Approx. 1,813
Web cast Training	Approx. 2,428

Step 5: Monitor and evaluate training plan

Conference Attendees



Web cast Attendees



Step 5: Monitor and evaluate training plan

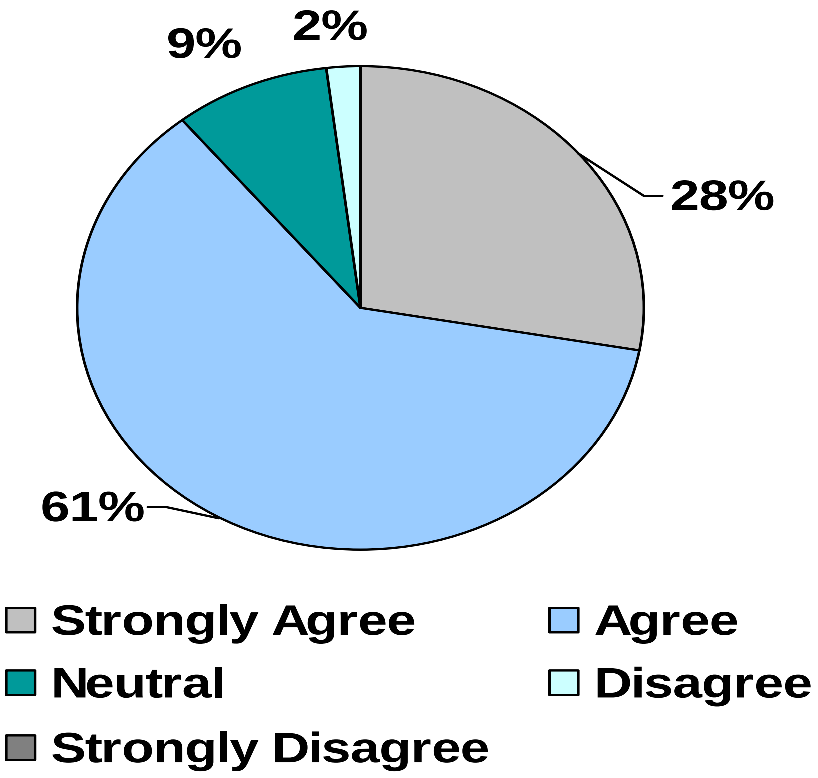
The HIPAA Training Participant Survey Demographics - 2006

- Total Survey Recipients
  - 355
- Total Responses
  - 107
- Service
  - Army: 35
  - Air Force: 43
  - Navy: 22
  - TMA: 1
- Advanced / Beginner
  - Beginner: 56
  - Advanced: 47

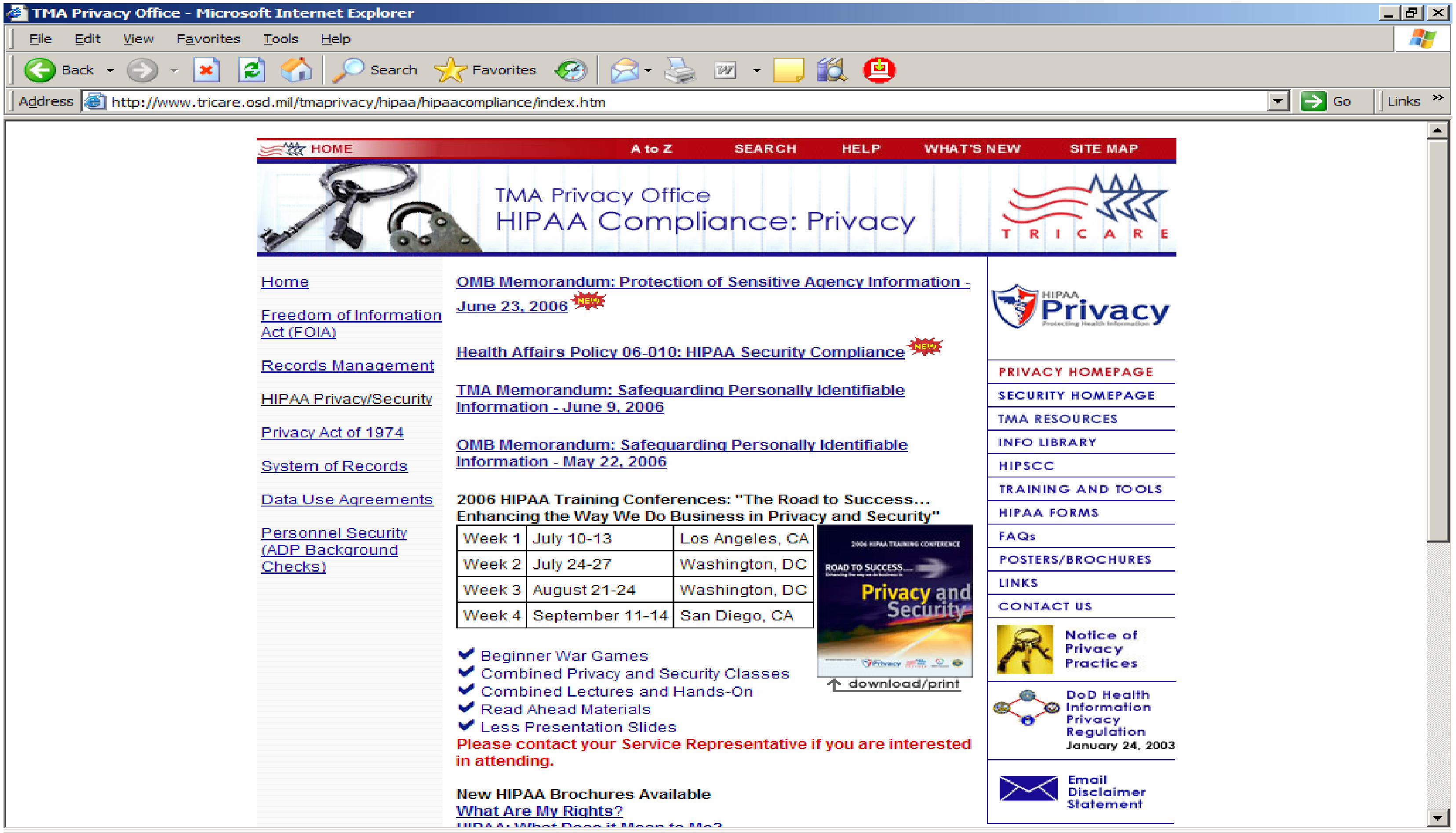
- Privacy Officer / Security Officer
  - PO: 58
  - SO: 31
  - Both: 13
- Years of Experience:
  - Less then a year: 38
  - 1-2 years: 40
  - 3-4 years: 17
  - 4+ years: 9

Step 5: Monitor and evaluate training plan
Training Results Tell the Story

The content of the 2006 Annual Training Conference helped me to understand the responsibilities of a HIPAA Privacy/Security Officer.



Step 6: Establish security and privacy reminders (Ongoing communications plan)


TMA Privacy Office - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.tricare.osd.mil/tmaprivacy/hipaa/hipaacompliance/index.htm
Go Links
HOME A to Z SEARCH HELP WHAT'S NEW SITE MAP
TMA Privacy Office
HIPAA Compliance: Privacy
TRICARE
Home
Freedom of Information Act (FOIA)
Records Management
HIPAA Privacy/Security
Privacy Act of 1974
System of Records
Data Use Agreements
Personnel Security (ADP Background Checks)
HIPAA Privacy Protecting Health Information
PRIVACY HOMEPAGE
SECURITY HOMEPAGE
TMA RESOURCES
INFO LIBRARY
HIPSCC
TRAINING AND TOOLS
HIPAA FORMS
FAQs
POSTERS/BROCHURES
LINKS
CONTACT US
Notice of Privacy Practices
DoD Health Information Privacy Regulation January 24, 2003
Email Disclaimer Statement
NEW
2006 HIPAA TRAINING CONFERENCE
ROAD TO SUCCESS...
Privacy and Security
download/print

OMB Memorandum: Protection of Sensitive Agency Information - June 23, 2006

Health Affairs Policy 06-010: HIPAA Security Compliance

TMA Memorandum: Safeguarding Personally Identifiable Information - June 9, 2006

OMB Memorandum: Safeguarding Personally Identifiable Information - May 22, 2006

2006 HIPAA Training Conferences: "The Road to Success... Enhancing the Way We Do Business in Privacy and Security"

Week 1	July 10-13	Los Angeles, CA
Week 2	July 24-27	Washington, DC
Week 3	August 21-24	Washington, DC
Week 4	September 11-14	San Diego, CA

- ✓ Beginner War Games
- ✓ Combined Privacy and Security Classes
- ✓ Combined Lectures and Hands-On
- ✓ Read Ahead Materials
- ✓ Less Presentation Slides

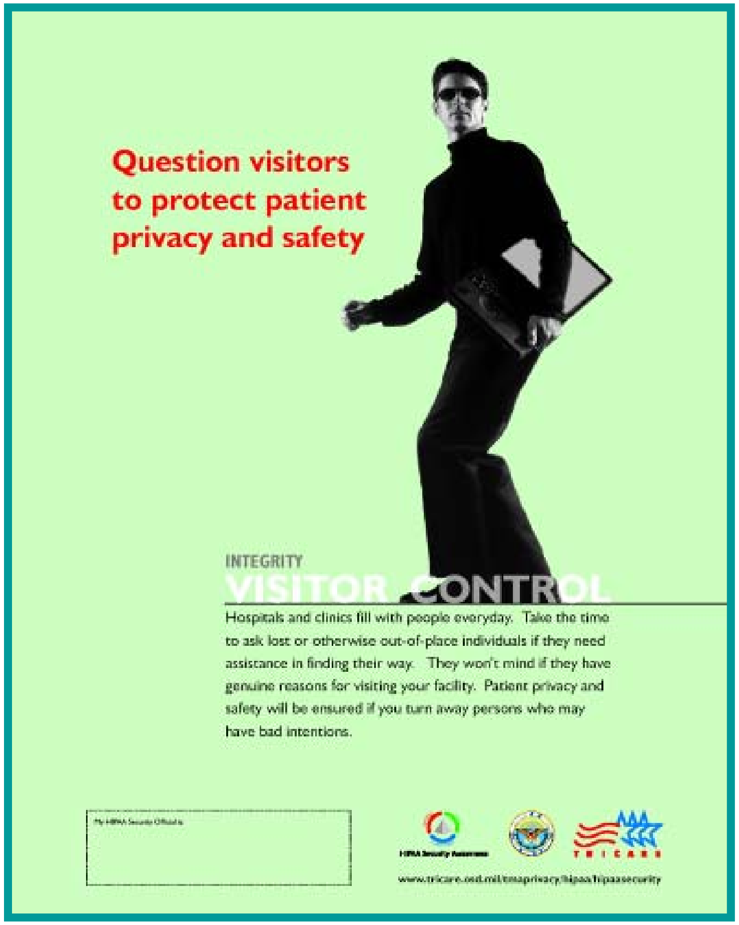
Please contact your Service Representative if you are interested in attending.

New HIPAA Brochures Available
What Are My Rights?
HIPAA: What Does it Mean to Me?

Step 6: Establish security and privacy reminders

Utilize several methods to distribute information

- Posters
  - Patient rights
  - Monthly message
- Website
  - Information Papers
  - Awareness Posters
  - Policies
  - Templates
  - Briefings


Question visitors to protect patient privacy and safety
INTEGRITY
VISITOR CONTROL
My HIPAA Security Official is:
HIPAA Security Awareness
TRICARE
www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

Hospitals and clinics fill with people everyday. Take the time to ask lost or otherwise out-of-place individuals if they need assistance in finding their way. They won't mind if they have genuine reasons for visiting your facility. Patient privacy and safety will be ensured if you turn away persons who may have bad intentions.

Training Lessons Learned

- No one single training delivery method will get the results you need.
- There must be a way to disseminate the latest training info quickly.
- Whenever possible use specific examples and scenarios to describe a concept or process.
- Use a ‘train-the-trainer’ methodology and utilize subject matter experts (SMEs) from the field to assist.
- There must be a way to receive feedback on the training offered.
- Make accommodations for global audiences.

Training is key to accountability and compliance.

Consequences can be severe.

Look Ahead – Training Trends

Training Trends
Implementation

- Student Demographics
  - Include entire workforce: Senior Executives, Providers, Administrators, Support Staff, Volunteers, etc
  - Include HIPAA Privacy and Security Officers, System Administrators and contractor support personnel
- Delivery Vehicles: Computer-based, self paced courses via a selected Learning Management System
- Teaching Modes:
  - In person, interactive On-site Training
  - Lecture/Classroom
  - War Gaming
  - Computer-based, instructor led courses via Web cast sessions

Training Trends

Concerns

Web-based Training - Disadvantages

- Does not allow students to participate in hands on group activities designed to reinforce the instruction
- Students are unable to practice using applications in a test environment with experts on-site to troubleshoot
- Removes the opportunity for interfacing with others in the MHS performing the same functions
- Is not conducive to allowing students to focus on learning when work issues interrupt

Training Trends

Research Shows

- Dave Ulrich, co-author of *The HR Principle*
  - Unlike adolescents who learn by mastering facts and digesting information, adults concentrate on *applying facts and turning information into action.*
  - Adults have already developed cognitive foundations through life experiences, and they're interested in learning how new ideas will help them get what they want rather than accumulating more knowledge.
- On-site experiential learning such as group activities and wargames provide this type of understanding

Training Trends

Research Shows

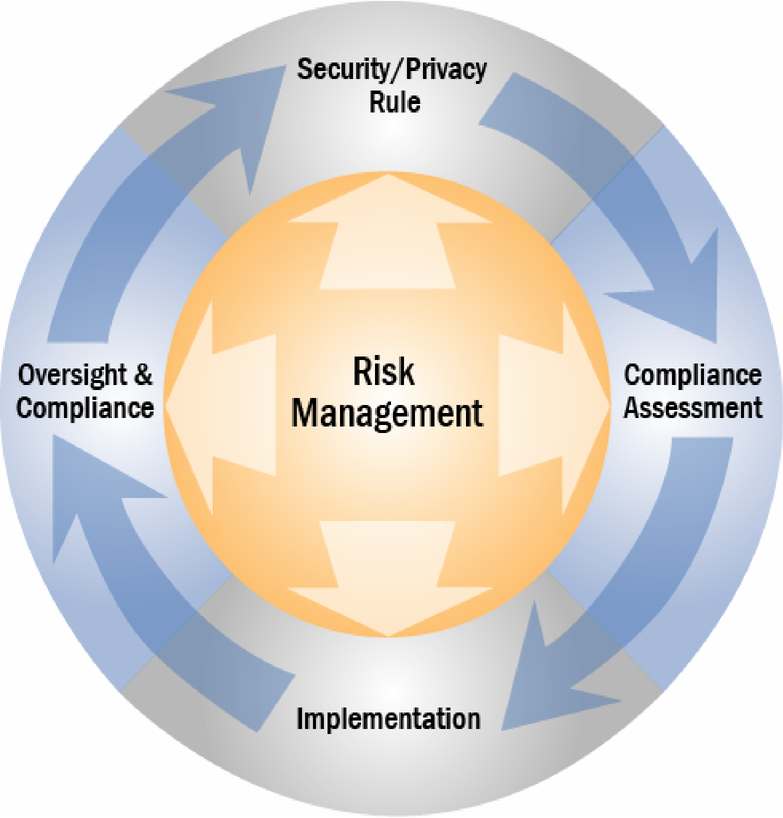
- John Keller, Motivation in cyber learning environments- *Educational Technology International* (1999) outlines the success or failure of any e-learning initiative which can be closely correlated to learner motivation. Mr. Keller encourages content developers to incorporate the ARCS model when designing any program.

- **The John Keller ARCS Model is** the "blueprint" for ensuring that computer-based training is instructionally sound for adult learners. The strategies that incorporate the following into the content:
  - **Attention** – Use graphics and write content that grabs the learner's attention. Provide interactivity (something to do) where appropriate.
  - **Relevance** – Relate the content to the learner's job role or life experiences.
  - **Confidence** – Provide opportunities for the learner to check their understanding
  - **Satisfaction** – Provide opportunities for the learner to receive feedback

Training Trends

Content

- Training is a critical component of the overall risk management plan
  - Training must respond to new socio-cultural trends (ex. increase in telework, mobile computing devices, etc.)
  - Training must address new privacy and security threats ex. medical identity fraud



Training must respond to new socio-cultural trends

Content - Increasing Telework

- Debate about how to count teleworkers continues
  - According to an IDC* study, 8.9 million Americans worked at home for a corporate job at least three days a month in 2004
  - The Industrial and Technology Assistance Corporation (ITAC) estimates 45.1 million Americans worked from home but used different criteria
  - Trending upwards…by all estimates

**Source: http://www.idc.com/about/about.jsp*

Training must address new privacy and security threats

Content - Medical identity fraud

- Privacy Officers need to be prepared to investigate and mitigate medical identity theft along with other violations
- According to a 2003 federal report, at least 200,000 identity theft cases involved medical identity fraud
- The transition from paper-based to electronic records may increase opportunities for medical identity theft
  - Victims may find it more difficult to recover from medical identity theft as medical errors are disseminated and redistributed through computer networks and other medical information-sharing pathways

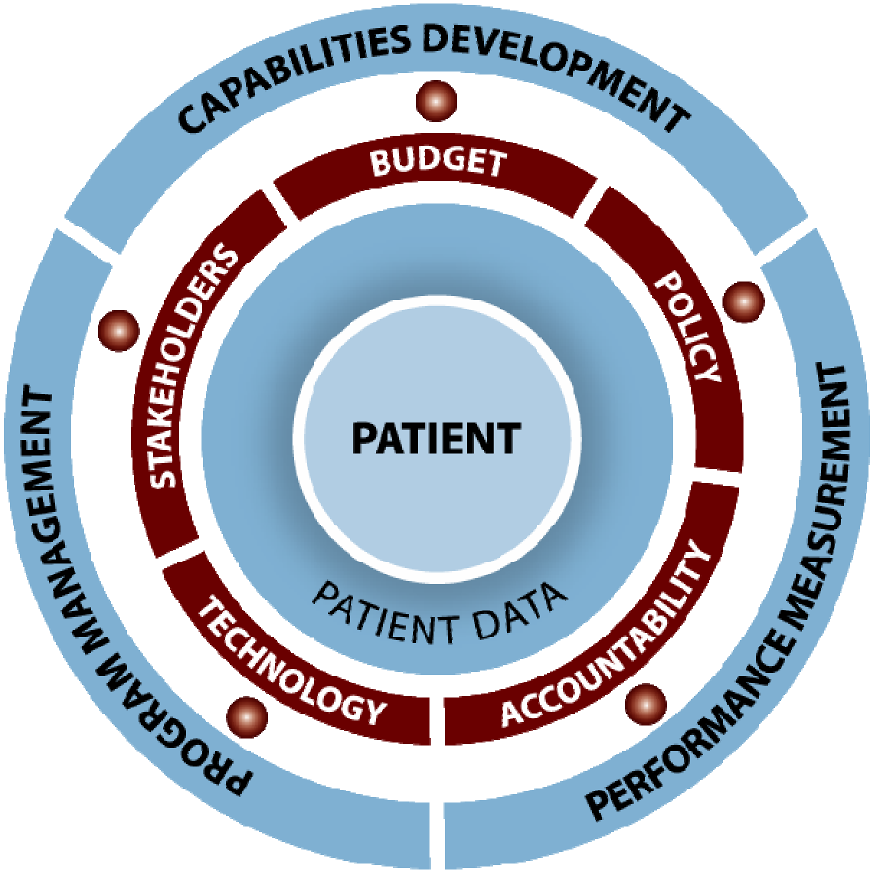
Source: "Medical Identity Theft: The Information Crime That Can Kill You," authored by Pam Dixon.

The Military Health System (MHS) training program is award winning

- MHS received United States Distance Learning Association (USDLA) 21st Century Best Practices Award (2005)
  - This award is given to an agency, institution, or company that has shown outstanding leadership in the field of distance learning
  - MHS was recognized for challenging existing practices by developing new and innovative solutions for distance learning instruction and employee distance learning training programs
- Awarded the ComputerWorld Laureate
  - Nominated by the Chairmen's Committee for visionary applications of IT
  - Promote positive social, economic and educational change

Source: http://www.usdla.org/ and http://www.cwhonors.org/

Summary


CAPABILITIES DEVELOPMENT
PERFORMANCE MEASUREMENT
PROGRAM MANAGEMENT
BUDGET
POLICY
ACCOUNTABILITY
TECHNOLOGY
STAKEHOLDERS
PATIENT
PATIENT DATA

Resources

- TMA Privacy Web Site: www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- TMA Privacy Office: privacymail@tma.osd.mil

THANKS!!!