Presentation for HIPAA Summit X
Baltimore, MD
April 7, 2005

The HIPAA Security Rule: Theory and Practice

Sam Jenkins
Privacy Officer
TRICARE Management Activity (TMA)

Dan Steinberg
Senior Consultant
Booz Allen Hamilton

Theory of the HIPAA Security Rule: Presentation Objectives

- Discuss the flexibility and adaptability of the HIPAA Security Rule
- Review HIPAA covered entities' need for further guidance
- Describe the role of National Institute of Standards and Technology (NIST) in providing security guidance to the federal government
- Provide an overview of NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*
- Describe covered entities' need to apply guidance judiciously

The HIPAA Security Rule was intended to provide covered entities with flexibility and adaptability

- Section 1173(d) of the Act required HHS to “take into account…the needs and capabilities of small and rural health providers”
- HHS relied on basic concepts in drafting the rule that included:
  - Scalability, so that it could be effectively implemented by covered entities of all types and sizes
  - Not be linked to any specific technologies, allowing covered entities to make use of future technology advancements.
- 2,300 comments received reinforced that entities affected by the Security Rule “are so varied in terms of installed technology, size, resources, and relative risk that it would be impossible to dictate a specific solution or set of solutions that would be useable by all covered entities”
- HHS declined to certify software, develop compliance checklists, or certify programs or tools
- Advised covered entities to identify white papers, tools, and recommended best practices, but cautioned that “HHS does not rate or endorse any such guidelines and/or modelsand the value of [their] content must be determined by the user.”

In response to a FAQ, HHS stated that no standard policy, procedure, or methodology can guarantee compliance for all covered entities

- **FAQ 3230:** *How will we know if our organization and our systems are compliant with the HIPAA Security Rule's requirements?*

- **Answer:** Compliance is different for each organization and no single strategy will serve all covered entities. …Compliance is not a one-time goal, it must be maintained. Compliance with the evaluation standard at § 164.308(a)(8) will allow covered entities to maintain compliance. By performing a periodic technical and nontechnical evaluation a covered entity will be able to address initial standards implementation and future environmental or operational changes affecting the security of electronic PHI.

The National Institute of Standards and Technology (NIST) is charged with developing security standards and guidelines for federal agencies

- Under the Federal Information Security Management Act of 2002 (FISMA), NIST is charged with “developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets” apart from national security systems
- NIST is cited four times in the preamble to the HIPAA Security Rule as an authority and potential source for more information on the security management process, evaluation, training programs, and auditing
- NIST’s Computer Security Division (CSD) produces the Special Publication 800 series on information technology security topics of general interest to the computer security community.

NIST's challenge was to assist federal agencies with understanding the HIPAA Security Rule without creating new requirements

- Drafting of Special Publication 800-66 was guided throughout development by our stated intent:
  - *To identify activities relevant to each standard and implementation specification of the HIPAA Security Rule, and provide direction to more extensive guidance.*
- Special Publication states multiple times that this guide is offered as an aid, but does not create new requirements
- Development further governed by the goals of of writing in an accessible, clear style and defining all technical terms
- Written for NIST's audience of federal agencies pursuant to its mandate, but private and commercial entities may voluntarily consult it and adapt it for their purposes
- Not subject to copyright, although attribution to NIST is appreciated.

Special Publication 800-66 discussed HIPAA within a federal framework of other information security requirements and NIST publications

- FISMA directs heads of federal agencies and their chief information officers (CIOs) to:
  - Ensure that each agency has an information security program in place
  - Ensure trained personnel are assigned to manage and support the program
  - Fully integrate security into their business processes
  - Prepare security plans and certification and accreditation for all agency systems.
- NIST developed a suite of publications relevant to addressing these FISMA requirements
- Appendix ("E" of current draft) identifies opportunities for aligning FISMA and HIPAA activities in order to maximize efficiency
- Emphasis throughout document on availability of other NIST publications which address certain security issues in greater detail.

Each administrative, technical, and physical standard was addressed in an educational "module"

Components of each module:

- Citation for the standard
- A reprinting of the exact text of the standard
- Introductory reference
- Key activities
- Description (of key activities)
- Sample Questions
- Supplemental references
- Examples
- Explanation

4.11 Workstation Use (§ 164.310(b))

HIPAA Standard: *Implement policies and procedures that specify the proper functions to be perform*
the manner in which those functions are to be performed, and the physical attributes of the surroundi
of a specific workstation or class of workstation that can access electronic protected health informatio

Key Activities	Description	Sample Questions
Note: This HIPAA Standard does not include any implementation specifications.	**Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapters 15 & 16)*	
1. **Identify Workstation Types and Functions or Uses**	• Inventory workstations and devices. • Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues (see note on workstations at the end of this section). • Classify workstations based on the capabilities, connections, and allowable activities for each workstation used.	• Do we have an inventory of workstation types and locations in my organization? • Who is responsible for this inventory and its maintenance? • What tasks are commonly performed on a given workstation or type of workstation? • Are all types of computing devices used as workstations identified along with the use of these workstations?
2. **Identify Expected Performance of Each Type of Workstation**	• Develop and document policies and procedures related to the proper use and performance of workstations.	• How are workstations used in day-to-day operations? • What are key operational risks that could result in a breach of security?
3. **Analyze Physical Surroundings for Physical Attributes**[70]	• Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts. • Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed.	• Where are workstations located? • Is viewing by unauthorized individuals restricted or limited at these workstations? • Do changes need to be made in the space configuration? • Do employees understand the security requirements for the data they use in their day-to-day jobs?
Supplemental References	• NIST SP 800-14 • NIST SP 800-53	

Each administrative, technical, and physical standard was addressed in an educational "module" (continued)

omponents of each module:

- Citation for the standard
- A reprinting of the exact text of the standard
- Introductory reference
- Key activities
- Description (of key activities)
- Sample Questions
- Supplemental references
- Examples
- Explanation

Key Activities	Description	Sample Questions
Note: This HIPAA Standard does not include ad[illegible]plementation specifications.	**Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapters 15 & 16)*	
1. Identify Workstation Types and Functions or Uses	• Inventory workstations and devices. • Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues (see note on workstations at the end of this section). • Classify workstations based on the capabilities, connections, and allowable activities for each workstation used.	• Do we have an inventory of workstation types and locati in my organization? • Who is responsible for this inventory and its maintenanc • What tasks are commonly performed on a given workstation or type of workstation? • Are all types of computing devices used as workstations identified along with the use of these workstations?
2. Identify Expected Performance of Each Type of Workstation	• Develop and document policies and procedures related to the proper use and performance of workstations.	• How are workstations used in day-to-day operations? • What are key operational risks that could result in a bre of security?
3. Analyze Physical Surroundings for Physical Attributes[i]	• Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts. • Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed.	• Where are workstations located? • Is viewing by unauthorized individuals restricted or limite at these workstations? • Do changes need to be made in the space configuration • Do employees understand the security requirements for data they use in their day-to-day jobs?
Supplemental References	• NIST SP 800-14 • NIST SP 800-53	

Example:

EXLHCP has existing formal Workstation Acceptable Use policy and procedures identifying the proper functions to be performed on workstations. T policy and procedures identify the attributes of the physical surroundings of an information system and the appropriate safeguards to be implemented the workstations. The procedures section also includes guidelines for manual protection of workstations to be practiced by all workforce members. T safeguards are discussed further in the Section 4.12, *Workstation Security*. The entity has determined the existing policy and procedures meet Securit Rule compliance and no revisions are needed (§ 164.310(b)).

Explanation:

The covered entity's decision to use the existing Workstation Acceptable Use policy a permissible way of meeting the requirements of this standard. standard for workstation security at § 164.310(b) requires a covered entity to implement policies and procedures that specify the proper functions and manner in which the functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation th access EPHI. The entity's existing workstation acceptable use policy and procedures identify proper functions to be performed, the attributes of the physical surroundings and appropriate safeguards to be implemented on all information systems, including those with EPHI. If the policy does not m the requirements of § 164.310(b), and thus does not enable the covered entity to comply with the standards or establishes insufficient workstation sec safeguards, the policy must be revised.

Each module begins with an Introductory Reference, and most also include Secondary References at the end of the module table

- Each Introductory Reference is the NIST Special Publication that will be the most informative to a covered entity on the security issue raised by that particular specification
- In some cases, only part of the Introductory Reference will be relevant to that particular standard; users will need to review the document to identify the relevant portion
- Supplemental References may also be helpful; some are written on more general topics than the standard and will provide a context for the standard and/or a background on information security
- A review of all references identified for each standard is provided in Appendix D of Special Publication 800-66.

The Key Activities suggest actions that are usually associated with the security function or functions for each HIPAA Security Rule standard

- In final draft, Key Activities will include all implementation specifications of each standard, and note whether each is “required” or “addressable”
- Other Key Activities are not specifically discussed or required by the HIPAA Security Rule
  - NOT meant to expand upon the intent of the Security Rule, but are usually included in a robust security process
  - Some are required of federal entities under other federal laws, regulations, or procedures.
- Each entity will need to identify what activities are necessary and appropriate in its environment, implement those activities, and document them.

The Description is a description of possible actions to take to address each Key Activity

- Includes an expanded explanation of the Key Activity
- Includes types of activities an organization may pursue in addressing a specific security function
- Abbreviated explanations designed to help get an organization started in addressing the HIPAA Security Rule
- The NIST publications identified as Introductory References for the HIPAA Security Rule can be consulted for more detailed information about the security topic.

Sample Questions are those that covered entities may ask themselves while determining whether Key Activities have been adequately considered or completed

- List of Sample Questions is not exhaustive, but merely representative
- Affirmative answers to these questions do not imply that an organization is meeting all of the requirements of the HIPAA Security Rule
- Negative answers to these questions should prompt the covered entity to consider whether it needs to take further action in order to comply with the standards
- Many organizations with existing information security infrastructure already in place will have considered most of the Sample Questions
- Sample Questions should be tailored to fit the unique circumstances of each entity.

The Examples describe the efforts of two hypothetical federal agencies that are also HIPAA covered entities

- The Examples describe how two hypothetical covered entities has chosen to address standards and implementation specifications of the HIPAA Security Rule
- Should be read in context of the overview of each entity's environmental and information systems characteristics
- The Examples are representative of what actions and issues may arise, but are not comprehensive descriptions of the actions an organization must perform
- The actual activities necessary to implement the standard requirement for any given entity may vary substantially depending on organization mission, size, and scope
- Each Example is followed by an Explanation detailing how the covered entity approached the HIPAA standard, containing references and citations to provisions of the HIPAA Security Rule.

NIST Special Publication 800-66 was intended to be a helpful, educational document

- Explanations of terms and concepts used in the rule
- “Builds a bridge” to other NIST documents that will be helpful in understanding the significance of each standard
- Not a “checklist,” a “methodology” or an “approach,” but a resource
- Individual compliance will require an understanding of security and alignment with the entity's:
  - Risk analysis
  - Risk mitigation strategy
  - Security measures already in place
  - Cost of implementation of particular security measures
  - Size, complexity, capabilities
  - Technical infrastructure, hardware, and software capabilities
  - Probability and criticality of potential risks to electronic protected health information
  - Other factors.

HEALTH AFFAIRS

Practice of the HIPAA Security Rule: Presentation Objectives

TRICARE Management Activity

- Provide overview of Military Health System (MHS) scope and structure as they relate to HIPAA
- Relate where the Military Health System is now in their compliance efforts
- Provide the steps and timeline for HIPAA compliance
- Review lessons learned

HEALTH AFFAIRS

Background

TRICARE Management Activity

- Department of Defense (DoD) MHS mission and care environments
  - Complex organizational structure
  - Treats both military personnel and civilian family members, retirees and others
  - Variety of settings - military and civilian treatment facilities
  - Echelons of care - deployed and non-deployed
    - Specialty and multi-service
    - Community hospitals
    - Clinics
    - Operation and deployed units

HEALTH AFFAIRS

TRICARE Management Activity

Compliance Date

- April 20, 2005
- Only 13 days from today…

Where are we now and how did we get here

Major milestones for HIPAA Security Implementation	2000	2001	2002	2003	2004				2005	
					1qtr	2 qtr	3 qtr	4 qtr	1qtr	2 qtr
OCTAVE tool development 1st Quarter 2000	■	■								
P3WG kick off March 2000 finished April 2003	■	■	■	■						
MISRT formation and initial training		■								
WIPT/IPT formation January 2002			■							
OCTAVE training		■	■							
Final Rule published Feb 2003				■						
IPT development of prgm and implementation products				■	■	■	■	■	■	■
Appoint CE HIPAA Security Officers						■				
Attend Security Officer Training							■			
Train workforce on HIPAA Security							■	■	■	■
HIPAA Security Awareness Campaign Kick-Off								■	■	■
Conduct Organizational Risk Assessments (OCTAVE)						■	■	■	■	
Conduct compliance gap analysis (HIPAA Basics)							■	■	■	
Develop and implement mitigation plan							■	■	■	
Evaluation									■	
Oversight and Compliance								■	■	■
Compliance date April 20, 2005										■

HEALTH AFFAIRS

TRICARE Management Activity

The key to compliance is risk management

- To correctly implement the security standards and establish compliance, each covered entity must:
  - Assess potential risks and vulnerabilities to EPHI
  - Develop, implement, and maintain appropriate security measures given those risks
  - Document those measures and keep them current

Implementing HIPAA Security is meant to be

flexible and scalable

HEALTH AFFAIRS

TRICARE Management Activity

Preparation prior to final rule

- Development and selection of Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE©) as risk assessment methodology
- DoD and Service level policy gap analysis
- Integrated Process Team and Medical Information Security Readiness Team (MISRT) formation
- Initial training in HIPAA and OCTAVE©

HEALTH AFFAIRS

TRICARE Management Activity and Service Implementation Actions

TRICARE Management Activity

- Development of HIPAA Security Program and Strategy
  - Program Management Plan
  - Training and Awareness Program
  - Policy development (Directive, Regulation and Implementation Guides)
  - Oversight and Compliance (Compliance Assurance Framework, Compliance and reporting tools)
  - Incident Response

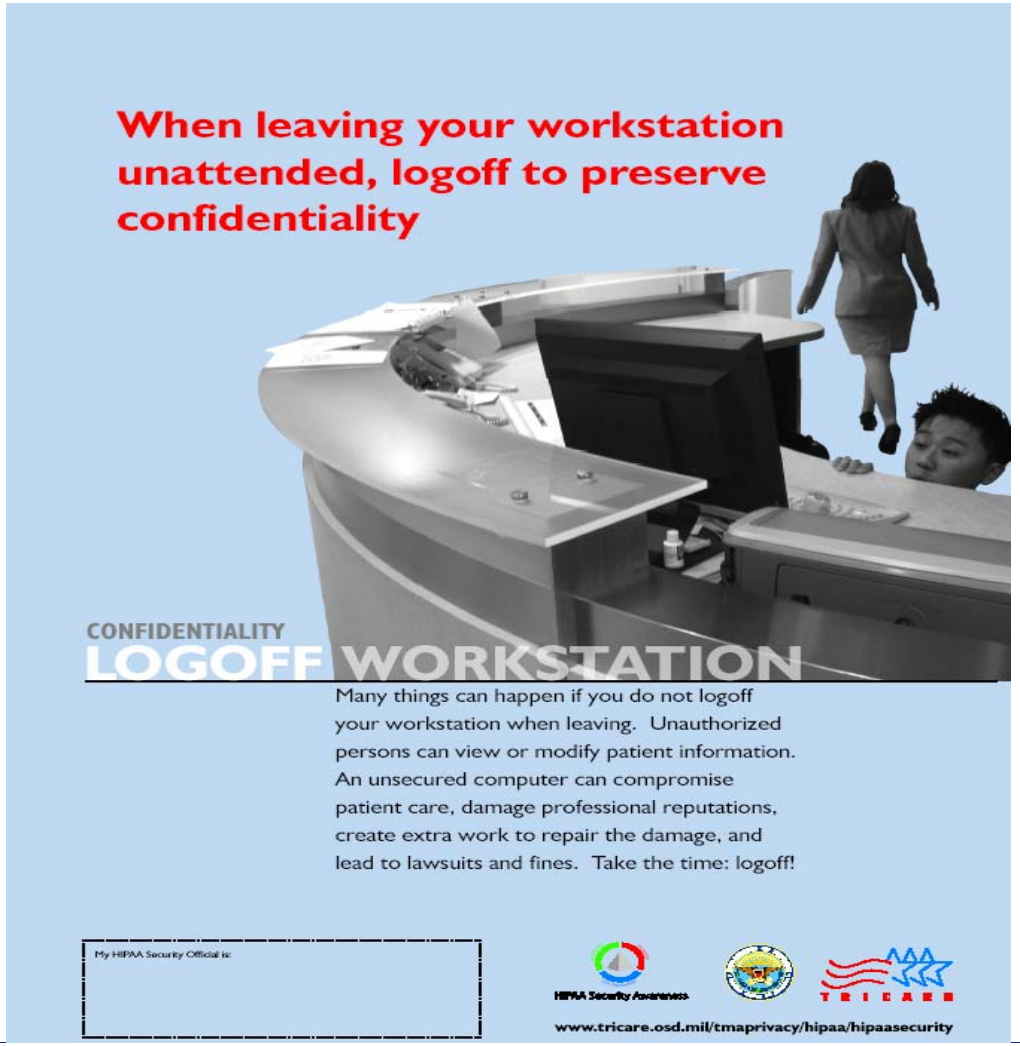
HEALTH AFFAIRS

Military Treatment Facility Implementation Actions

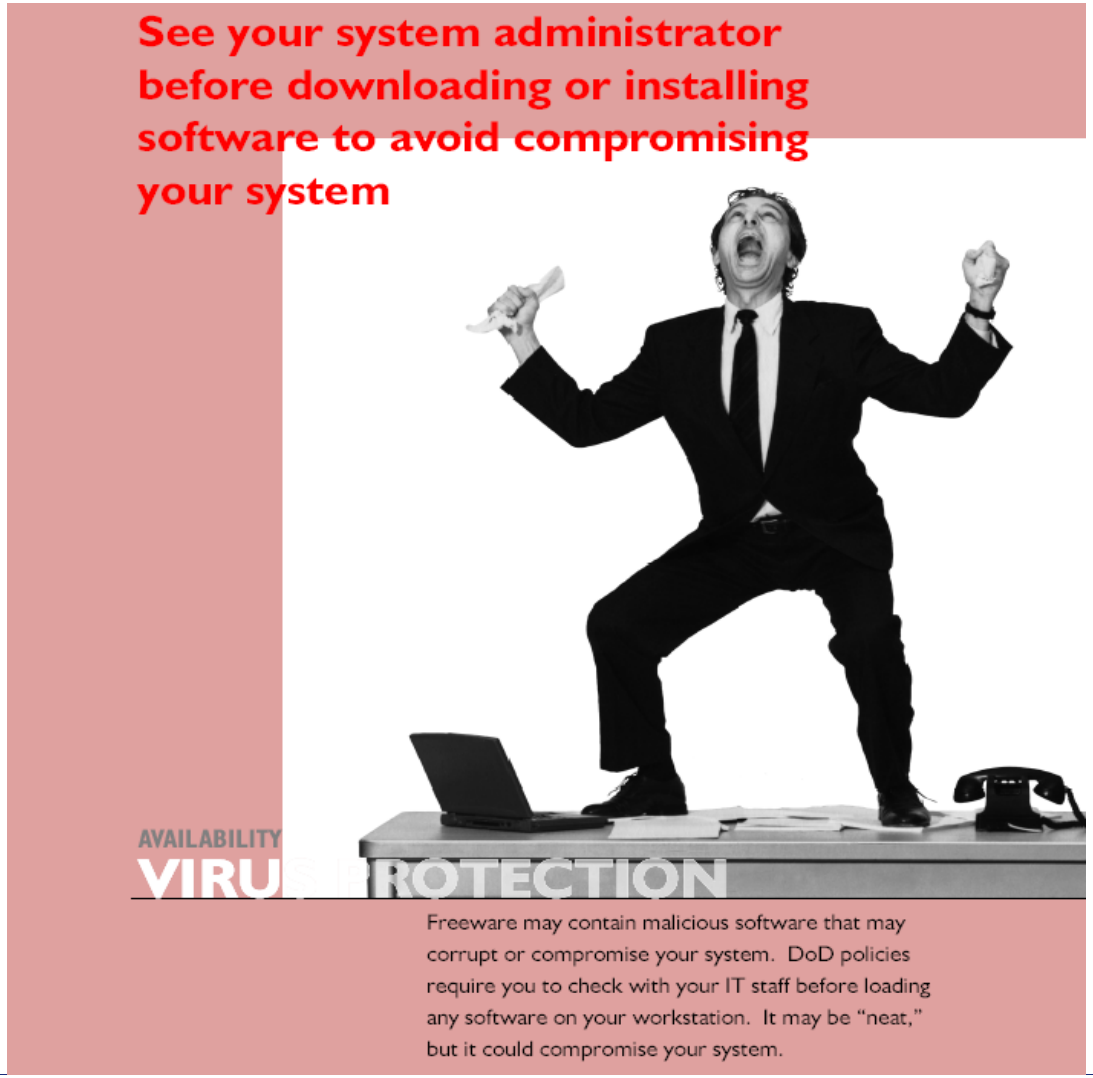
TRICARE Management Activity

- Implementation of treatment facility HIPAA Security Program
  - Appointment of Security Official and MISRT
  - Workforce training and awareness program
  - Perform HIPAA risk assessment
  - Perform HIPAA compliance gap analysis
  - Mitigation plans
  - Implementation strategies
  - Evaluation and documentation

HIPAA Security Awareness Posters (1 of 3)



HIPAA Security Awareness Posters (2 of 3)



HIPAA Security Awareness Posters (3 of 3)

HEALTH AFFAIRS

Oversight and Compliance (1 of 2)

TRICARE Management Activity

- Compliance is established and maintained by implementing business practices including measurement against metrics and periodic reports through an appropriate reporting structure
  - Measuring success
  - Completion percentages
  - Identifying areas for improvement
  - Preparations and contingencies
  - Communication of issues

HEALTH AFFAIRS

Oversight and Compliance (2 of 2)

TRICARE Management Activity

- Methodologies
  - Initial requirements

    Reports that provide information on compliance within organizations and across the Military Health System

    Metrics to gauge compliance performance and monitor the progress of HIPAA privacy and security programs

HEALTH AFFAIRS

Reporting Requirements

TRICARE Management Activity

- Type and frequency:
  - Training Reports

    Monthly or as needed to verify compliance
  - Compliance Reports

    Baseline for HIPAA Security and then monthly during the implementation phase (December 2004 - TBD)

    Phased decrease to a quarterly or less often report for HIPAA Security Compliance after implementation phase

HEALTH AFFAIRS

Tools for Compliance Reporting

TRICARE Management Activity

- TRICARE Management Activity has provided 2 centrally funded and managed HIPAA Security tools to facilitate compliance reporting efforts across the Military Health System
  - Training Tool

    Plateau's Learning Management System (**LMS**)
  - Compliance Tool

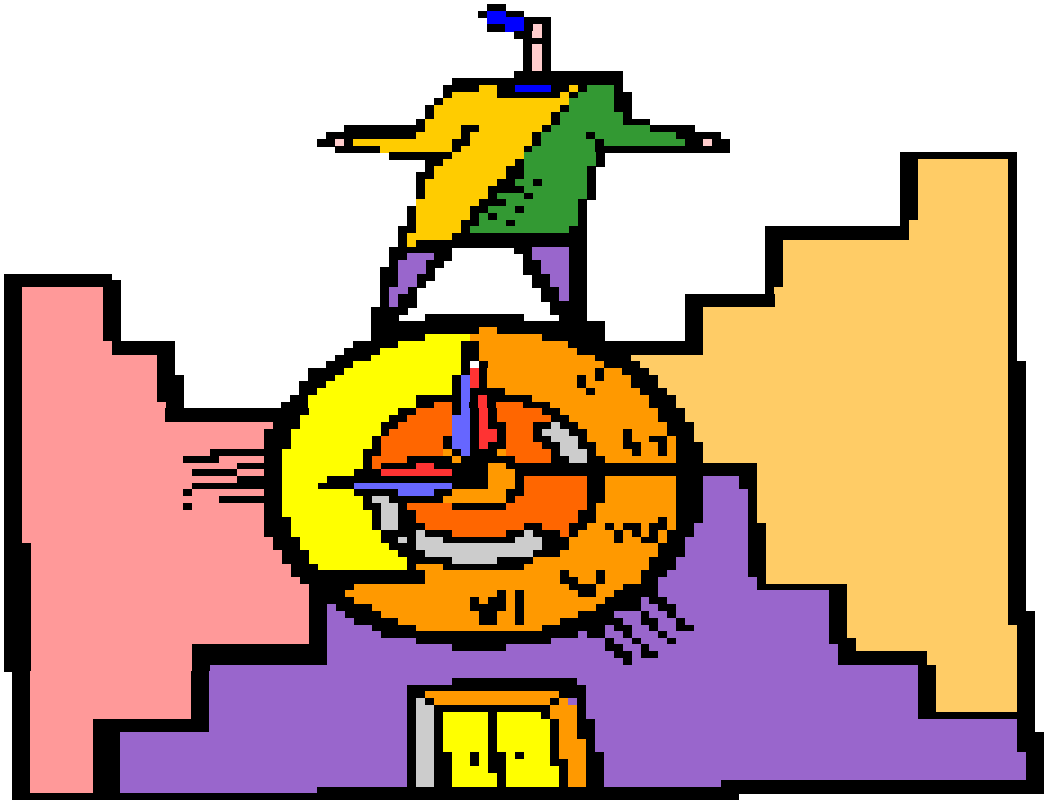
    Strategic Management Systems, Inc **HIPAA BASICS** ™

HEALTH AFFAIRS

TRICARE Management Activity

Are You Ready?

- Remember - compliance is required by every covered entity in 13 days …



HEALTH AFFAIRS

TRICARE Management Activity

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- *Special Publication 800-66: An Introductory Resource Guide for Implementing the HIPAA Security Rule*, National Institute of Standards and Technology available at http://crsc.nist.gov/publications/draft/DRAFT-sp800-66.pdf
- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm

For TMA Healthplan, DoD, and Uniformed Service use only

- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA security representatives

HEALTH AFFAIRS

TRICARE Management Activity

Our Commitment

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.