TRICARE Europe Council (TEC)

HIPAA Privacy and Security: Current Status, Current Risks

Privacy Act & Health Insurance Portability and Accountability Act (HIPAA)

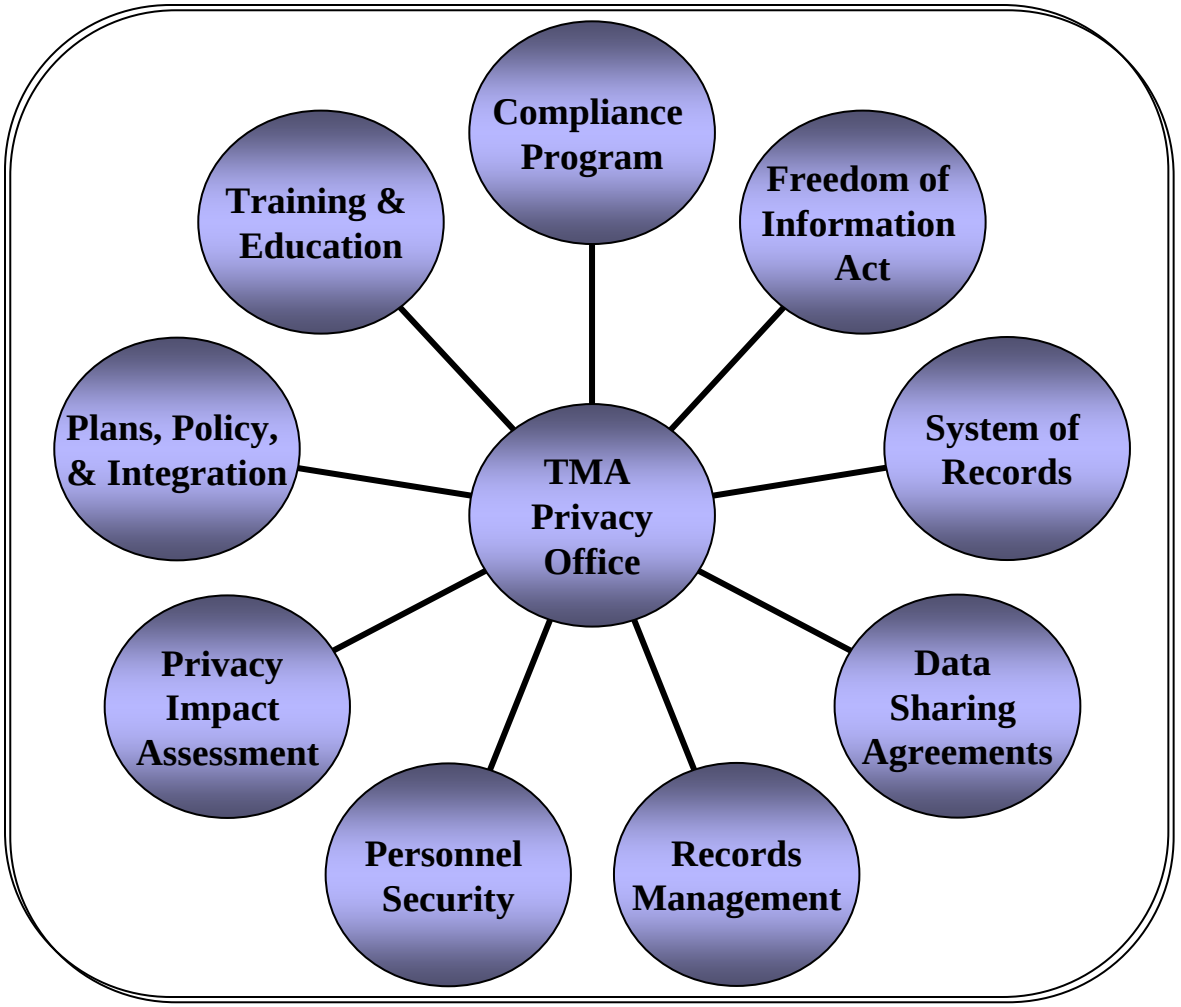
Director, TMA Privacy Office

The Vulnerability of Private Information

The use of this video is to raise awareness surrounding the privacy of personal information. The TMA Privacy Office does not endorse or support the views expressed by the maker of this video, the American Civil Liberties Union (ACLU).

Mission of the TMA Privacy Office

To ensure stakeholders' personally identifiable and protected health information are safeguarded at the highest level as TRICARE delivers the best medical support possible to all those entrusted to our care.



Military Health System Oversight

Federal Laws

- Freedom of Information Act of 1966
- Privacy Act of 1974
- Computer Security Act of 1987
- 44 USC Ch. 31 Records Management Program
- Health Insurance Portability and Accountability Act of 1996:
  - Privacy Rule
  - Security Rule
- E-Government Act of 2002
- Federal Information Security Management Act (FISMA)

DoD Governance

- DoD 5400.7-R DoD Freedom of Information Act Program
- DoD 5400.11-R DoD Privacy Program
- DoD 5200.1-R Information Security Program
- DoD 8580.02-R DoD Health Information Security Regulation
- DoD 6025.18-R DoD Health Information Privacy Regulation
- DoD CIO Memo Privacy Impact Assessments (PIA) Guidance
- ASD(HA) Memo Breach Notification Reporting for the MHS
- DoDI 8510.01 DIACAP (C&A)
- DoD 8500.1 & 2 Information Assurance (IA)

Types of Data

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)

Reporting Requirements

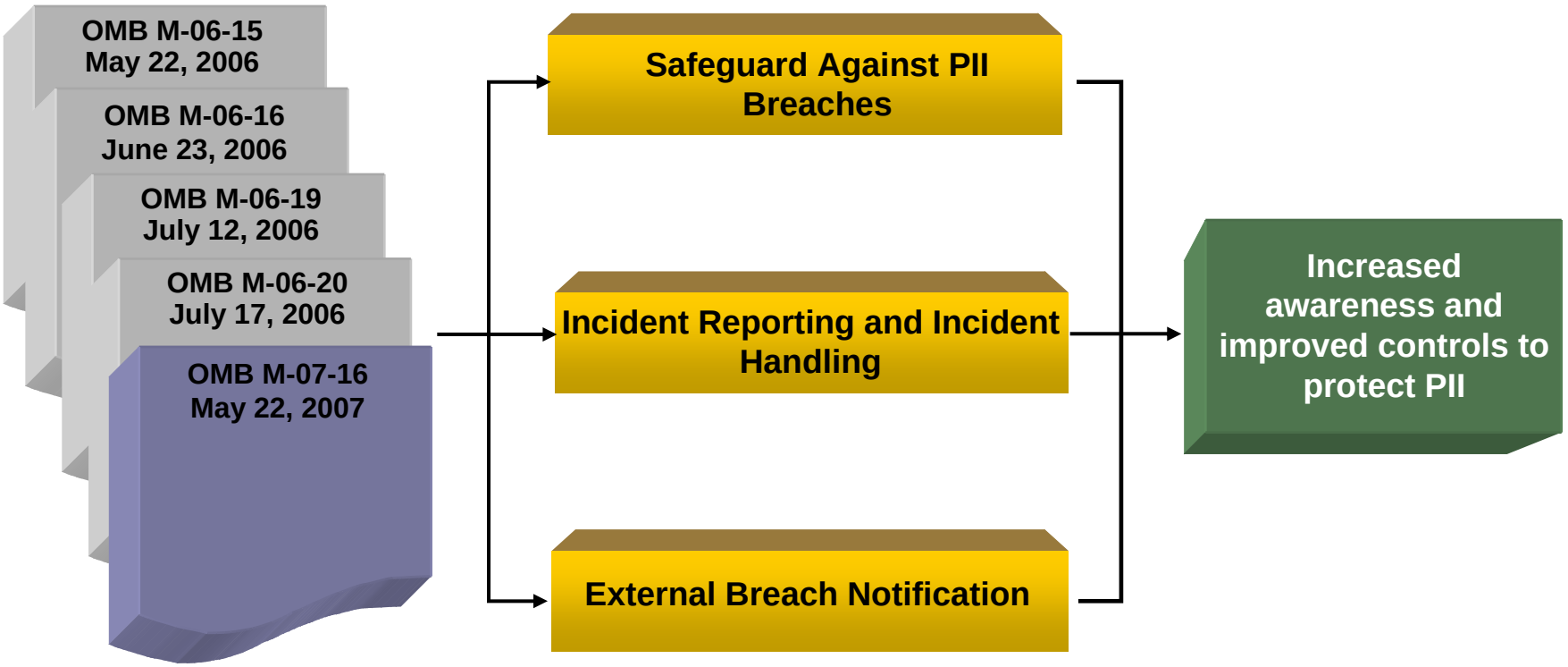
- Congress
- Office of Management and Budget (OMB)
- US-CERT (Computer Emergency Response Team)
- Dept of Health and Human Services (HHS)
- Assistant Secretary of Defense (Networks & Information Integration)
- DoD Inspector General (IG)
- DoD Privacy Office

OMB Memos on Safeguarding PII

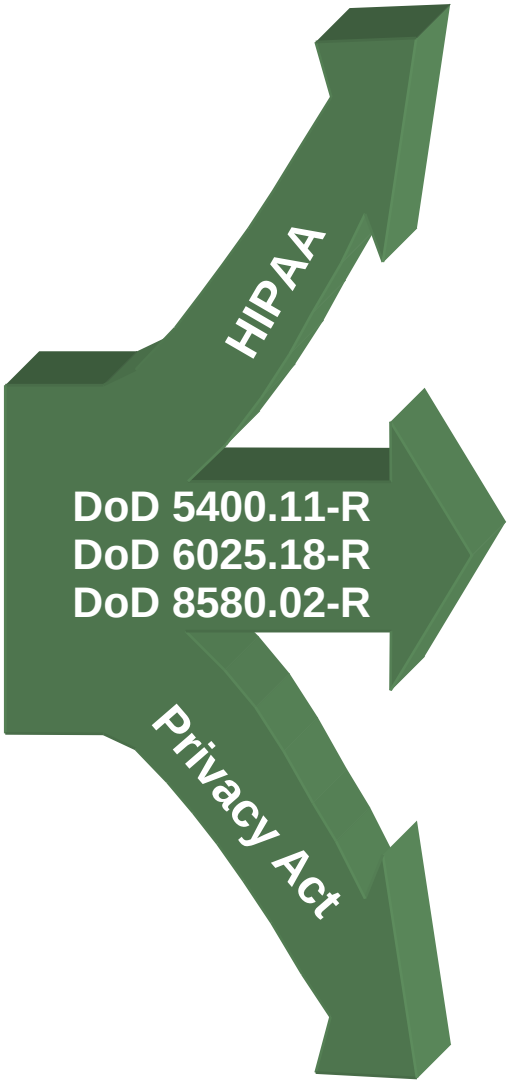
OMB has issued requirements…

… focused on protection of Personally Identifiable Information (PII), handling breaches and notification…

… to safeguard against and respond to PII breaches



Foundation



Enacted to safeguard and regulate protected health information in any media, specifically through the HIPAA Privacy and Security Rules. Requirements include that PHI is properly protected and is not inappropriately disclosed.

DoD 5400.11-R (DoD Privacy Program), DoD 6025.18-R (DoD Health Information Privacy Regulation), and DoD 8580.02-R (DoD Health Information Security Regulation) provide further guidance on implementing both the Privacy Act and HIPAA.

Enacted to safeguard individual privacy contained in Federal records. The Act requires Federal agencies to comply with Federal laws on collecting, maintaining, using, and disseminating information from personal records owned and held by Federal agencies.

Sensitive Information (SI) Categories

Personally Identifiable Information (PII)

Information which can be used to distinguish or trace an individual's identity, including personal information which is linked or linkable to a specified individual

Protected Health Information (PHI)

Information that is created or received by a Covered Entity and relates to the past, present, or future physical or mental health of an individual; providing or payment for healthcare to an individual; and can be used to identify the individual

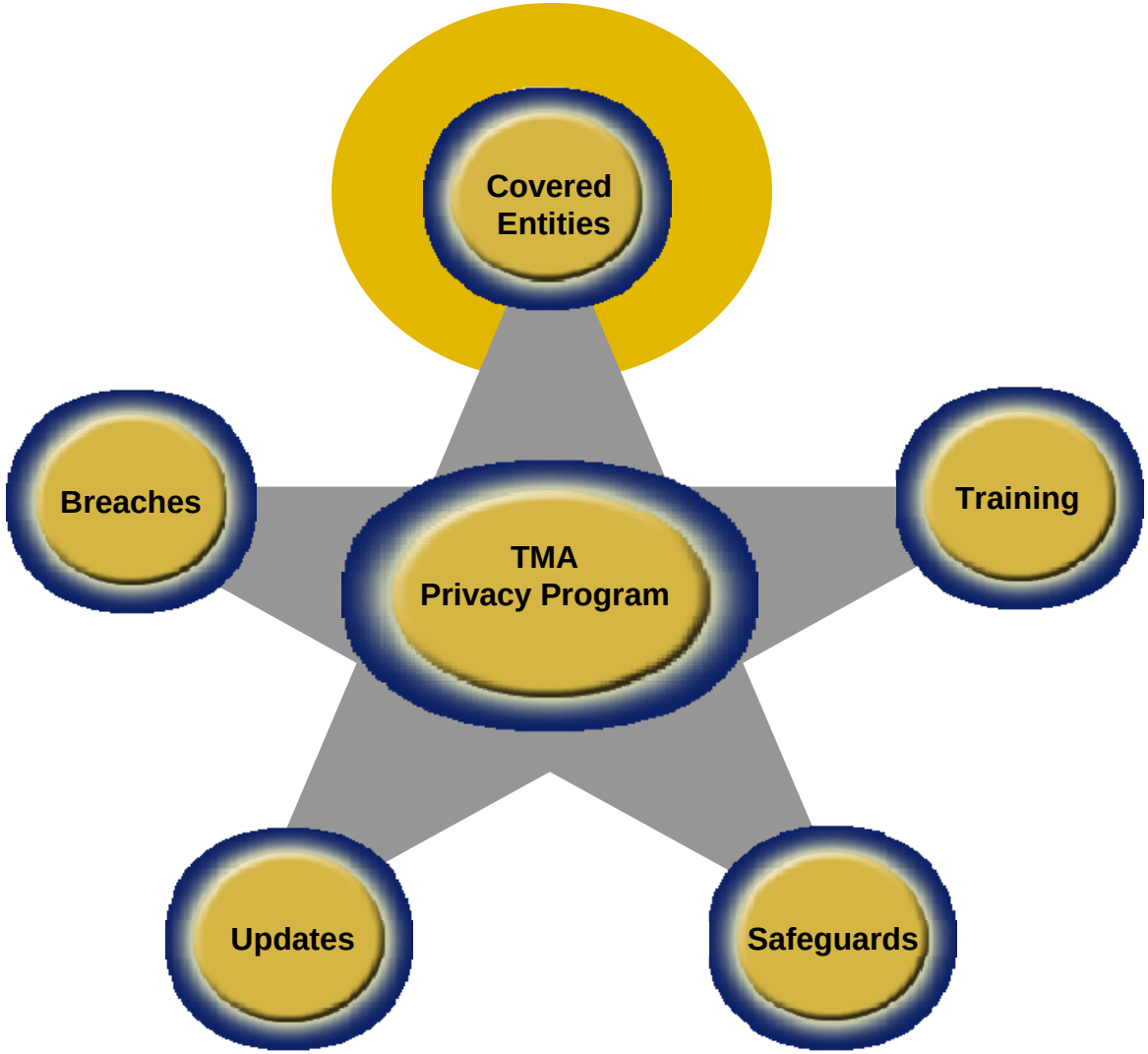
Electronic Protected Health Information (ePHI)

Protected Health Information that is transmitted by or maintained in electronic media

Examples

- Name
- Social Security Number
- Age
- Date and place of birth
- Mother's maiden name
- Biometric records
- Marital status
- Military Rank or Civilian Grade
- Race
- Salary
- Home/office phone numbers
- Other personal information which is linked to a specific individual (including Health Information)
- Electronic mail addresses
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Claim form
- Electronic claim form

Covered Entities



HIPAA Privacy and Security Rules

Privacy Rule
(DoD 6025.18-R)

- Regulates how covered entities (CEs) use and disclose PHI
- Limits use and release of health records
- Establishes safeguards to protect the privacy of PHI
- Holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights
- Enables patients to find out how their information may be used and what disclosures of their information have been made
- Limits release of information
- Grants patients the right to obtain a copy of their health records and request corrections

Security Rule
(DoD 8580.02-R)

- Addresses the implementation of Administrative, Physical, and Technical Safeguards to protect the confidentiality, integrity, and availability of data
- Implementation specifications support specific standards
- May be “required” or “addressable”
- Required means that covered entities must carry out the implementation specification at their facility
- Addressable means that covered entities must carry out the implementation specification if it is reasonable and appropriate

Covered Entities

HIPAA Allowable Disclosures

Disclosures are allowed:

- To the individual
- With an individual's valid written authorization
- For treatment, payment, and health care operations (TPO)

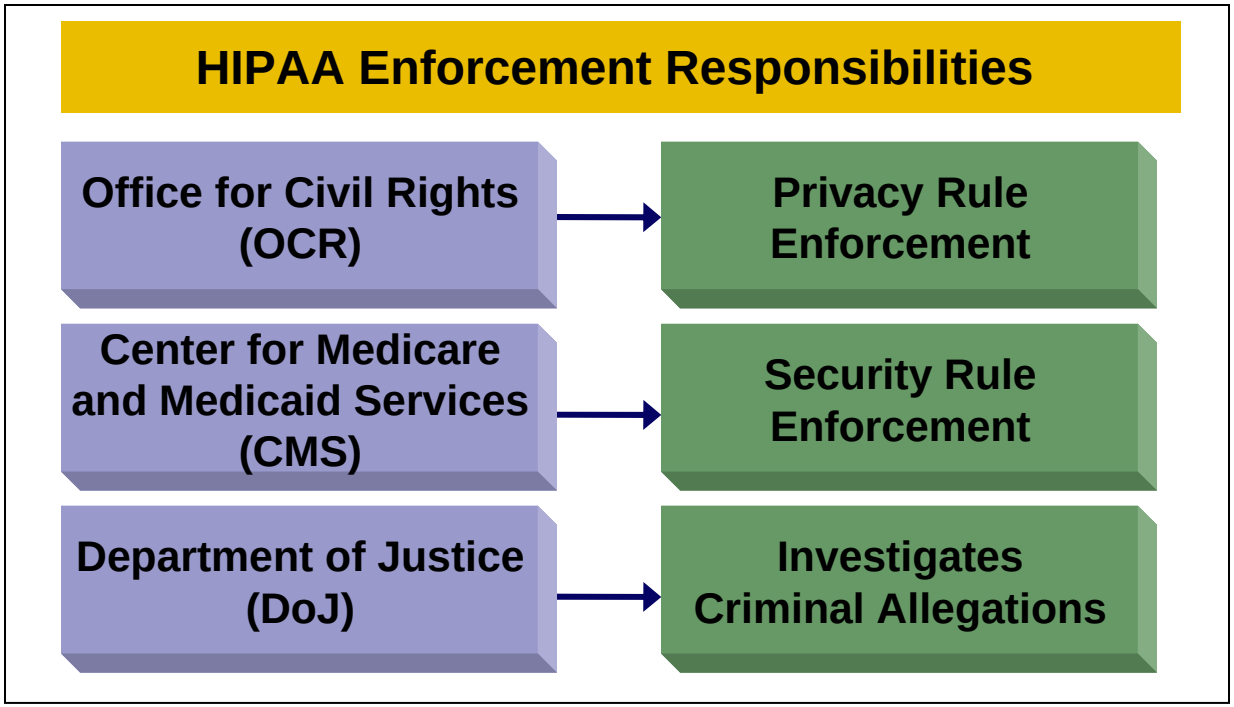
14 Allowable Disclosures that Require Accounting under HIPAA	
■ When required by law or government regulations ■ For public health purposes ■ For medical facility patient directory ■ About inmates in correctional institutions or in custody ■ About victims of abuse or neglect ■ For health oversight activities authorized by law ■ For judicial or administrative proceedings	■ For law enforcement purposes ■ Concerning decedents in limited circumstances ■ For cadaver organ, eye, or tissue donation purposes ■ For research involving minimal risk ■ To avert a serious threat to health or safety ■ For specialized government functions, including certain activities relating to Armed Forces personnel ■ For workers' compensation programs

Disclosures to Military Personnel

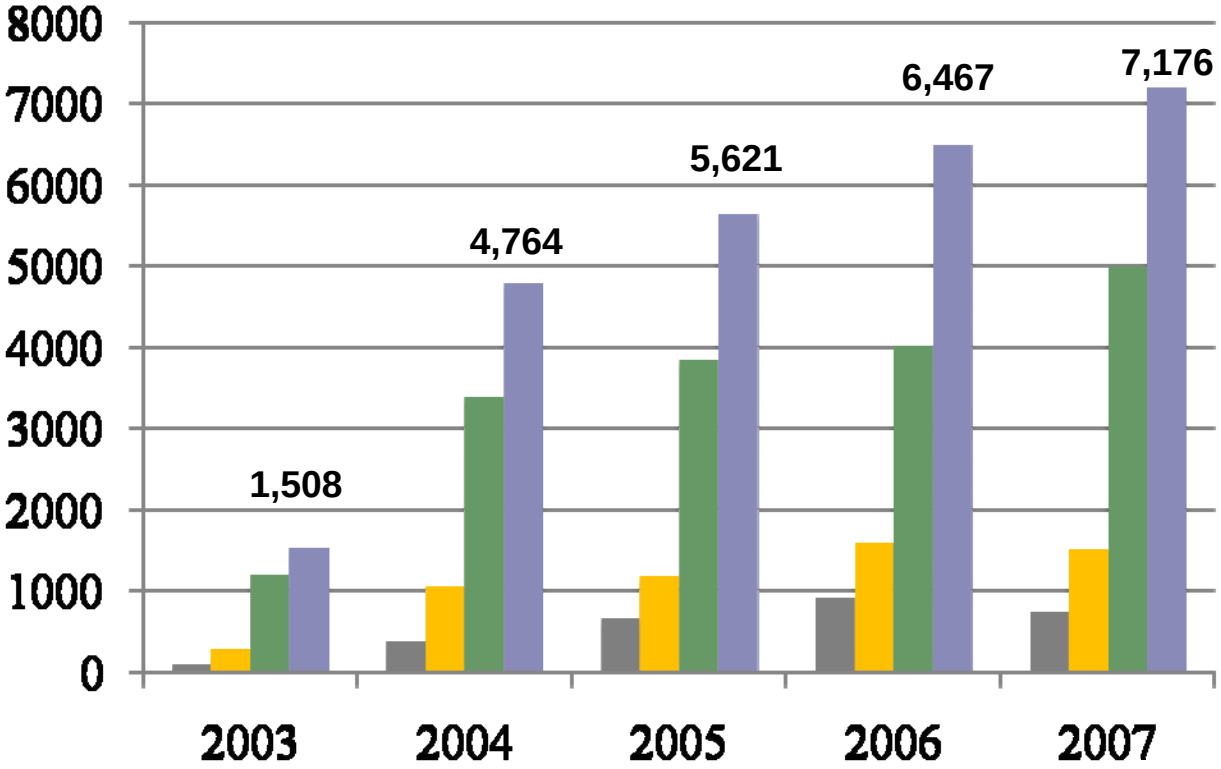
- HIPAA allows for the use and disclosure of PHI of Armed Forces personnel for activities deemed necessary by appropriate Military Command Authorities to assure execution of the military mission.*
- Appropriate Military Command Authorities include:
  - All Commanders who exercise authority over an individual or other person designated by a Commander to receive PHI
  - The Secretary of Defense or the Secretary of the military department for which the individual is a member or any official delegated authority by the Department of Homeland Security for the Coast Guard
- Disclosures of PHI may occur to ensure personnel are able to execute military missions:
  - To determine the member's fitness to perform
  - To report on casualties in any military operation or activity
  - To carry out any other activity necessary to the proper execution of the mission of the Armed Forces
- Disclosures will be documented in the Protected Health Information Management Tool (PHIMT)

*HIPAA only applies to the United States and to the Military Treatment Facilities (MTFs) operated in foreign countries. At MTFs operated by the Military Health System (MHS) in foreign countries, a foreign citizen who is a member of the MHS and who violates privacy standards will be dealt with under the laws of the Host Country.

Tracking HIPAA Complaints



HHS Resolutions by Year & Type: 4/14/03 through 12/31/07



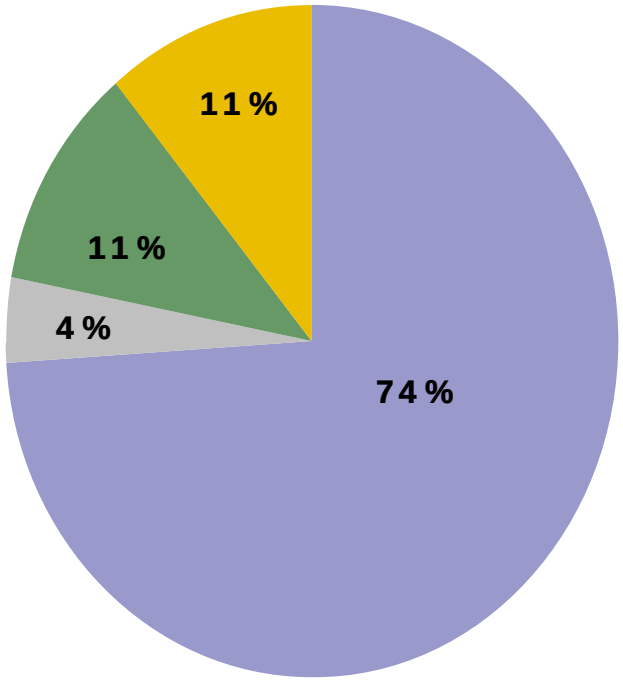
Top Five Issues with Corrective Action	2003	2004	2005	2006	2007
	Impermissible Uses & Disclosures	Impermissible Uses & Disclosures	Impermissible Uses & Disclosures	Impermissible Uses & Disclosures	Impermissible Uses & Disclosures
	Safeguards	Safeguards	Safeguards	Safeguards	Safeguards
	Access	Access	Access	Access	Access
	Minimum Necessary	Minimum Necessary	Minimum Necessary	Minimum Necessary	Minimum Necessary
	Training	Mitigation	Mitigation	Complaints to CE	Notice

HIPAA Complaints
Fiscal Year 2008 (Through September)

TMA Privacy Office coordinated the investigation of 27 complaints to date

Complaints were filed because of:

- Unauthorized disclosures of PHI – 20 (74%)
- Failure to recognize patient request for rights – 3 (11%)
- Failure to have or follow safeguards – 3 (11%)
- Lack of Workforce Training – 1 (4%)



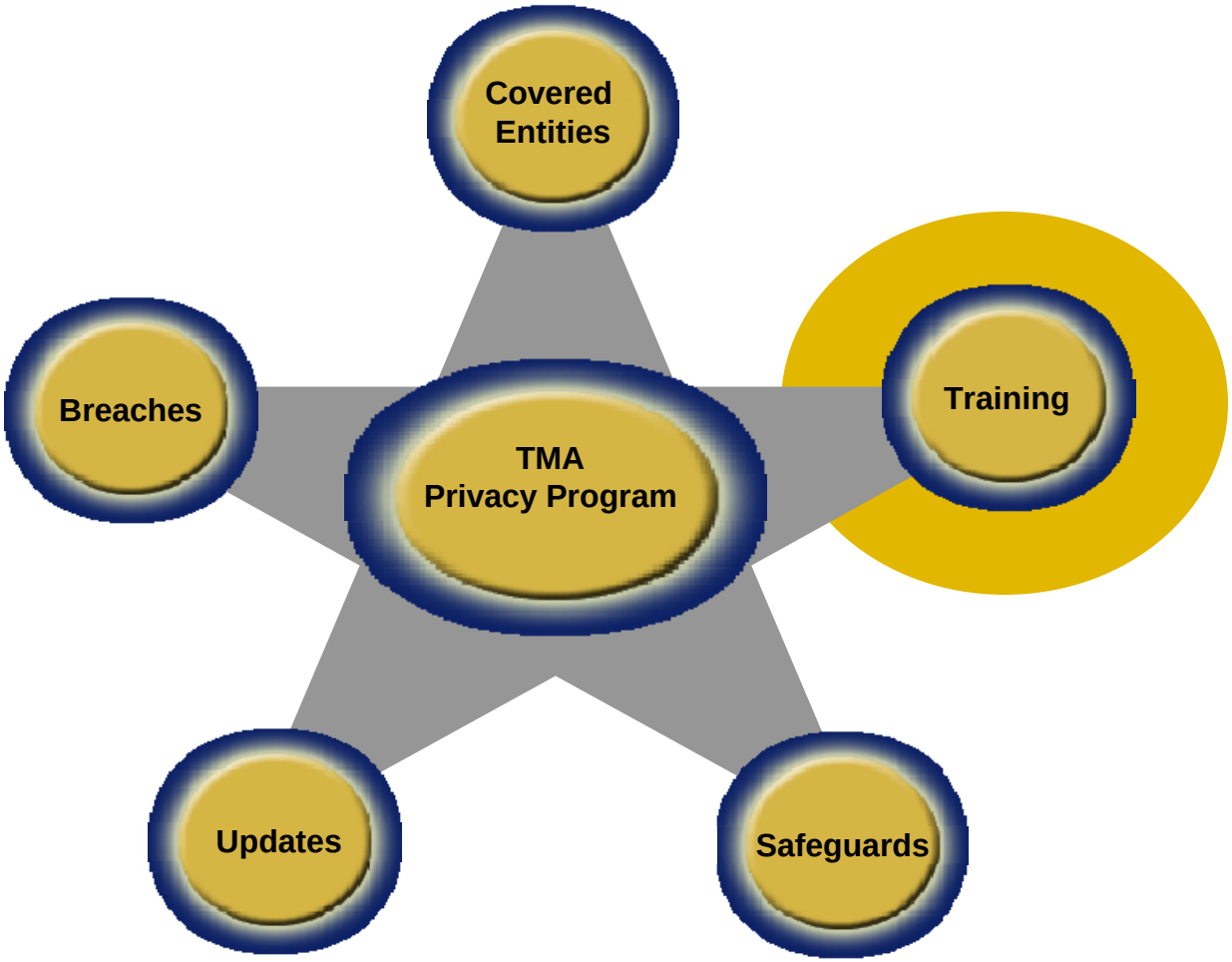
Scenario

HIPAA Privacy Rule

A psychiatrist disclosed an officer's protected health information to commanding authorities for the purpose of determining the member's fitness to perform any particular mission, assignment, order, or duty. The psychiatrist also had several additional phone conversations with the commanding officer. The officer filed a complaint with Health and Human Services, Office of Civil Rights, claiming the psychiatrist violated his HIPAA rights by talking with his commanding authorities.

Did the psychiatrist violate DoD 6025.18-R?

Training


Covered Entities
Breaches
TMA Privacy Program
Training
Updates
Safeguards

Training

In addition to mandatory HIPAA training…

DoD 5400.11-R & "Donley Memo"*

Training is:

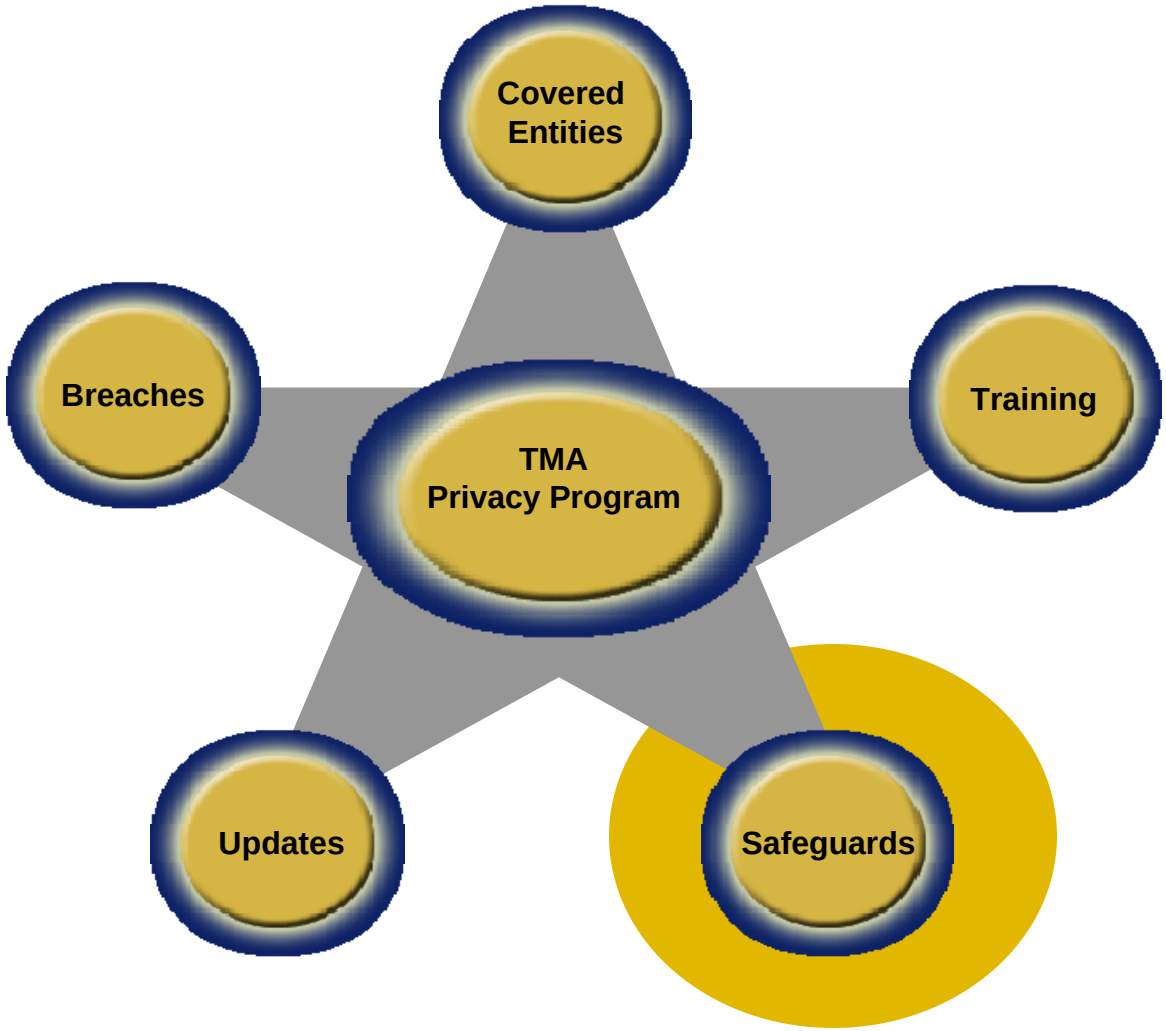
- Mandatory for affected DoD military personnel, employees, managers, and contractors or business partners
- A prerequisite **before** an employee, manager, or contractor is permitted to access DoD systems
- Must be job-specific and commensurate with an individual's responsibilities

Training

- Orientation
- Specialized Training or Role-Based Training
- Management
- System of Records
- Refresher Training

* September 21, 2007 DoD memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"

Safeguards


Covered Entities
Breaches
Training
TMA Privacy Program
Updates
Safeguards

Safeguards

Security Safeguards

- DoD 5400.11-R, “DoD Privacy Program”
- DoD 6025.18-R, “DoD Health Information Privacy Regulation”
- DoD 8500.02, “Information Assurance Implementation”
- DoD 8580.02-R, “DoD Health Information Security Regulation”

Administrative

- ❑ Security Management Process
- ❑ Assigned Security Responsibility
- ❑ Workforce Security
- ❑ Information Access Management
- ❑ Security Awareness and Training
- ❑ Security Incident Procedures
- ❑ Contingency Plan
- ❑ Evaluation
- ❑ Business Associates and Contractors

Physical

- ❑ Facility Access Controls
- ❑ Workstation Use
- ❑ Workstation Security
- ❑ Device and Media Controls

Technical

- ❑ Access Controls
- ❑ Audit Controls
- ❑ Person / Entity Authentication
- ❑ Transmission

Safeguards

Data Sharing Agreements Updates and Enhancements

Draft

1 Agreement to Protect Sensitive De-Identified Data

- Recipient is not regulated by DoD 6025.18-R
- De-identified data
- Data contains sensitive information

2 Data Use Agreement

- Recipient is not regulated by DoD 6025.18-R
- "Limited data set"
- For research, public health, or healthcare operations

3 Business Associates Agreement

- Recipient is not regulated by DoD 6025.18-R
- Is not a provider that needs the information for treatment purposes
- Protected Health Information (PHI)
- Needs the information to provide a service to TMA or MHS

4 Systems Maintenance and Operations Agreement

- Recipient is a contractor that provides maintenance and/or operations to an MHS system
- PHI
- Must also include BAA provisions

5 Agreement for the Disclosure of De-identified Data for Quality Assurance Purposes

- De-identified data
- For quality assurance purposes per DoD 6025.13-R
- TMA tracks disclosures made in this regard

6 Research Disclosure Agreement

- To a researcher
- PHI
- For purposes consistent with the regulation (e.g., Institutional review board (IRB) approved studies, surveys, etc.)

7 Computer Matching Agreements

- PII
- Records from Federal personnel or payroll system of records
- Matching programs involving Federal benefit programs (e.g., eligibility for benefits, payment recovery)

Data Sharing Agreement Formats *(continued)*

- Formalized Agreement
  - Between DoD and external, non-government organizations
- Memorandum of Agreement (MOA)
  - Between DoD and external government agencies
- Memorandum of Understanding (MOU)
  - Within the DoD
- Data Use and Reciprocal Support Agreement (DURSA)
  - Between participating health information exchange organizations (a multi-party agreement)

De-Identified PHI

De-identified PHI is data that ***excludes*** the following **18** categories of direct identifiers of the individual or of relatives, employers, or household members of the individual:

De-Identified PHI	
▪ Names ▪ All geographic subdivisions smaller than a State ▪ All elements of dates (except year) ▪ Telephone numbers ▪ Fax numbers ▪ Electronic mail addresses ▪ Social Security Numbers ▪ Medical Record numbers ▪ Account numbers ▪ Health plan beneficiary numbers ▪ Certificate or license numbers	▪ Internet protocol (IP) address ▪ Device identifiers and serial numbers ▪ Web universal resource locators (URLs) ▪ Biometric identifiers, including finger and voice prints ▪ Vehicle Identification Numbers and License Plate Numbers ▪ Full-face photographic images and comparable images ▪ Any other unique, identifying characteristic or code, except as permitted for re- identification in the HIPAA Privacy Rule

Limited Data Set (LDS)

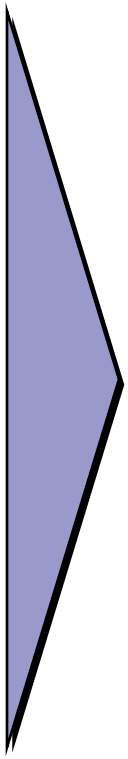
A limited data set is PHI that ***excludes*** the following **16** categories of direct identifiers of the individual or of relatives, employers, or household members of the individual:

PII Direct Identifiers	
▪ Names ▪ Address other than town, city, state, and zip code ▪ Telephone numbers ▪ Fax numbers ▪ Electronic mail addresses ▪ Social Security Numbers ▪ Medical Record numbers ▪ Account numbers ▪ Health plan beneficiary numbers ▪ Certificate/license numbers	▪ Vehicle identifiers and serial numbers, including license plate numbers ▪ Device identifiers and serial numbers ▪ Web universal resource locators (URLs) ▪ Internet protocol (IP) address ▪ Biometric identifiers, including finger and voice prints ▪ Full-face photographic images and comparable images

Privacy Impact Assessments (PIAs)

What is a PIA?

- Analysis of how personally identifiable information (PII) is handled and protected in an Information Technology (IT) system
  - PII includes both personal and protected health information
- Required by the E-Gov Act section 208, for all systems which maintain PII



Why is a PIA conducted?

- To assess risks and mitigate potential risks
- To ensure that systems conform to privacy requirements
- To ensure accountability
- To ensure that PII maintained in the system is properly protected
- To document privacy protection in place

System of Records Notice (SORN)

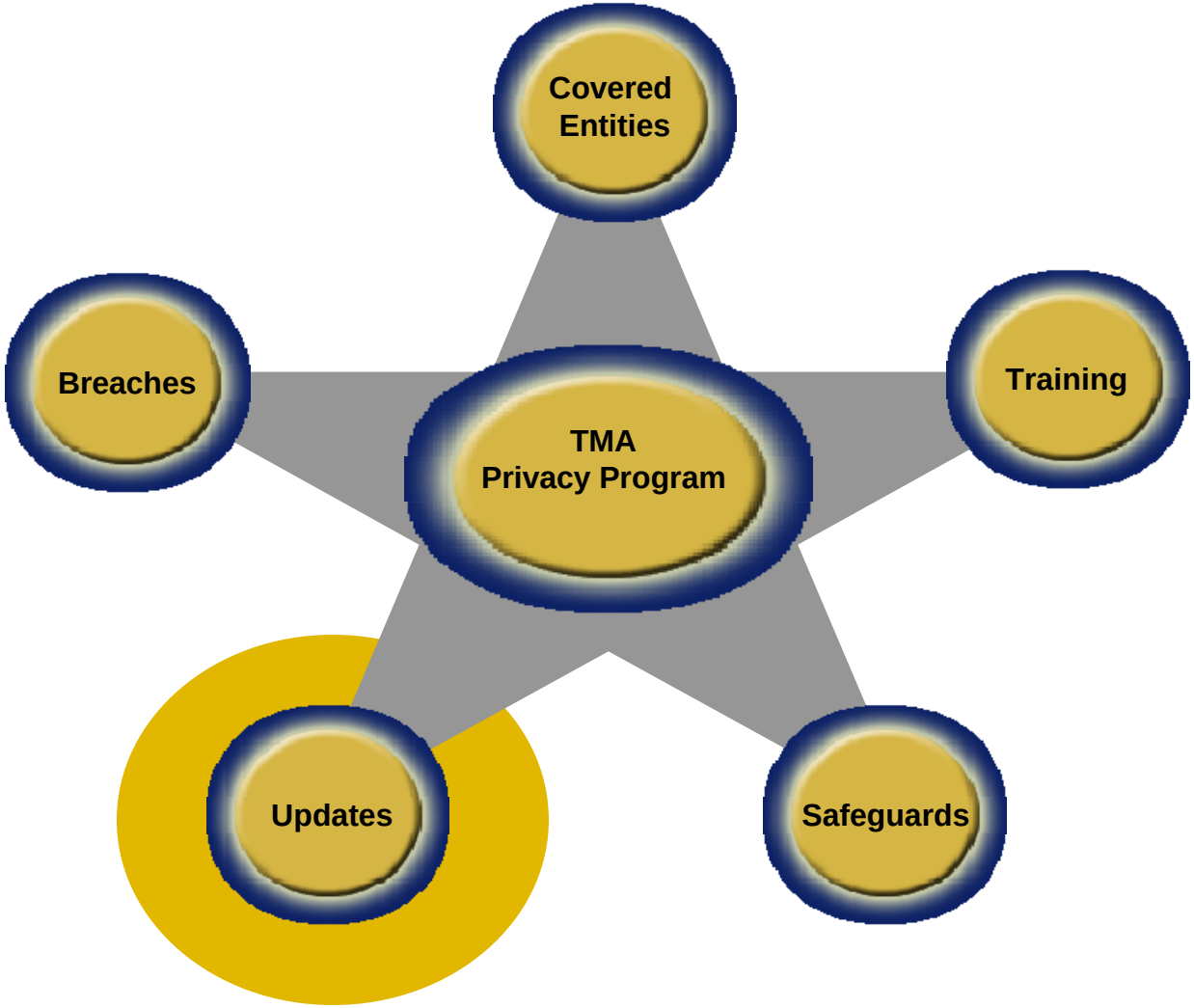
System of Records

A group of records under the control of a federal agency from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifier assigned to the individual

System of Records Notice

- Advance public notice must be published 30 days before an Executive Agency begins to collect personal information for a new System of Record
- Publication in the Federal Register is required to provide an opportunity for interested persons to comment

Updates

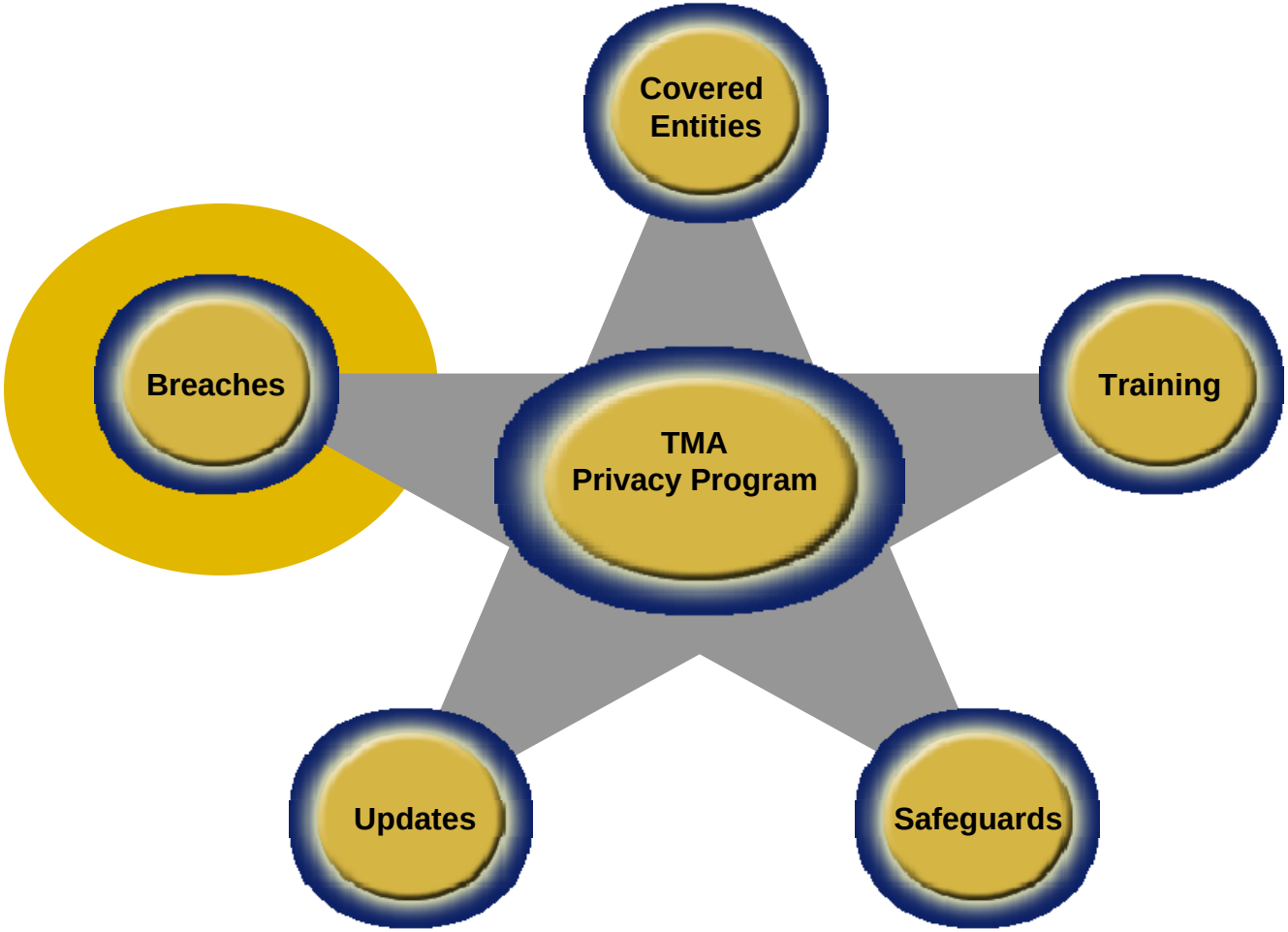

Covered Entities
Breaches
TMA Privacy Program
Training
Updates
Safeguards

Updates

Social Security Number (SSN) Reduction Plan

- DoD DTM 07-015 USD (P&R) “Social Security Number Reduction Plan” establishes new DoD requirements for the use, reduction, and elimination of Social Security Numbers (SSNs) as a unique identifier, where applicable
- Focus areas of this plan include:
    - Reducing or eliminating SSNs for both paper based records and information systems
    - Justifying SSN use on existing and new DoD forms and in automated systems
    - Reviewing SSN use at least every three years, the same as System Of Record Reviews
- Under this plan, use of SSN includes, but is not limited to truncation, masking, partially masking, encrypting, or disguising SSNs

Breaches


Covered Entities
Breaches
TMA Privacy Program
Training
Updates
Safeguards

Data Breaches

What is a Breach?

The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personally identifiable information (PII) where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected

Examples of Breaches

- Laptops stolen from automobiles
- Emails and attachments containing PII sent unencrypted to inappropriate/unauthorized persons
- Documents containing PII posted to sites allowing both staff and public access
- Inappropriate disposal of documents containing PII

You play a critical role in responding to a breach

What Should I Do If a Breach Occurs?	
When a loss, theft, or compromise of information occurs, the breach shall be reported as follows:	
TMA Components	***Uniformed Services***
▪ Leadership – **Immediately** ▪ TMA Privacy Office – Within **1 Hour** (**PrivacyOfficerMail@tma.osd.mil**) ▪ US CERT – Within **1 Hour** ▪ Defense Privacy Office – Within **48 Hours**	▪ Leadership – **Immediately** ▪ US CERT – Within **1 Hour** ▪ DoD Component Sr. Privacy Officials – Within **24 Hours** ▪ TMA Privacy Office – Within **24 Hours** (**PrivacyOfficerMail@tma.osd.mil**) ▪ Defense Privacy Office – Within **48 Hours**
Note: If necessary, notify issuing banks if government issued credit cards are involved; law enforcement; and all affected individuals within 10 working days of breach and identity discovery.	

Breach Notification

Five factors need to be considered when assessing the likelihood of risk and/or harm:

1. **Nature of the data elements breached**
2. **Number of individuals affected**
3. **Likelihood the information is accessible and usable**
4. **Likelihood the breach may lead to harm**
5. **Ability of the agency to mitigate the risk of harm**

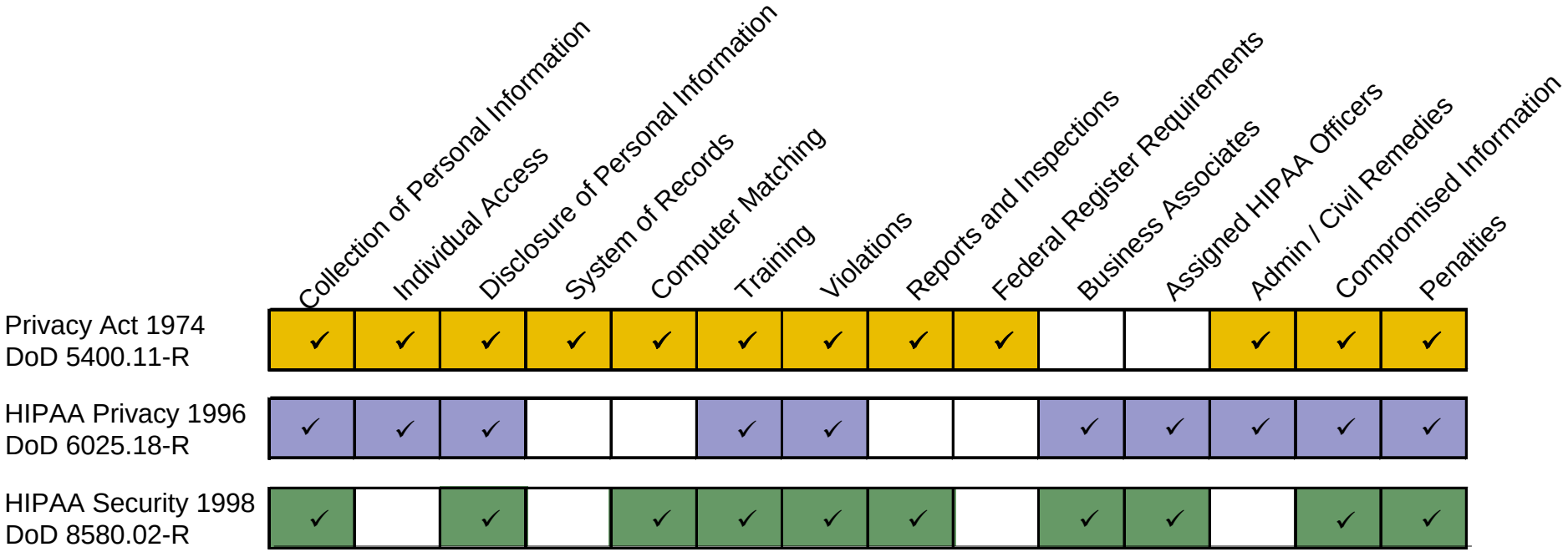
Based on the assessment of these factors, breaches are then classified as Low, Medium, or High.

Scenario

During routine network monitoring, Joint Task Force - Global Network Operations (JTF-GNO) detected suspicious activity on your network and reported it to the appropriate individuals within your Command. JTF-GNO asked that your IT staff conduct a security review of your network. Your CIO reported that an unsecured server was discovered. The server contained files that included protected health information (PHI) for over 20,000 individuals. After the review, your IT staff could not rule out the possibility that the server was accessed inappropriately. The IT staff reported that potentially compromised files included names, sponsor and individual social security numbers, dates of birth, insurance information and some medical diagnosis.

Is this a reportable breach?

Privacy Act and HIPAA



Questions?

For additional information please visit our website at http://www.tricare.mil/tmaprivacy/
or email PrivacyOfficerMail@tma.osd.mil