Department of Defense
TRICARE Management Activity (TMA)
Privacy Office

Non-Purchased Care Contract Language

For the Privacy and Security of
Personally Identifiable Information
and
Protected Health Information

October 25, 2007

Welcome from the TRICARE Management Activity (TMA)

Why Do We Need Contract Language?

- We need contract language to ensure that contractors understand their responsibility in protecting the health information of TMA beneficiaries.
- Contractors must follow the same privacy and security regulations as government TMA entities.
- Contractors can be held accountable for misuse or mishandling of protected health information (PHI) and personally identifiable information (PII).

Impact of Insufficient Non-Purchased Care Contract Language (1 of 3)

- TMA faces challenges for ensuring that appropriate contract language is used by contractors.
  - A recent breach of PHI involved all of the Services and Homeland Security (Coast Guard) who held various agreements with one contractor.
  - Several hundred thousand beneficiaries were affected.

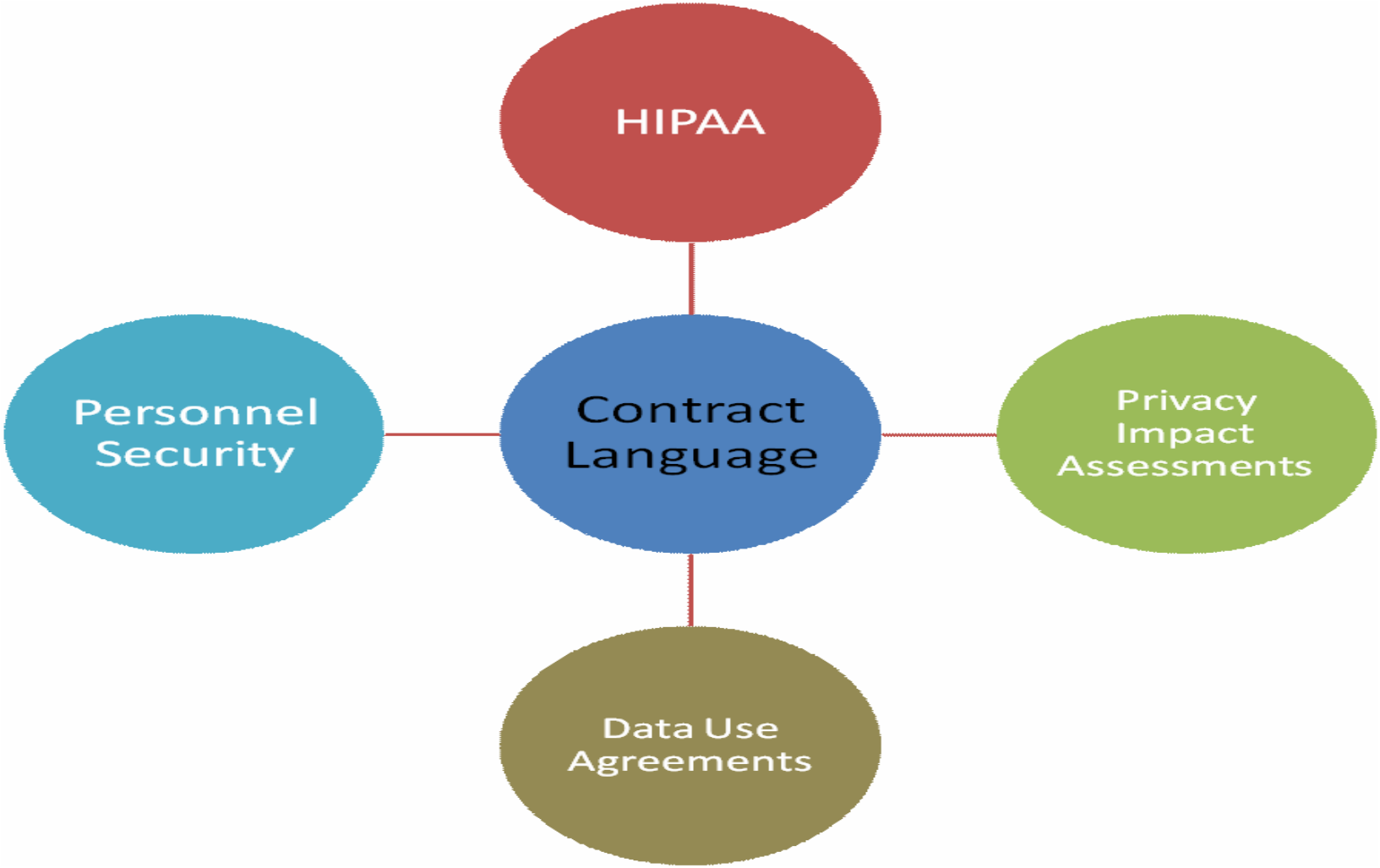
Impact of Insufficient Non-Purchased Care Contract Language (2 of 3)

- The impact of contract language:
  - Only one of the contracts contained the required HIPAA Business Associate Agreement (BAA) language.
  - The other contracts made no specific obligations on the contractor to notify TMA or the Services, or to safeguard PHI, or concerning notification of beneficiaries or mitigation of any harm.

Impact of Insufficient Non-Purchased Care Contract Language (3 of 3)

- Inappropriate contract language can effect additional areas:
  - HIPAA complaints
  - Privacy Act Compliance
  - Inappropriate PHI disclosures
  - Additional data breaches

Comprehensive Contract Language Critical to Safeguard Beneficiary Data



Health Insurance Portability and Accountability Act (HIPAA)

What is the HIPAA Privacy Rule?

- The HIPAA Privacy Rule provides the first national standards for protecting the privacy of health information, effective April 14, 2003.

- Requires contract language be included in agreements between Covered Entities (CEs) and individuals or organizations that use or disclose PHI on behalf of the CE. Those individuals or organizations are known as Business Associates (BAs).

HIPAA and Contract Language

- HIPAA Privacy/Security Rules require CEs to contractually impose safeguards for PHI on persons or entities who work with PHI on a CE's behalf (i.e., "business associate agreements").

- The requirement of the Business Associate (BA) to safeguard PHI is contractual. HIPAA does not "pass through" to the BA.

HIPAA and Contract Language

- HIPAA contract language includes training for the contractor workforce and management and mitigation of complaints.

- HIPAA contract language provides a vehicle to deal with inappropriate activities, which could include termination of a contract.

Responsibilities of the CE

- CEs may disclose PHI and PII to these contractors if the providers or plans obtain satisfactory assurances from these contractors that:
  - The information will be used only for the purposes for which it was engaged by the CE
  - The contractor will safeguard the information from misuse
  - The contractor will help the CE comply with some of the CE's duties

Contract Language

If a contract is required, ensure that the TMA "HIPAA Privacy and Security Business Associate Contract Language" (August 2005) is incorporated into your contract.

For the required contract clause go to: http://www.tricare.mil/tmaprivacy/hipaa/hipaacompliance/ba_agreements/index.htm.

Privacy Impact Assessments (PIAs) and System of Records (SORs)

What is a PIA? (1 of 2)

- A PIA is an analysis of how Information in Identifiable Form (IIF)/Personally Identifiable Information (PII) and Protected Health Information (PHI) is handled and protected in an Information Technology (IT) system.
- IIF can be personal and healthcare information.
- Requirement of Section 208 of the Electronic (E)-Government Act of 2002.

What is a PIA? (2 of 2)

- PIAs are conducted to:
  - Ensure that systems conform to legal, regulatory, and policy requirements for privacy.
  - Assess risks in the collection, maintenance and dissemination of IIF in an IT system.
  - Mitigate potential privacy risks.

PIAs and Contract Language

- Instances when PIA contract language is appropriate:
  - Contractor provides for the completion of a PIA, in DoD format, for any applicable system that maintains IIF on any individual, whether foreign or US Citizen.
  - Contractor is assisting the government in preparing a PIA.

- The TMA Privacy Office is always available to answer questions about the PIA process.

What is a SOR?

- System of Records are required by the Privacy Act of 1974.
- A Privacy Act "system of records" is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

SORs and Contract Language

- If contractors will be assisting the government in preparing a SOR, PIA contract language should be added.
- Please contact the TMA Privacy Office at SORmail@tma.osd.mil for assistance.

Data Use Agreements (DUAs)

What are DUAs and AARFs?

- A DUA is an agreement between the DoD and an outside entity.
- DUAs ensure that uses and disclosures of PII meet the requirements for both Federal laws and DoD regulations.
- An Account Authorization Request Form (AARF) is a document that authorizes requestors to access or retrieve data from applicable systems or databases within the MHS to carry out business operations or tasks outlined in the DUA.

DUAs Not Required

- DUAs are required if the contract specifies research, analysis, or human subjects research.
- DUAs are not required
  - For tasks that fulfill a part of normal operations for the contract.
  - For tasks that do not involve research or data analysis.
  - Contracts let to provide maintenance, development or technical support to the MHS.

Purpose for DUAs and AARFs

- Grant authorization for data retrieval and extraction from applicable systems or databases within the MHS.
- Control, monitor, and enforce compliance with Federal laws and DoD regulations related to the release of PII or PHI to internal and external requestors.

DUAs and Contract Language

- Contract language is an important component of DUAs because it specifies how data will be passed between TMA and another entity and further holds contractors accountable for protecting PII or PHI.
- Certification of Data Destruction is required when the contract has expired and will not be renewed.
- AARFs provide additional security by holding contractors to the same security standards in applying for access to a particular TMA system.

DUAs and Contract Language

In most cases, if you have a DUA, you do not need a PIA.

Personnel Security

Personnel Security

- All contractor employees who manage, design, develop, operate or access DoD Automated Information Systems (AIS) or DoD network systems are required to undergo appropriate background investigation and security awareness training.

- DoD personnel are subject to appropriate levels of IT/ADP security clearances.

Personnel Security and Contract Language

- The contractor workforce must meet strict guidelines before being granted access to HA/TMA network.

- Contract language ensures that contractors are held to the same level of investigations and training, as well as appropriate clearances.

Templates

- The three types of contract language are:
  - Protected Health Information (PHI)
  - Business Associate Agreement (BAA)
  - Contractor Access to HA/TMA Network

- Templates can be found at: http://www.tricare.mil/tmaprivacy/contract.cfm

- Simply click on the appropriate link, and copy and paste the language into the contract document.

PHI Contract Language

- PHI Standard Contract Language is located at:
  - http://www.tricare.mil/tmaprivacy/downloads/PHILanguage.doc

- There are three sections within the PHI Contract Language template:
  - HIPAA
  - PIA
  - DUA

- Utilize any and all applicable sections.

PHI Contract Language Requirements

- If the contractor utilizes any element of PHI in any form, include HIPAA contract language.

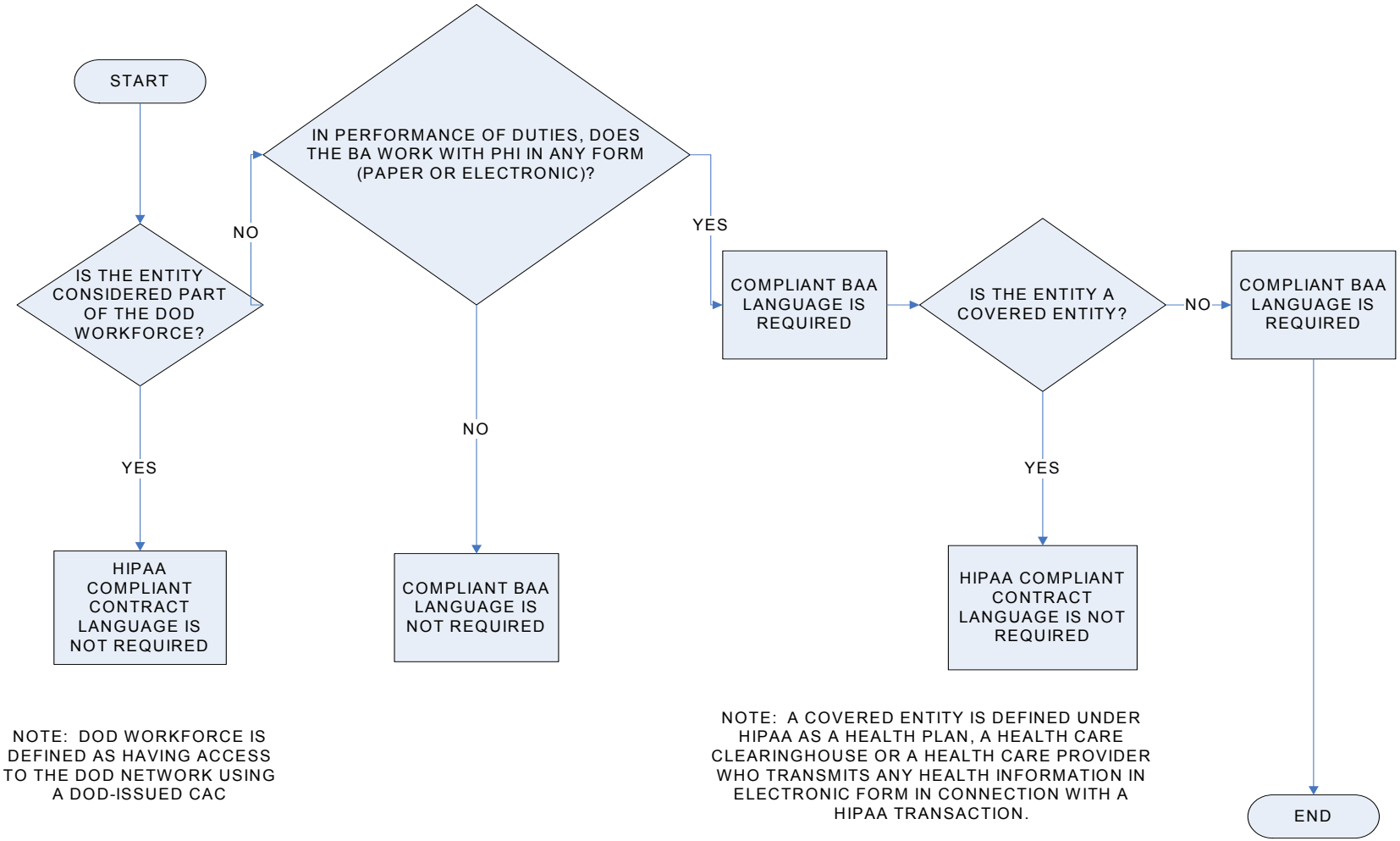
- If records are collected, stored or disseminated with IIF and the contractor is using the data for a secondary purpose, include the PIA contract language.

BAA Contract Language

- The BAA Standard Contract Clause can be found at:
  - http://www.tricare.mil/tmaprivacy/downloads/DoDBAclauseAUG07.doc

- BA Contract language is mandatory whenever a contract is awarded that requires an outside person or entity to provide certain functions, activities, or services involving the use and/or disclosure of PHI.

BA Contract Language Requirements



NOTE: DOD WORKFORCE IS DEFINED AS HAVING ACCESS TO THE DOD NETWORK USING A DOD-ISSUED CAC

NOTE: A COVERED ENTITY IS DEFINED UNDER HIPAA AS A HEALTH PLAN, A HEALTH CARE CLEARINGHOUSE OR A HEALTH CARE PROVIDER WHO TRANSMITS ANY HEALTH INFORMATION IN ELECTRONIC FORM IN CONNECTION WITH A HIPAA TRANSACTION.

Contractor Access to HA/TMA Network

- Contractor Access contract language can be found at:
  - http://www.tricare.mil/tmaprivacy/downloads/AccessLanguage.doc

- Contractor Access Contract language is mandatory whenever a contract is awarded that requires the contractor employee to access the HA/TMA Network and/or other DoD systems on a TRICARE Contract.

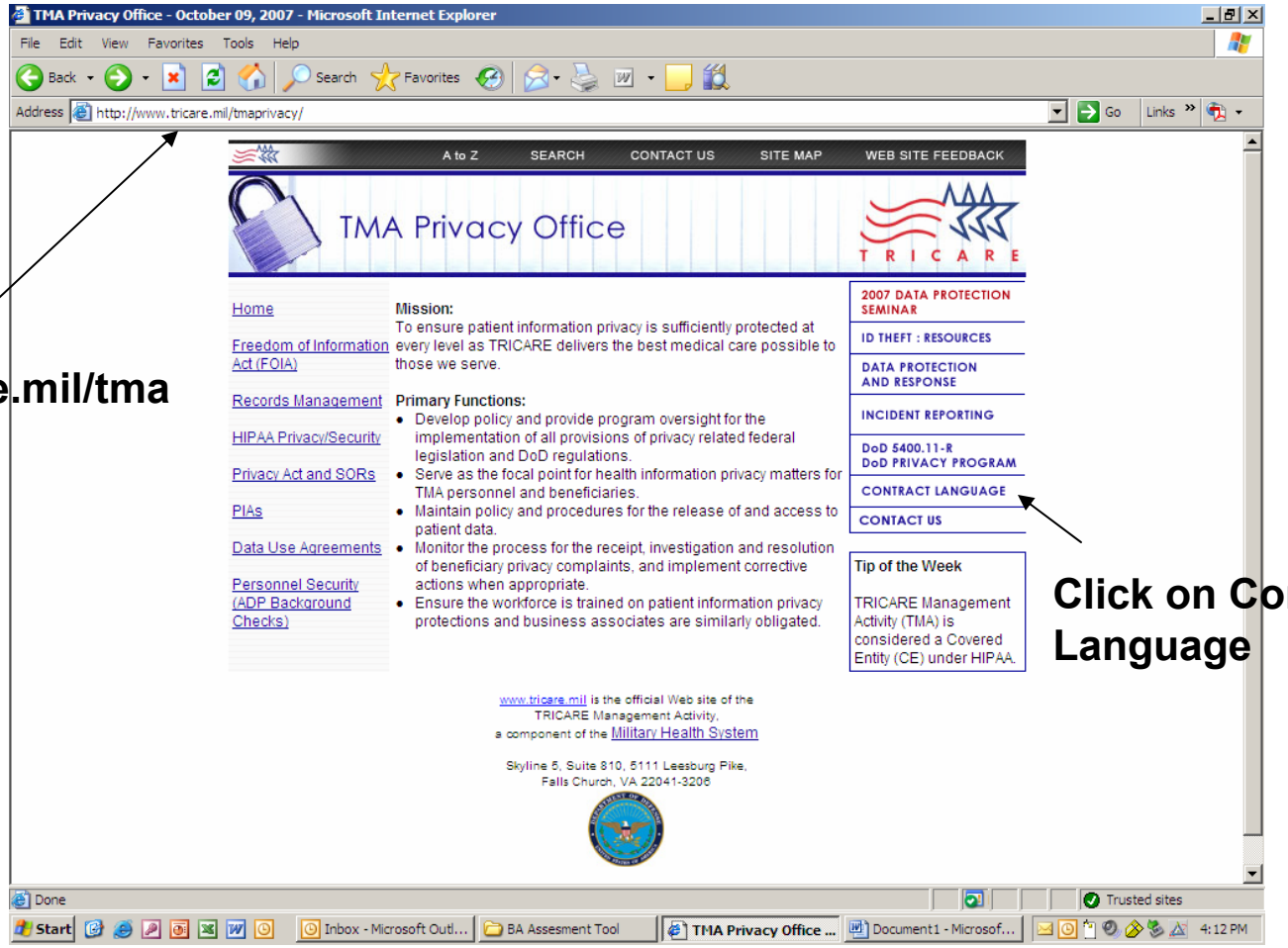
Contractor Access Language Requirements

- Contractor Access Contract language is mandatory whenever a contract is awarded that requires the contractor employee to access the HA/TMA Network and/or other DoD systems on a TRICARE Contract.
- The TMA Privacy Office is constantly monitoring applicable laws and regulations to determine if a change could impact the contract language.
  - Check the updates to the contract language frequently.

Demonstration

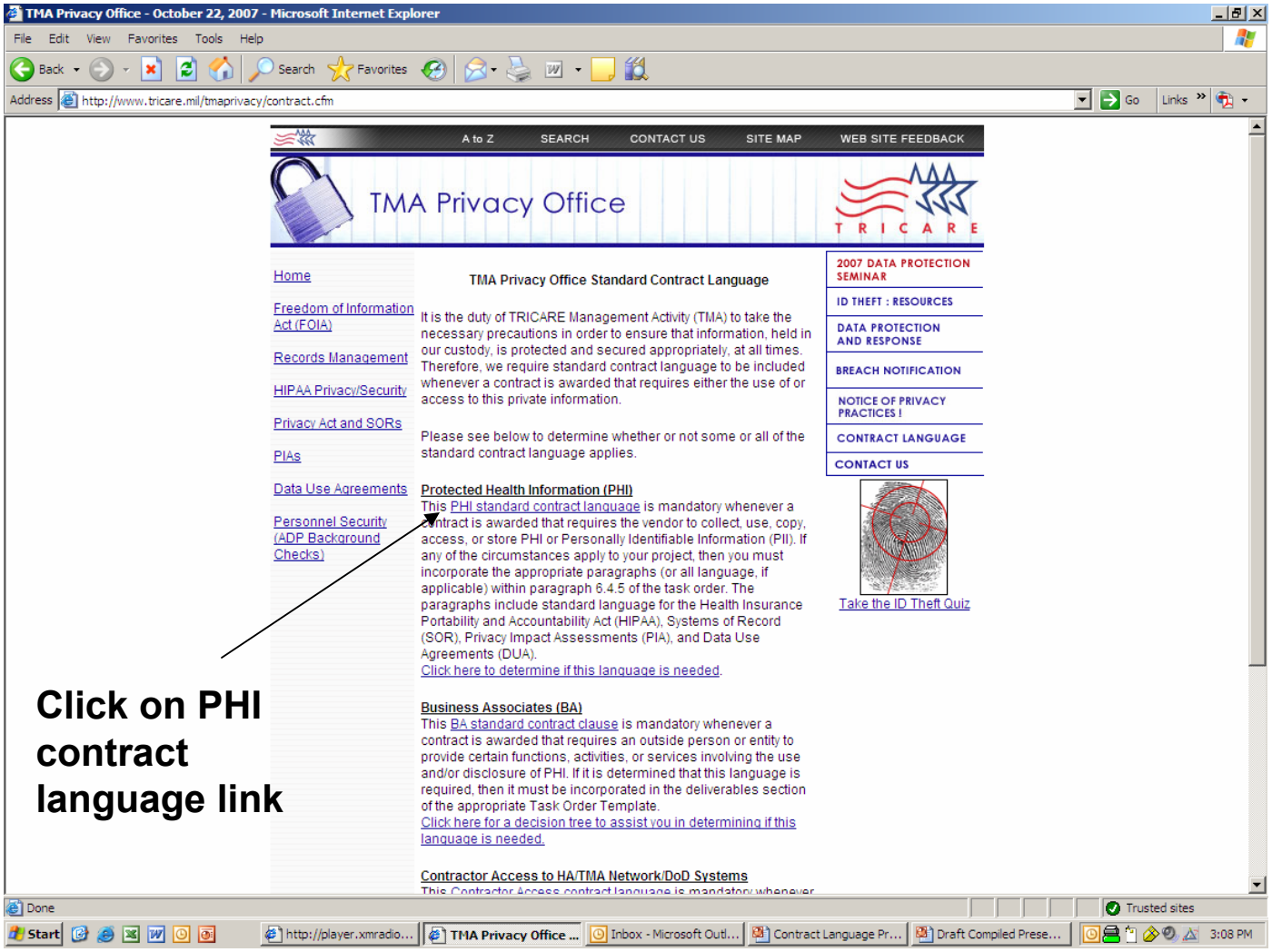
Contract Language Requirement
(1 of 4)

www.tricare.mil/tma privacy



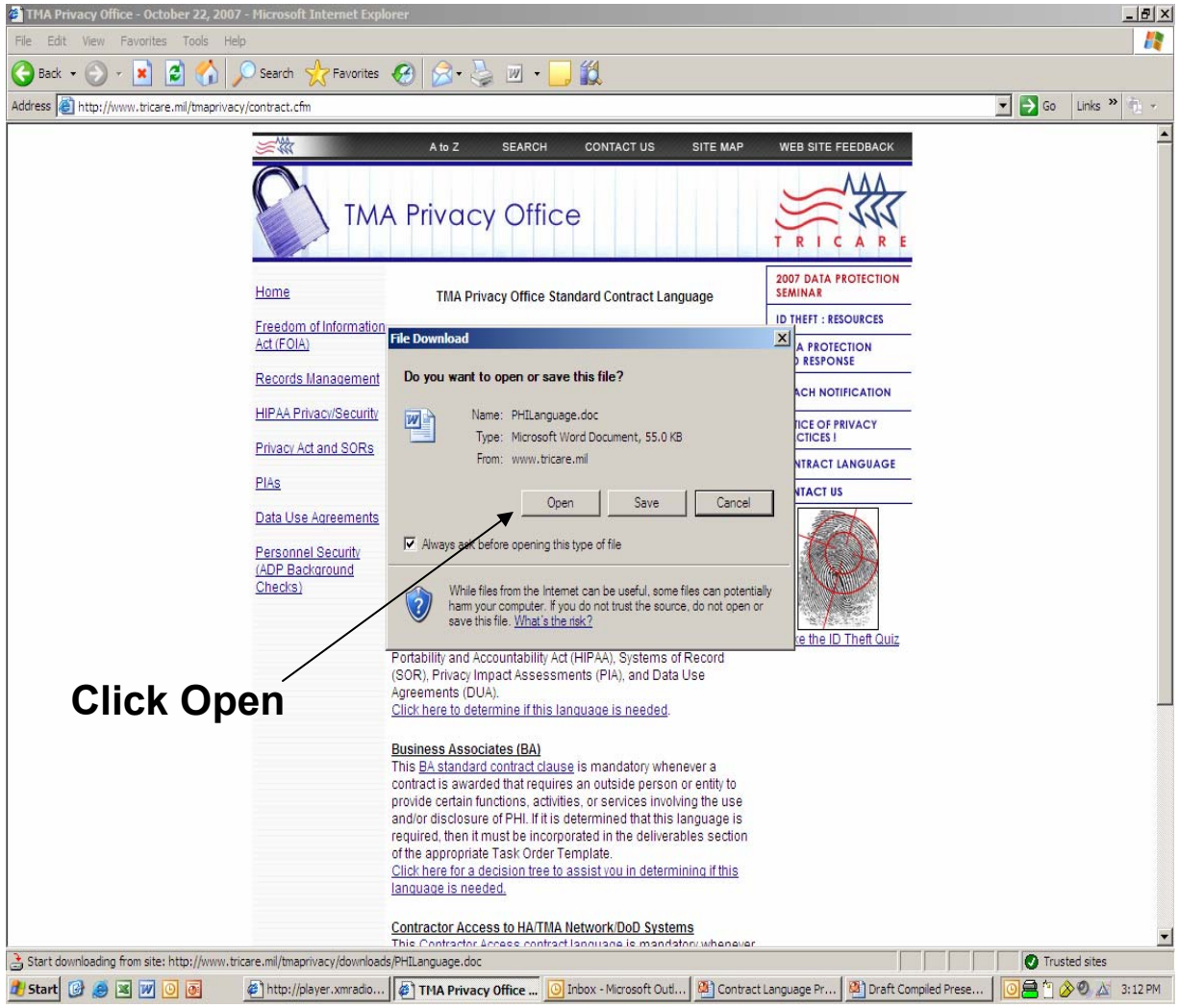
Click on Contract Language

Contract Language Requirement
(2 of 4)



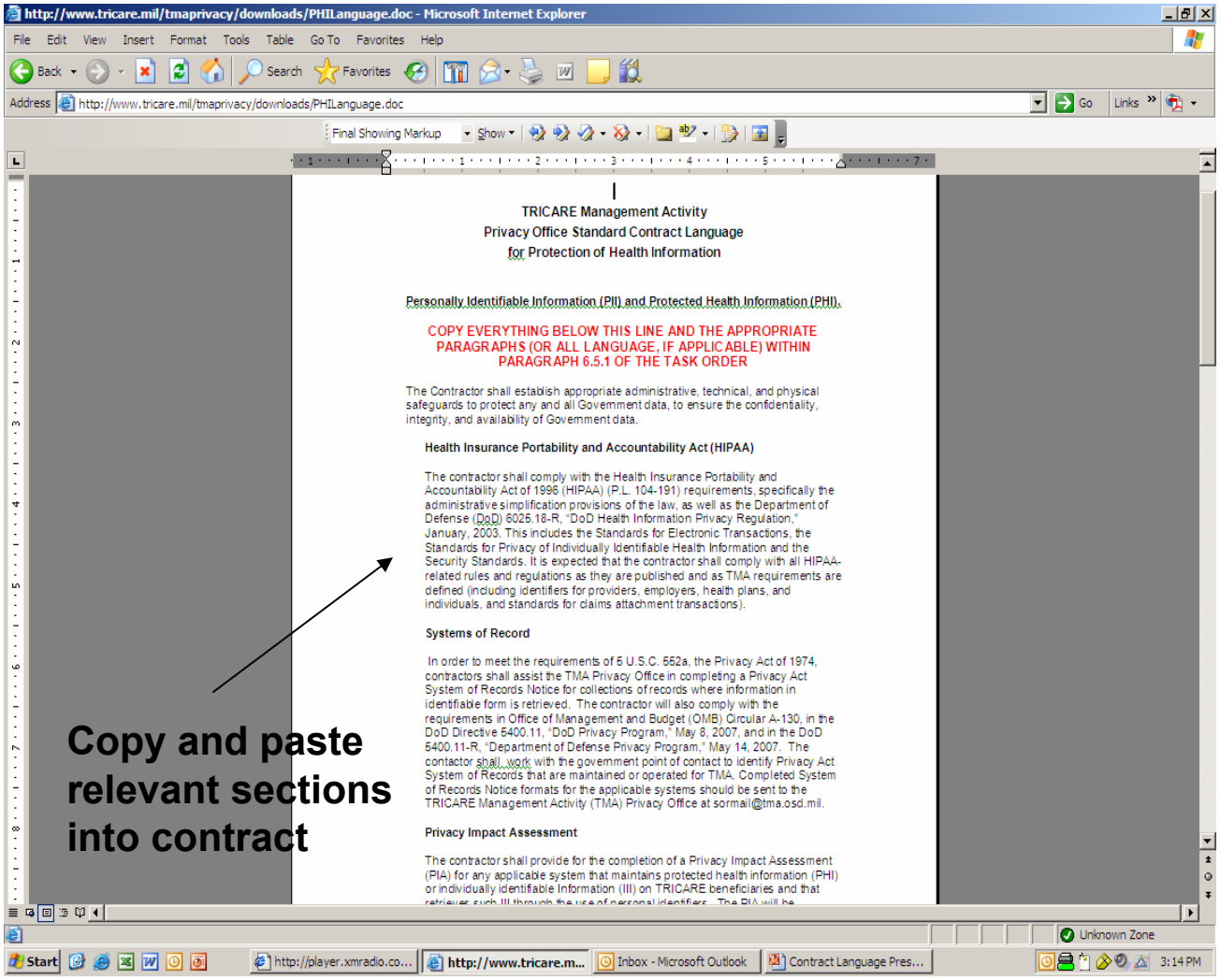
Click on PHI contract language link

Contract Language Requirement
(3 of 4)



Click Open

Contract Language Requirement
(4 of 4)



Copy and paste relevant sections into contract

Federal and DoD Regulations (1 of 2)

- DoD and Federal Regulations protect health information by requiring contractors to abide by certain criteria:
  - The Privacy Act of 1974
  - DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
  - DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007
  - DoD Directive 5400.11-R, "DoD Privacy Program," May 8, 2007
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - The E-Government Act, December 17, 2002

Federal and DoD Regulations (2 of 2)

- DoD and Federal Regulations protect health information by requiring contractors to abide by certain criteria:
  - Department of Defense (DoD) Deputy Chief Information Officer Memorandum, "Privacy Impact Assessment (PIA) Guidance," October 28, 2005
  - OMB M-01-05, "Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy," December 20, 2000
  - OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003
  - TRICARE Management Activity Privacy Impact Assessment (PIA) Policy," February 10, 2006

Summary

- Contract Language helps to ensure that the PHI and privacy of the 9.2 M of TMA beneficiaries is well protected.

- Thank you for your assistance in making sure that these regulations are followed.

Questions?