General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

ADMINISTRATIVE SAFEGUARDS

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.308(a)(1)(i) 164.308(a)(1)(i) 164.308(a)(1)(i)	Security Management Process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	C2.2.	R	R	DoDD 8500.1 DoDI 8500.2 DoDD 8000.01	4.6. and 4.20. E3.3.9., E3.4.6., E3.4.6.4., ECAT-1 and ECAT-2 4. and E2
164.308(a)(1)(ii)(A)	Risk Analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	C2.2.3.	R	R	DoDD 8500.1 DoDI 8500.2	4.20., 4.21., 5.2.3. 5.1., 5.1.3., 5.1.3.4., E3.2.3., E3.3., E3.3.10, DCII-1, VIIR-1 and 2, VIVM-1
164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(B)	Risk Management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	C2.2.4.	R	R	DoDD 5000.01 DoDD 8500.1 DoDI 8500.2 DoDI 8510.01	E1.1.14. 4.14., 4.14.3., 4.21., 4.4., 4.6. 5.7.16. , E3.1.2., E3.1.3., E3.3.8., E3.3.10., E3.4.4., E3.4.6.4., VIVM-1 4.1., 6.3.3.1.4.
164.308(a)(1)(ii)(C)	Sanction Policy	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	C2.2.5.	R	R	TMA Sanction Policy 4/9/2008	4.1., 4.2.
164.308(a)(1)(ii)(D)	Information System Activity Review	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	C2.2.6.	R	R	DoDI 8500.2	5.7.9.3., E3.3.10., ECCD-2, ECRG-1, ECAT-1, ECAT-2, ECWM-1, EBRP-1

(R = Required A = Addressable)

Disclaimer: ***This document is intended to provide a general mapping of HIPAA Security Rule requirements to existing DoD policies and IA controls and does not constitute the rendering of legal advice or an exhaustive list of all possible mappings to existing DoD or Component policies.***

Last Update: 9/14/2009

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.308(a)(2)	Assigned Security Responsibility	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	C2.3.	R	R	DoDD 8000.1 DoDD 8500.1 DoDI 8500.2	Enclosure 2, section 6.e. 5.1., 5.1.3., 5.10.1. 5., E3.3.5., E3.3.6., E3.3.11., DCSD-1 IA
164.308(a)(3)(i) 164.308(a)(3)(i) 164.308(a)(3)(i)	Workforce Security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	C2.4.	R	R	DoD 5200.2-R DoDD 8500.1 DoDI 8500.2	C2.1.1. 4.8., 4.8.1. 5.7.11., 5.7.15., 5.9.2., 5.9.5., 5.10.1., 5.11.2., 5.12., 5.12.2., 5.12.4., E4.1.7.3., Table E4.T3., DCFA-1, ECCD-2, ECPA-1, ECAN-1, ECLP-1, PRNK-1
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	C2.4.3.	A	R	DoDI 8500.2	5.9.1., E3.4.6., E3.4.6.2., E3.3.2., E3.3.6., E3.3.7., E3.3.11., 5.7.7., 5.8.2., 5.9.6., ECAN-1, ECLP-1, PRNK-1, DCSD-1, PRTN-1

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	C2.4.4.	A	R	DoDD 5200.2 DoDI 8500.2	3.9., 3.10 5.10.1., E3.4.7., ECAN-1, ECLP-1, PRNK-1
164.308(a)(3)(ii)(C)	Termination Procedure	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	C2.4.5.	A	R	DoDI 8500.2	IAAC-1, PRNK-1
164.308(a)(4)(i)	Information Access Management	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	C2.5.	R	R	DoDI 8500.2	5.7.11., 5.7.15., 5.9.2., 5.10.1., 5.11.2., 5.12.2, 5.12.4., E4.1.7.3., Table E4.T3., DCFA-1, ECCD-2, ECAN-1
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	N/A	R	N/A	N/A	
164.308(a)(4)(ii)(B)	Access Authorization	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	C2.5.4.	A	R	DoDI 8500.2	5.9.1., E3.4.6., E3.4.6.2.
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	C2.5.5.	A	R	DoDI 8500.2	5.7.11.

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.308(a)(5)(i) 164.308(a)(5)(i)	Security Awareness and Training	Implement a security awareness and training program for all members of its workforce (including management).	C2.6.	R	R	DoDD 8500.1 DoDI 8500.2	5.1.3., 5.1.8.3., 5.10.7. 5.1.3.7., 5.1.3.9., 5.4.5., 5.7.7., 5.8.2., 5.9.6., E3.3.7, E3.4.6.6., PRTN-1
164.308(a)(5)(ii)(A)	Security Reminders	Implement periodic security updates.	C2.6.4.	A	R	DoDI 8500.2	ECVP-1, E3.2.5.7.
164.308(a)(5)(ii)(B)	Protection from Malicious Software	Implement procedures for guarding against, detecting, and reporting malicious software.	C2.6.5.	A	R	DoDI 8500.2	ECVP-1, VIVM-1
164.308(a)(5)(ii)(C)	Log-in Monitoring	Implement procedures for monitoring log-in attempts and reporting discrepancies.	C2.6.6.	A	R	DoDI 8500.2	E3.3.9., ECAN-1, ECAR-3
164.308(a)(5)(ii)(D)	Password Management	Implement procedures for creating, changing, and safeguarding passwords.	C2.6.7.	A	R	DoDI 8500.2	IAIA-2
164.308(a)(6)(i)	Security Incident Procedures	Implement policies and procedures to address security incidents.	C2.7.1.	R	R	TMA Standard Operating Procedure 10/12/2007 DoDD 8500.1 DoDI 8500.2	1.1 4.20. 5.7.9., 5.7.9.1., 5.7.9.2., 5.7.9.3., 5.9.10., 5.10.2., E3.4.6., E3.4.6.4., DCDS-1, VIIR-2, PRTN-1

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.308(a)(6)(ii)	Response and Reporting	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	C2.7.2.	R	R	DoDD 8500.1 DoDI 8500.2	4.20., 4.21. 5.7.9., 5.7.9.1., 5.7.9.2., 5.7.9.3., 5.9.10., VIVM-1, VIIR-1
164.308(a)(7)(i)	Contingency Plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	C2.8.1.	R	R	DoDI 8500.2	5.10.4., COTR-1
164.308(a)(7)(ii)(A)	Data Backup Plan	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	C2.8.2.	R	R	DoDI 8500.2	COTR-1, COAS-2, CODB-2
164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Establish (and implement as needed) procedures to restore any loss of data.	C2.8.3.	R	R	DoDI 8500.2	CODP-1, CODP-2, CODP-3, COTR-1, COAS-2, COED-1, COED-2, CODB-2
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	C2.8.4.	R	R	DoDI 8500.2	DCFA-1, COEF-1
164.308(a)(7)(ii)(D)	Testing and Revision Procedure	Implement procedures for periodic testing and revision of contingency plans.	C2.8.5.	A	R	DoDI 8500.2	DCAR-1, COED-1

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Assess the relative criticality of specific applications and data in support of other contingency plan components.	C2.8.6.	A	R	DoDD 8500.1 DoDI 8500.2	4.7. 5.7.1.1., 5.7.1.3.
164.308(a)(8) 164.308(a)(8) 164.308(a)(8)	Evaluation	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	C2.9.(C2.9.1. - C2.9.3.)	R	R	DoDD 8500.1 DoDI 8500.2 DoDI 8510.01	4.6., 5.1.1. 9.8., E3.2.3., DCAR-1 4.9., 5.16.8., 6.3.4., 6.3.4.3., E3.A3.2.2.
164.308(b)(1)	Business Associate Contracts and Other Arrangements	A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.	C2.10.	R	R	DoD 6025.18-R DoDI 8500.2	C3.4.2.2., C3.4.2.2.1., C3.4.2.2.2. 5.7.10.
164.308(b)(4)	Written Contract or Other Arrangement	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a).	C2.10.1.	R	R	DoD 6025.18-R	C8.5.4.

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

PHYSICAL SAFEGUARDS

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.310(a)(1)	Facility Access Controls	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	C3.2.1.	R	R	DoD 5200.08-R DoDI 8500.2	C2.2. PEPF-2, PEPS-1, PESS-1, PEVC-1
164.310(a)(2)(i) 164.310(a)(2)(i)	Contingency Operations	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	C3.2.3.	A	R	DoD 5200.08-R DoDI 8500.2	C3.4.2., C3.4.2.1., C5.2.4., C6.3.2 COTR-1, COAS-2, CODB-2
164.310(a)(2)(ii)	Facility Security Plan	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	C3.2.4.	A	R	DoDD 5200.8 DoD 5200.08-R DoDI 8500.2	3.1., 3.2., 5.1. C3.2., C3.2.2., C3.2.4., C3.2.5., C3.2.6., C7.3.1., C7.3.1.1. PEPF-2, PEPS-1, PESS-1, PEVC-1
164.310(a)(2)(iii) 164.310(a)(2)(iii) 164.310(a)(2)(iii)	Access Control and Validation Procedures	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	C3.2.5.	A	R	DoD 5200.08-R DoDI 8500.2 DoDI 8500.2	C1.3.4., C3.2., C3.2.5., C3.2.6. 5.12., 5.12.2., 5.12.4., E4.1.7.3., Table E4.T3., DCFA-1, ECCD-2, ECPA-1 PEPF-2, PEPS-1, PESS-1, PEVC-1, COMS-1

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.310(a)(2)(iv)	Maintenance Records	Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).	C3.2.6.	A	R	DoDI 8500.2 MHS IA Implementation Guide 5 - Physical Security 10/10/2008	PRMP-1 e.
164.310(b) 164.310(b)	Workstation Use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	C3.3.1.	R	R	DoDI 8500.2 MHS IA Implementation Guide 5 - Physical Security 10/10/2008	5.12., 5.12.2., 5.12.6., 5.12.11., 5.12.12. b., d., f..
164.310(c)	Workstation Security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	C3.4.	R	R	DoDI 8500.2	PEPF-2, PEVC-1, PEDI-1
164.310(d)(1)	Device and Media Controls	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	C3.5.1.	R	R	DoDI 8500.2	5.12.5., 5.12.12.
164.310(d)(2)(i)	Disposal	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	C3.5.3.	R	R	DoDI 8500.2	E3.4.3., PECS-1

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.310(d)(2)(ii)	Media Re-Use	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	C3.5.4.	R	R	MHS IA Implementation Guide 2 – Sanitization 10/10/2008	3.3., 3.3.1.
164.310(d)(2)(iii)	Accountability.	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	C3.5.5.	A	R	DoDI 8500.2	5.9.2., E3.1.5., PESS-1
164.310(d)(2)(iv)	Data Backup and Storage	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	C3.5.6.	A	R	DoDI 8500.2	5.10.4., COBR-1, CODB-1, CODB-2, CODB-3, COSW-1, COTR-1, DCHW-1, DCSW-1, ECTB-1

TECHNICAL SAFEGUARDS

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.312(a)(1)	Access Controls	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	C4.2.1.	R	R	DoDD 8500.1 DoDI 8500.2	4.8.1., 4.8.2., 4.11., 4.11.1, 4.11.2. 5.12., 5.12.2., 5.12.4., E4.1.7.3., Table E4.T3., DCFA-1, ECCD-2, ECPA-1
164.312(a)(2)(i)	Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity.	C4.2.2.	R	R	DoDI 8500.2	IAIA-1, IAIA-2
164.312(a)(2)(ii)	Emergency Access Procedure	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	C4.2.3.	R	R	DoDI 8510.01	6.3.1.1., Table E3.A1.

(R = Required A = Addressable)

***Disclaimer:** This document is intended to provide a general mapping of HIPAA Security Rule requirements to existing DoD policies and IA controls and does not constitute the rendering of legal advice or an exhaustive list of all possible mappings to existing DoD or Component policies.*

Last Update: 9/14/2009

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.312(a)(2)(iii)	Automatic Logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	C4.2.4.	A	A	DoDI 8500.2	PESL-1
164.312(a)(2)(iv)	Encryption and Decryption	Implement a mechanism to encrypt and decrypt electronic protected health information.	C4.2.5.	A	A	DoDI 8500.2	DCFA-1, DCNR-1, ECCR-1, ECCR-2, ECCR-3, ECCT-1, ECCT-2, ECNK-1, ECNK-2, EBRU-1, ECTM-2, IAIA-2
164.312(b)	Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	C4.3.	R	R	DoDI 8500.2	5.7.9.3., EBRP-1, ECAT-1, ECAT-2, ECND-2, ECRG-1, ECRR-1, ECLC-1, ECTB-1, ECTP-1, ECAN-1, ECAR-1, ECAR-2, ECAR-3
164.312(c)(1)	Integrity	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	C4.4.1.	R	R	DoDI 8500.2	DCFA-1, DCNR-1, ECCR-1, ECCR-2, ECCR-3, ECCT-1, ECCT-2, ECNK-1, ECNK-2, EBRU-1, ECTM-2, IAIA-2
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	C4.4.2.	A	R	DoDI 8500.2 DoDI 8510.01	5.12.4., E3.2.4.3.3., E3.2.4.3.4., E3.2.9., IAGA-1, IAIA-2, IAKM-2, IATS-1, IATS-2, ECAN-1, PESL-1 Table E3.A1.T1.
164.312(d) 164.312(d)	Person or Entity Authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	C4.5.	R	R	DoDD 8500.1 DoDI 8500.2	4.8., 4.8.1. IAIA-1, IAIA-2
164.312(e)(1)	Transmission Security	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	C4.6.1.	R	R	DoDD 8500.1 DoDI 8500.2	4.2., 4.26., 4.5., 4.14.2. DCFA-1, DCNR-1, ECCR-1, ECCR-2, ECCR-3, ECCT-1, ECCT-2, ECNK-1, ECNK-2, EBRU-1, ECTM-2, IAIA-2

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.312(e)(2)(i)	Integrity Controls	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	C4.6.2.	A	R	DoDD 8500.1 DoDI 8500.2	4.2., 4.26., 4.5., 4.14.2. DCFA-1, DCNR-1, ECCR-1, ECCR-2, ECCR-3, ECCT-1, ECCT-2, ECNK-1, ECNK-2, EBRU-1, ECTM-2, IAIA-2
164.312(e)(2)(ii)	Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	C4.6.3.	A	A	DoDI 8500.2	DCFA-1, DCNR-1, ECCR-1, ECCR-2, ECCR-3, ECCT-1, ECCT-2, ECNK-1, ECNK-2, EBRU-1, ECTM-2, IAIA-2

ORGANIZATIONAL SAFEGUARDS

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.314(a)(1)	Business associate contracts or other arrangement	(i) The contract or other arrangement between the covered entity and its business associate required by Sec. 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in Sec. 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.	C2.10.	R	R	DoD Standard Contract Clause for Business Associates	See TMA Privacy Office website for business associate contract language.

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.314(a) (2)(i) 164.314(a) (2)(i)	Business associate contracts	The contract between a covered entity and a business associate must provide that the business associate will— (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	C2.10.2	R	R	DoD 6025.18-R DoDI 8500.2	C8.5.4., C3.4.1., C3.4.1.1., C3.4.1.2., C3.4.1.3. 5.7.7., 5.7.10., E3.2.5., E3.2.5.4., E3.3.6., E3.4.1.3.

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.314(a) (2)(ii))	Other arrangements	(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if-- (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section. (B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in Sec. 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. (C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.	C2.10.	R	R	DoDI 8500.2	E3.4.1.3.

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

POLICIES, PROCEDURES AND DOCUMENTATION

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.316 (a))	Policies and procedures	A covered entity must, in accordance with Sec. 164.306: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in Sec. 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	C1.6.	R	R	DoDD 8500.1 DoDD 8510.01 DoDD 5015.2 DoD 6025.18-R	
164.316(b)(1)	Documentation	A covered entity must, in accordance with §164.306: (i) Maintain the policies and procedures implementedto comply with this subpart in written (which may beelectronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity or assessment	C1.6.4.4, C1.6.4.5	R	R	DoDD 5015.2	4.1.
164.316(b)(2)(i)	Time Limit	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever islater.	C1.6.4.5.1.	R	R	DoDD 5015.2	4.1.
164.316(b)(2)(ii)	Availability	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	C1.6.4.5.2.	R	R	DoDD 8500.1 DoDI 8500.2 DoDI 8510.01	4.3. 5.10.5. 4.6.

General Mapping of Health Insurance Portability and Accountability Act (HIPAA) Security Rule to Existing Department of Defense (DoD) Policies and Information Assurance (IA) Controls

Section of HIPAA Security Rule	HIPAA Safeguard	Description	Section of DoD 8580.02-R	HIPAA Required	DOD Required	DoD Relevant References	DoD Relevant Sections and IA Controls
164.316(b)(2)(ii) 164.316(b)(2)(ii)	Updates	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	C1.6.4.5.3.	R	R	DoDI 8500.2 DoDI 8510.01	5.10.5. 4.9., 6.3.4.3., 6.3.4.2.