Information Shield Solution Matrix for HIPAA Security Standards

The following table illustrates how specific policies within *Information Security Policies Made Easy* map to the "required" and "addressable" security standards found in the HIPAA Final Security Rule [1], issued in February 2003. Where applicable, other Information Shield products are included.

Security Standards	**Implementation Specifications (R)=Required, (A)=Addressable**	**Specific ISPME Policies and Solution**
General Rules 164.306 Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.	**(R)**	Information Shield publications are designed to facilitate a policy-based security program as required by HIPAA. *Information Security Policies Made Easy (ISPME)* provides over 1400 detailed security and privacy policies that can be easily customized for any organization. *Information Security Roles and Responsibilities Made Easy* is a complete guide for building a best-practices security organization, including 40 pre-written job descriptions with security requirements. VigilEnt Policy Center (VPC)*, available through our reseller arrangement with NetIQ, provides automation for creating and distributing policies, tracking which users have read and acknowledged policies, and testing user awareness via on-line quizzes. Detailed audit reports and management reports ensure compliance with your corporate policies.

Administrative Safeguards		**ISPME Specific Policies**
Security Management Process 164.308(a)(1) “Policies and procedures to prevent, detect, contain, and correct security violations.”	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)	5.1.1 Information Security Policy Document 6.1.2 Information Security Coordination 6.1.1- 2. Risk Assessments 6.2.1 Identification of risks related to external parties 14.1.2 Business continuity and risk assessment 15.1.1- 6. System Risk Assessments 7.2 Information Classification 7.2.1 Classification Guidelines (23 policies) 7.2.2 Information Labeling And Handling (42 policies) 8.2.3 Disciplinary Process (5 policies) 10.10.2 Monitoring System Use 15.3.1 Information systems audit controls 15.3.2 Protection of information systems audit tools
Assigned Security Responsibility 164.308(a)(2) “Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.”	(R)	6.1.2 Information security co-ordination 6.1.3 Allocation Of Information Security Responsibilities

Workforce Security 164.308(a)(3) Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, […] 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.	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)	8 HUMAN RESOURCES SECURITY 8.1 PRIOR TO EMPLOYMENT 8.1.1 Roles and responsibilities 8.1.2 Screening 8.1.3 Terms and conditions of employment 8.2 DURING EMPLOYMENT 8.2.1 Management responsibilities 8.2.2 Information security awareness, education, and training 8.2.3 Disciplinary process 8.3 TERMINATION OR CHANGE OF EMPLOYMENT 8.3.1 Termination responsibilities 8.3.2 Return of assets 8.3.3 Removal of access rights
Information Access Management 164.308(a)(4) “Implement policies and procedures for authorizing access to electronic protected health information”	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)	11 Access Control 11.2 User Access Management 11.4 Network Access Control (30+ policies) 11.5 Operating System Access Control (20+ policies) 11.6 Application and Information Access Control (25 policies)
Security Awareness and Training 164.308(a)(5) “Implement a security awareness and training program for all members of its workforce (including management).”	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)	8.2.2 Information security awareness, education, and training 10.4.1 Controls against malicious code. 10.4.2 Controls against mobile code 10.10.2 Monitoring System Use 11.3.2 Unattended user equipment 11.2.3 User password management 11.3.1 Password use

Security Incident Procedures 164.308(a)(6) “Implement policies and procedures to address security incidents.”	Response and Reporting (R)	13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES. 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses 13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 13.2.1 Responsibilities and procedures 13.2.2 Learning from information security incidents 13.2.3 Collection of evidence
Contingency Plan 164.308(a)(7) “Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence […]”	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)	10.5.1 Information back-up 14.1.1 Including information security in the business continuity management process 14.1.2 Business continuity and risk assessment 14.1.3 Developing and implementing continuity plans including information security 14.1.4 Business Continuity Planning Framework
Evaluation 164.308(a)(8) “Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently [..]that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	(R)	5.1.2 Review of the information security policy 15.2 Reviews Of Security Policy And Technical Compliance 15.2.1 Compliance With Security Policy (6 policies) 15.2.2 Technical Compliance Checking (3 policies)
Business Associate Contracts and Other Arrangement 164.308(b)(1)	Written Contract or Other Arrangement (R)	6.2.1 Identification of risks related to external parties 6.2.2 Addressing security when dealing with customers 6.2.3 Addressing security in third party agreements 10.2.1 Third Party Service Delivery

Physical Safeguards		**ISPME Specific Policies**
Facility Access Controls 164.310(a)(1) 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.	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)	9 Physical And Environmental Security 9.1.1 Physical security perimeter (7 policies) 9.1.2 Physical entry controls (26 policies) 9.1.3 Securing offices, rooms, and facilities 9.2.1 Equipment siting and protection 9.2.2 Supporting utilities 9.2.3 Cabling security 9.2.4 Equipment maintenance 9.2.5 Security of equipment off-premises 9.2.6 Secure disposal or re-use of equipment 9.2.7 Removal of property
Workstation Use 164.310(b) “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”	(R)	11.3.1 Password use. 11.3.2 Unattended user equipment 11.3.3 Clear desk and clear screen policy 11.5.1 Secure log-on procedures 11.5.2 User identification and authentication 11.5.3 Password management system 11.5.4 Use of system utilities 11.5.5 Session time-out 11.5.6 Limitation of connection time
Workstation Security 164.310(c) “Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”	(R)	9.1.3 Securing offices, rooms, and facilities 9.2.1 Equipment Siting And Protection (16 policies) 11.3.3 Clear desk and clear screen policy
Device and Media Controls 164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)	9.2.6 Secure disposal or re-use of equipment 9.2.7 Removal of property 10.7.1 Management of removable media 10.7.2 Disposal of media 10.7.3 Information handling procedures 10.5.1 Information Backup (22 policies)

Technical Safeguards (see Sec. 164.312)		**ISPME Specific Policies**
Access Control 164.312(a)(1)	Unique User Identification(R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)	11 Access Control 11.2.1 User registration 11.2.2 Privilege management 11.2.3 User password management 11.2.4 Review of user access rights 11.4 Network Access Control (30+ policies) 11.05 Operating System Access Control (20+ policies) 11.5.2 User identification and authentication 11.5.5 Session time-out 11.5.6 Limitation of connection time 11.5.6-2 Duress Alarm To Safeguard Users
Audit Controls 164.312(b)	(R) “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”	10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.4 Administrator and operator logs 10.10.5 Fault logging 10.2.2 Monitoring and review of third party services 15.3.1 System Audit Controls (3 policies)
Integrity 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	11.5.2 User Identification And Authentication (6 policies) 11.6.1 Information Access Restriction (19 policies) 11.6.2 Sensitive system isolation
Person or Entity Authentication 164.312(d)	(R)	11.5.2 User Identification And Authentication 11.4.2 User authentication for external connections 11.4.3 Equipment identification in networks
Transmission Security 164.312(e)(1)	Integrity Controls (A) Encryption (A)	10.8 Exchanges Of Information And Software 10.8.2 Exchange agreements 10.8.3 Physical media in transit 10.8.4 Electronic messaging 10.9.1 Electronic commerce 12.3 CRYPTOGRAPHIC CONTROLS 12.3.1 Policy on the use of cryptographic controls 12.3.2 Key management

Organizational Requirements 164.314 (R)		**ISPME Specific Policies**
Business Associate Contracts or Other arrangements 164.314 (a)	Contracts must be amended […] to assure that business partners and agents agree to provide reasonable and appropriate security to protect information (and) (C) Report to the covered entity and security violation of which it becomes aware.	6.2.1 Identification of risks related to external parties 6.2.3 Addressing security in third party agreements
Requirements for Group Health Plans 164.314 (b)	Plan documents must be amended […] to assure that business partners and agents agree to provide reasonable and appropriate security to protect information (and) (iv) Report to the Group Health Plan any security incident of which it becomes aware.	VPC can certify that Group Health Plan associates are aware of and agree to abide by the cover entities security policies and procedures. VPC also allows for security incident reporting of business associates via extranets or other online access.
Policies and Procedures and documentation Requirements 164.316		**ISPME Specific Policies**
Policies and Procedures 164.316 (a)	(R) Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart…	ISPME provides over 1400 policies and standards for every aspect of information security. 5.1 INFORMATION SECURITY POLICY 5.1.1 Information security policy document
Documentation (Maintain the policies and procedures in written form) 164.316 (b)	Time Limit (R) – 6 year Availability (R) Updates (R)	5.1.2 Review of the information security policy

[1] Information based on material found in the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, available from the Department and Health and Human Services at http://www.cms.hhs.gov/hipaa/. Policy categories based on Information Security Policies Made Easy, Version 11, by Charles Cresson Wood and published by Information Shield, Inc.

[2] NetIQ and VigilEnt Policy Center (VPC) are registered trademarks of NetIQ Corporation.