



EVMS
HEALTH SERVICES

Patient-Centered Quality Care

Eastern Virginia Medical School

EVMS Health Services

EVMS Pediatric Faculty Associates

**SECURITY
POLICY MANUAL**

For The
Health Insurance Portability and Accountability Act (HIPAA)

06/16/2006

Table of Contents

9.30.00	Overview.....	1
	HIPAA Security Rule Requirements – Administrative	2
	HIPAA Security Rule Requirements – Physical.....	4
	HIPAA Security Rule Requirements – Technical	5
9.30.01	Certification Policy	6
9.30.02	Business Associate Agreement.....	7
9.30.03	Data Contingency Plan	8
9.30.04	Processing Records	9
9.30.05	Information Systems Access.....	10
9.30.06	Internal Audit.....	11
9.30.07	Personnel Security	12
9.30.08	Security Configuration Management.....	13
9.30.09	Security Incident Procedures	14
9.30.10	Security Management Process	15
9.30.11	Termination Procedures.....	16
9.30.12	Training.....	17
9.30.13	Assigned Security Responsibilities.....	18
9.30.14	Media Controls.....	19
9.30.15	Physical Access Controls.....	20
9.30.16	Workstation Use.....	21
9.30.17	Workstation Location.....	22
9.30.18	Emergency Access	23
9.30.19	Technical Security Audit Controls.....	24

Table of Contents

9.30.20 Authorization Control	25
9.30.21 Data Authentication	26
9.30.22 Entity Authentication	27
9.30.23 Communication/Network Controls	28
9.30.24 Data Authentication (Received).....	29
9.30.25 Network Controls.....	30
9.30.26 Electronic Signature (Optional)	31
9.30.27 Collection and Disclosure of PHI on Personal Digital Assistants and PCs.....	32
9.30.28 Portable Computer Policy	33
9.30.29 Password Policy	34

Table of Contents

HIPAA – Transactions and Code Sets	35
9.30.30 Health Care Claims Control.....	36
9.30.31 Health Care Payment and Remittance Advice.....	37
9.30.32 Coordination of Benefits.....	38
9.30.33 Health Care Claim Status Request Response.....	39
9.30.34 Benefit Enrollment and Maintenance	40
9.30.35 Health Care Eligibility/Benefit Inquiry Controls.....	41
9.30.36 Health Care Premium Payments	42
9.30.37 Health Care Services Review.....	43
9.30.38 Code Sets	44

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.00 Overview	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 7

OVERVIEW

EVMS Information Technology Security policies and procedures are based in large part on the legislative mandates of the Department of Health and Human Services' Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition to the regulatory compliance related to patient or protected health information (PHI), significant effort was committed to produce formal documentation of normal standards of operation for use by all information technology providers within the EVMS framework regardless of primary emphasis: clinical, academic, administrative or research.

Throughout the policies and procedures the term EVMS refers to the EVMS enterprise comprised of the following entities:

- Eastern Virginia Medical School (EVMS).
- Eastern Virginia Medical School Health Services (EVMSHS).
- Eastern Virginia Medical School Pediatric Faculty Associates (EVMSPPFA).

The preparation, presentation, adoption, monitoring and revision of these policies are the responsibility of the Information Technology Management Team (ITMT), a subcommittee of the Dean's Information Technology Advisory Council (ITAC) comprised of director level representatives from all major EVMS information technology providers. Throughout the policies and procedures the term ITMT refers to the management personnel of the following areas:

- EVMSHS Information Systems.
- EVMS Business and Financial Information Systems Center.
- EVMS Network Information Center.
- EVMS Data Base Center.
- EVMS Communications Department.
- EVMS Library Services.

HIPAA regulations require the appointment of both a privacy and security officer. The privacy officer is responsible for compliance related to the standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to the health information. The security officer is responsible for compliance related to the standards for administrative, physical, and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information (e-PHI) from unauthorized access, alteration, deletion and transmission. EVMS' privacy officer is a senior administrator within EVMSHS; the security officer is EVMS' chief information officer and chair of the Dean's Information Technology Advisory Council (ITAC).

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.00 Overview	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 2 of 7

Additional information and definitions are available in the EVMS HIPAA Privacy Manual.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.00 Overview

APPROVED:

1/26/2005

CATEGORY: SECURITY

REVISED:

Page 3 of 7

HIPAA SECURITY RULE REQUIREMENTS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS	REQUIRED ADDRESSABLE	EVMS POLICY
Administrative Safeguards				
<u>Security Management Process</u> Prevent, detect, contain and correct security violations	164.308(a)(1)	1. Risk Analysis – assess potential risks and vulnerabilities to confidentiality, integrity and availability of e-PHI 2. Risk management – security measures to reduce risk and vulnerabilities to a reasonable and appropriate level 3. Sanction policy 4. Information system activity review records of information systems activity (e.g., audit logs, access reports, security incident tracking reports)	1. Required 2. Required 3. Required 4. Required	9.30.10
<u>Assigned Security Responsibility</u> Regular review of information services activity (e.g., audit logs, access reports, security incident tracking reports)	164.308(a)(2)		Required	9.30.13
<u>Workforce Security</u> Ensure members of workforce have appropriate access to e-PHI and prevent those workforce members who do not have access from obtaining access to e-PHI	164.308(a)(3)	1. Authorization and/or supervision – determine who has access to e-PHI and supervise their access 2. Workforce clearance procedure – determine that the access of a workforce member to e-PHI is appropriate 3. Termination procedures – termination of access to e-PHI	1. Addressable 2. Addressable 3. Addressable	9.30.11
<u>Information Access Management</u> Implementing policies and procedures consistent with the Security Rule	164.308(a)(4)	1. Isolating health care clearinghouse function – if clearinghouse is part of larger organization, it must implement policies and procedures to protect 3-PHI from unauthorized access by larger organization 2. Access authorization – grant access to e-PHI (e.g., through access to workstation, transaction, program) 3. Access establishment and modification – based on access authorization policies, establish, document, review and modify user's right of access to workstation, transaction, program, process	1. Required 2. Addressable 3. Addressable	9.30.05 9.30.20

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.00 Overview

APPROVED:

1/26/2005

CATEGORY: SECURITY

REVISED:

Page 4 of 7

HIPAA SECURITY RULE REQUIREMENTS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS	REQUIRED ADDRESSABLE	EVMS POLICY
Administrative Safeguards				
<u>Security Awareness and Training</u> Awareness and training program for all members of workforce	164.308(a)(5)	1. Security reminders 2. Protection from malicious software 3. Log-in monitoring – monitor attempts and report discrepancies 4. Password management – creating, changing, and safeguarding passwords	1. Addressable 2. Addressable 3. Addressable 4. Addressable	9.30.06 9.30.12 9.30.29
<u>Security Incident Procedures</u>	164.308(a)(6)	Response and reporting – identify and respond to suspected or known security incidents; mitigate harmful effects; document incidents, mitigation, outcomes	Required	9.30.09
<u>Contingency Plan</u> Respond to an emergency or occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain e-PHI	164.308(a)(7)	1. Data backup plan – create and maintain retrievable exact copies of e-PHI 2. Disaster recovery plan – restore loss of data 3. Emergency mode operation plan – enable continuation of critical business processes for protection of the security or e-PHI while operating in emergency mode 4. Testing and revision of contingency plan 5. Applications and data criticality analysis – assess relative criticality of specific applications and data in support of other contingency plan components	1. Required 2. Required 3. Required 4. Addressable 5. Addressable	9.30.03
<u>Evaluation</u> Periodic technical and non-technical evaluation, based upon standards implemented and subsequently, in response to changes affecting the security of e-PHI, that establishes the extent to which policies and procedures comply with the Security Rule	164.308(a)(8)		Required	9.30.01 9.30.08
<u>Business Associate Contracts and Other Arrangements</u>	164.308(b)(1) 164.314(a)	Written contract or other arrangement	Required	9.30.02

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.00 Overview

APPROVED:

1/26/2005

CATEGORY: SECURITY

REVISED:

Page 5 of 7

HIPAA SECURITY RULE REQUIREMENTS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS	REQUIRED ADDRESSABLE	EVMS POLICY
Physical Safeguards				
<u>Facility Access Controls</u> Limit physical access to electronic information services and the facility in which they are housed, while ensuring that properly authorized access is allowed	164.310(a)(1)	1. Contingency operations – allow facility access in support of restoration of lost data under the disaster recovery plan and emergency operation mode plan in the event of an emergency 2. Facility security plan – safeguard facility and equipment from unauthorized physical access, tampering and theft 3. Access control and validation procedures – 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 4. Maintenance records – document repairs /modifications to physical components of a facility which are related to security (e.g., hardware, walls, doors, locks)	1. Addressable 2. Addressable 3. Addressable 4. Addressable	9.30.15
<u>Workstation Use</u> Specify 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 e-PHI	164.310(b)		Required	9.30.16
<u>Workstation Security</u> Physical safeguards for all workstations that access e-PHI to restrict access to authorized users	164.310(c)		Required	9.30.17
<u>Device and Media Controls</u> Govern the receipt and removal of hardware and electronic media that contain e-PHI into and out of a facility, and the movement of these items within the facility	164.310(d)(1)	1. Disposal – final disposition of e-PHI and/or the hardware or electronic media on which it is stored 2. Media re-use – removal of e-PHI from electronic media before media are made available for re-use 3. Accountability – maintain a record of movements of hardware and electronic media and any person responsible 4. Data backup and Storage – create a retrievable, exact copy of e-PHI, when needed, before movement of equipment	1. Required 2. Required 3. Addressable 4. Addressable	9.30.14

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.00 Overview

APPROVED:
1/26/2005

CATEGORY: SECURITY

REVISED:

Page 6 of 7

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.00 Overview

APPROVED:

1/26/2005

CATEGORY: SECURITY

REVISED:

Page 7 of 7

HIPAA SECURITY RULE REQUIREMENTS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS	REQUIRED ADDRESSABLE	EVMS POLICY
Technical Safeguards				
<u>Access Controls</u> For electronic information services, maintain e-PHI to allow access only to those persons or software programs that have been granted access and rights	164.312(a)(1)	1. Unique user identification – for identifying and tracking user identity 2. Emergency access procedure – for obtaining e-PHI during an emergency 3. Automatic logoff – after predetermined time of inactivity 4. Encryption and decryption	1. Required 2. Required 3. Addressable 4. Addressable	9.30.07 9.30.18 9.30.24
<u>Audit Controls</u> Hardware, software and/or procedural mechanisms that record and examine activity in information services that contain or use e-PHI	164.312(b)		Required	9.30.19 9.30.25
<u>Integrity</u> Protect e-PHI from improper alteration or destruction	164.312(c)(1)	Mechanism to authenticate e-PHI – mechanisms to corroborate that e-PHI has not been altered or destroyed in any unauthorized manner	Addressable	9.30.21 9.30.24
<u>Person or Entity Authentication</u>	164.312(d)		Required	9.30.22
<u>Transmission Security</u> Technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communication network	164.312(e)(1)	1. Integrity controls – ensure that electronically transmitted e-PHI is not improperly modified without detection until disposed of 2. Encryption	1. Addressable 2. Addressable	9.30.23

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.01 Certification	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(8)		

POLICY: It is the policy of EVMS to evaluate all computer systems and corresponding networks to certify the level of security using an approved Certification Plan.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.02 Business Associate Agreement	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.308(b)(1) and § 164.314(a)		

POLICY: It is the policy of EVMS to require all technology contractors who share PHI to execute a Business Associate Agreement that requires the contractor to establish and maintain a written security policy that contains statements of information values, protection responsibilities, and organization commitment to protection of the availability, confidentiality and integrity of data stored or processed in its information systems. The security policy must address a contingency plan for responding to emergencies that includes applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

The agreement provides that the business associate will (1) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic protected health information; (2) ensure that any agent agrees to implement reasonable and appropriate safeguards; (3) report to EVMS any security incident of which it becomes aware; and (4) authorize termination of the agreement by EVMS if it determines that the business associate has violated a material term of the agreement.

EVMS ITMT will use the policy, procedure and form contained in the EVMS HIPAA Privacy Rule manual which contains the necessary modifications related to the security requirements.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.03 Data Contingency Plan	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(7)	

POLICY: It is the policy of EVMS to secure electronic data from damage or loss through the application of periodically tested data contingency and disaster recovery plans.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.04 Processing Records	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: No requirement; SOP Best Practice	

POLICY: It is the policy of EVMS to maintain the integrity of confidential healthcare information using methods designed to safeguard contents from unauthorized access, loss, defacement, tampering or inappropriate disposal.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.05 Information Systems Access	APPROVED: 1/26/2025	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(4)		

POLICY: EVMS' policy is to maintain an adequate level of security to protect EVMS data and information systems from unauthorized access. This associated procedure will define the rules necessary to achieve this protection and to ensure a secure and reliable operation of EVMS information systems.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.06 Internal Audit	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(5)	

POLICY: It is the policy of EVMS to monitor the electronic log-ins, electronic medical record file accesses and any security incidents on a regular basis for client/server systems containing PHI.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.07 Personnel Security	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.312(a)(1)	

POLICY: It is the policy of EVMS to secure all confidential data and information throughout the organization. All individuals expected to utilize computer systems will be assigned an access code subsequent to the execution of an EVMS Confidentiality Statement. Execution of the confidentiality statement is generally completed as part of the Human Resources new employee orientation.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.08 Security Configuration Management	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(8)	

POLICY: It is the policy of EVMS to utilize measures to ensure the security of confidential patient healthcare information located within or in support of the client/server computer software programs of the organization.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.09 Incident Procedure	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(1)	

POLICY: It is the policy of EVMS to monitor and report any breaches of security of confidential patient healthcare information to the Information Technology Management Team (ITMT) for handling by the appropriate administrative management.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.10 Security Management Process	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(1)		

POLICY: It is the policy of EVMS to manage the security of all confidential patient healthcare information judiciously. EVMS believes that all patient healthcare information is confidential and must be kept in a secure manner. EVMS upholds the highest level of security of all confidential patient healthcare information. In the event of any breaches of this security, EVMS will strive to recover the information released in the breach, identify the employee(s) responsible for the breach and discipline those responsible for the breach.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.11 Termination Procedures	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(3)	

POLICY: It is the policy of EVMS to uphold the security of all confidential patient healthcare information when an employee separates from EVMS or at the ending of a business association, by eliminating access, both local and remote, to all EVMS systems on the last work day or earlier if requested by management.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.12 Training	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(5)		

POLICY: It is the policy of EVMS to train all employees on the measures taken to ensure the security of confidential patient healthcare information before system access is granted.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.13 Assigned Security Responsibilities	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308(a)(2)	

POLICY: It is the policy of EVMS to ensure the physical safety of all confidential patient healthcare information. EVMS has assigned responsibility to manage the physical security of this information to the ITMT using established protocols for physical access.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.14 Media Controls	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.310(d)(1)		

POLICY: It is the policy of EVMS to secure and maintain the confidentiality of all patient healthcare information during the delivery, removal and transmission of the information using both physical and technical measures.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.15 Physical Access Controls	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.310(a)(1)	

POLICY: It is the policy of EVMS to restrict access to EVMS property to those employed for the provision of patient care, those providing support for the facility's operations, authorized visitors and students attending EVMS. In addition, technology areas within EVMS use positive locks requiring keys, electronic doors, code keys, access codes and/or coded identification cards. Security will be contacted for any unauthorized individuals attempting to access a restricted area.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.16 Workstation Use	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.310(b)	

POLICY: It is the policy of EVMS to ensure the security of all confidential patient healthcare records by structuring and safeguarding the access to electronic information via workstations by both technical and physical means such as access codes, automatic session timeouts, and restricted login periods.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.17 Workstation Location	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.310(c)	

POLICY: It is the policy of EVMS to ensure the security of all confidential patient healthcare records by structuring the physical access to electronic information through strategically located work stations and documenting the periodic auditing of their placement, environment, implemented security measures, and supervision by completing a Physical Site Survey to be forwarded to the HIPAA Steering Committee for any necessary corrective action.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.18 Emergency Access	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.312(a)(1)	

POLICY: It is the policy of EVMS to ensure the security and confidentiality of patient healthcare information in the event of an emergency or crisis. Short term access codes will be issued to personnel identified by the EVMSHS CEO or his/her designee, as needing specific patient information that may help alleviate/mitigate the emergency or crisis. These access codes will be deactivated when the emergency has been resolved. All other access codes will be restricted during the emergency.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.19 Technical Security Audit Controls

APPROVED:
1/26/2005

CATEGORY: SECURITY

REVISED: **Page 1 of 1**

HIPAA REFERENCE: § 164.312(b)

POLICY: It is the policy of EVMS to record and periodically examine all electronic tracking records created by those accessing and documenting confidential patient healthcare information.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.20 Authorization Control	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.308 (a)(4)	

POLICY: It is the policy of EVMS to restrict the access to confidential healthcare information based on authorization received from the EVMSHS CEO or his/her designee. Special approval may also be required from the EVMS Internal Review Board, the Offices of Education or Student Affairs, depending on the requestor and the defined need.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.21 Data Authentication	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.312(c)(1)	

POLICY: It is the policy of EVMS to ensure that all confidential patient healthcare information has not been altered or destroyed in an unauthorized manner by periodically auditing related electronic log entries.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.22 Entity Authentication	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.312(d)	

POLICY: It is the policy of EVMS to authenticate employees, business associates or other individuals prior to authorizing local or remote access to confidential patient healthcare information. Authentication will be conducted electronically through the use of measures such as access codes, passwords, PINs, callbacks, tokens, or biometrics.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.23 Communication/Network Controls	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.312(e)(1)	

POLICY: It is the policy of EVMS to ensure the validity of confidential patient information being electronically transmitted or stored by utilizing electronic security mechanisms such as batch controls, hashing, check digits and encryption.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.24 Data Authentication (Received)	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: § 164.312(c)(1) and§ 164.312(a)(1)		

POLICY: It is the policy of EVMS to authenticate information transmitted electronically by matching the information sent with the information that is received by using processes such as control totals, record counts, transmission size, and hashing.

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.25 Network Controls	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: § 164.312(b)	

POLICY: It is the policy of EVMS to protect confidential healthcare information by using specific controls when transmitting or receiving confidential healthcare information such as alarms, logs, event recording and restricted logins.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.26 Electronic Signature (Optional)	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: No requirement; SOP Best Practice		

POLICY: It is the policy of EVMS to utilize electronic signatures to document access to confidential healthcare information. Electronic signatures will be defined as: digital certificates, combined access codes and passwords, PINs, biometric data, tokens and official EVMS email accounts.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.27 Collection and Disclosure of PHI on Personal Digital Assistants and PCs	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: No requirement; SOP Best Practice		

POLICY: It is the policy of EVMS to control collection and disclosure of protected health information (PHI) on Personal Digital Assistants (PDAs) and all personal computing devices by employees and students at the EVMS.

All EVMS employees and students are responsible for the protection from improper use or disclosure of all PHI contained on their PDAs and personal computing devices. Security of data maintained and stored on computers and portable electronic devices is subject to the provisions of relevant state and federal statutes and regulations, and the federal Health Insurance Portability and Accountability Act (HIPAA) and EVMS security policies. Unauthorized use or disclosure may be cause for disciplinary action.

Departments and divisions of EVMS wishing to mandate the additional collection of PHI unrelated to the authorized management of an EMR, on PDAs and/or personal computing devices by one or more employees or students have to fully comply with all privacy protection procedures required by EVMS. Prior to implementing any such mandate to collect non-EMR PHI, the Health System element shall submit a privacy protection proposal to and obtain written approval from a body to be designated by the HIPAA Steering Committee or from the EVMSHS CEO or his/her designee.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.28 Portable Computer Policy	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: No requirement; SOP Best Practice		

POLICY: EVMS has adopted the Portable Computer Policy to comply with: The Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is the policy of EVMS to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. The right of any person to use an EVMS portable computer to download, maintain or transmit PHI unrelated to the authorized management of an EMR, is conditioned upon agreement to and signature of the Portable Computer Agreement which stipulates user responsibilities and required security measures.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.29 Password Policy	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 2
HIPAA REFERENCE: § 164.308(a)(5)		

POLICY: To gain access to EVMS information systems, authorized users, as a means of authentication must supply individual user passwords. These passwords must conform to certain rules contained in this document.

Who is Affected: This policy affects all employees and students of EVMS and its subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

Affected Systems: This policy applies to all computer and communication systems owned or operated by EVMS and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

User Authentication: All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an individual user will be deleted or disabled.

Password Storage: Passwords will not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

Application Passwords Required: All client/server programs, including third party purchased software and applications developed internally by EVMS must be password protected.

Choosing Passwords: All user-chosen passwords must be at least six (6) but not more than thirty-two (32) alpha-numeric characters. The use of control characters and other non-printing characters is prohibited. All users will be automatically forced to change their passwords every 180 days (or less). To obtain a new password, a user must present suitable identification.

Changing Passwords: All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties. All users will change their passwords at least once every one-hundred-eighty (180) days.

Password Constraints: The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe and subsequently recover them. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b)

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.29 Password Policy

APPROVED:
1/26/2005

CATEGORY: SECURITY

REVISED: **Page 2 of 2**

HIPAA REFERENCE: § 164.308(a)(5)

temporarily disabled for no less than three minutes, or (c) if dial-up or other external network connections are involved, disconnected.

HIPAA

TRANSACTIONS AND CODE SETS

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.30 Health Care Claims Control	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically submit healthcare claims to health plans.

Health Care claims will be filed electronically utilizing the following transaction platforms for submission:

- Retail and professional pharmacy claims: NCPDP Telecommunications Standard Format Version 5.1 and NCPDP Batch Standard 1.0
- Dental claim: ASC X12N 837 - healthcare claim: dental, version 4010
- Professional claim: ASC X12N 837 - healthcare claim: professional, version 4010 implementation and HCFA (CMS) National Standard Format (NSF), version 002.00
- Institutional claim: ASC X12N 837 - healthcare claim: institutional, version 4010 implementation and HCFA (CMS) Uniform Bill (UB-92) version 4.1

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.31 Health Care Payment and Remittance Advice	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically receive an explanation of healthcare payment or remittance advice from a patient's health plan.

- This transaction is used by health plans to make payments to the EVMS' financial institution.
- This transaction may be used to receive explanations of benefits or remittance advices from a patient's health plan.
- Receiving healthcare payment and remittance advice information will be conducted using the following transaction platform:

ASC X12N 835 - Health Care Claim Payment/Advice, Version 4010

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.32 Coordination of Benefits	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically transmit patient healthcare claims and billing payment information when coordinating benefits is required.

- This transaction is to be used to transmit healthcare claims to one insurer who in turn will submit the claim on to the next insurer if applicable.
- Coordination of benefits may be completed without additional intervention by the EVMS or any patient intervention.
- Health Care claims will be filed electronically utilizing the following transaction platforms for submission:

➔Professional Claim: ASC X12N 837 - healthcare claim:
professional, version 4010 implementation and HCFA (CMS)
National Standard Format (NSF), version 002.00

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.33 Health Care Claim Status Request Response	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically request the status of a healthcare claim submitted to a patient's health plan.

- The purpose of accessing this platform is to obtain the current status of the claim.
- Status information can be requested at two levels:
- Level 1: Information about the entire claim.
- Level 2: Information at the service line level to obtain the status of a specific service within the claim.
- ASC X12N 276 Health Care Claim Status Request and Response (004010X093) is the platform to be used to request status information from a health plan.
- ASC X12N 277 Health Care Claim Status Request and Response (004010X093) is the platform to be used by the health plan to transmit the current status of the health claim back to the EVMS. This transaction set can identify where in the process the claim is: accepted/rejected, claim pending, development, suspended, information and finalized status.

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.34 Benefit Enrollment and Maintenance	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically request patient enrollment and health plan maintenance information.

- The use of this policy would be to exchange information between health plan sponsors and the EVMS.
- This transaction provides enrollment data such as subscriber and dependents, employer information and other healthcare provider information. It would be used to enroll and disenroll both the subscriber and any covered dependents.
- The transaction data elements for the ASC X12 834 platform are defined as either required or conditional.
- This transaction platform may have other secondary uses such as analyses of healthcare utilization, quality, cost and demographics.
- Requesting benefit enrollment and maintenance information will be conducted using the following transaction platform:

➔ ASC X12N 834 - Benefit Enrollment and Maintenance
Transaction Set (004010X095)

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.35 Health Care Eligibility/Benefit Inquiry Controls	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically verify a patient's eligibility and benefits within a health insurance plan.

- Evaluating eligibility is to be used for simple status requests such as a query for all benefits and coverage conditions, eligibility status (whether the patient is active in the health plan), maximum benefits (policy limits), exclusions, in-plan/out-of-plan benefits, coordination of benefits information, deductibles and co-payments.
- Evaluating eligibility for specific requests may be related to specific clinical procedures or include procedure coverage dates, procedure coverage maximum, amounts for deductible, co-insurance, co-payment or patient responsibility, coverage limitations; and noncovered amounts.
- Evaluating eligibility only identifies a patient's eligibility and benefits. This does not provide a history of benefit use.
- Evaluating eligibility will be conducted using the following transaction platform:
 - ➔ ASC X12N 270/271 - Health Care Eligibility Inquiry and Response (004010X092) Version 4010

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.36 Health Care Premium Payments	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically transmit employee health plan premiums.

- These transactions are used by the EVMS to make and keep track of health plan premiums for the employees.
- Tracking health plan premium payments will be conducted using the following transaction platform:

➔ ASC X12N 820 - Payment Order/Remittance Advice
Transaction Set (004010X061)

EASTERN VIRGINIA MEDICAL SCHOOL		
POLICY: 9.30.37 Health Care Services Review	APPROVED: 1/26/2005	
CATEGORY: SECURITY	REVISED:	Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets		

POLICY: It is the policy of EVMS to electronically request healthcare services from a patient's health plan.

- The EVMS may request information about different episodes of healthcare. These include: reviews for treatment, authorization, specialty referrals, pre-admission certifications, certifications for healthcare services (such as home health and ambulance), extension of certifications and certification appeals.
- Requesting review for healthcare services will be conducted using the following transaction platform:
 - ➔ ANSI ASC X12N 278 - Health Care Services and Review and Response (004010X094)

EASTERN VIRGINIA MEDICAL SCHOOL

POLICY: 9.30.38 Code Sets	APPROVED: 1/26/2005
CATEGORY: SECURITY	REVISED: Page 1 of 1
HIPAA REFERENCE: Transactions and Code Sets	

POLICY: It is the policy of EVMS to utilize uniform codes when documenting episodes of patient care.