

| STANDARD | IMPLEMENTATION SPECIFICATIONS | DESCRIPTION | REQUIRED/ ADDRESSABLE | COMPLETED & DOCUMENTED |
|---|------------------------------------|---|-----------------------|------------------------|
| ADMINISTRATIVE SAFEGUARDS | | | | |
| Security Management Process | | Policies and procedures to prevent, detect, contain and correct security violations. | Required | |
| | 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. | Required | |
| | Risk Management | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level based on the size, complexity and capabilities of the covered entity. | Required | |
| | Sanction Policy | Implement and apply appropriate sanctions against employees that do not comply with security policies and procedures of the covered entity. | Required | |
| | Information System Activity Review | Implement procedures to regularly review system activity records like audit logs, access reports and security incident tracking reports. | Required | |
| Assigned Security Responsibility | None | Assign a Security Officer who is responsible for the development and implementation of policies and procedures relating to compliance with the Security Rule. | Required | |
| Workforce Security | | Implement policies and procedures to ensure that all employees have appropriate access to electronic protected health information and to prevent those employees that do not have access from gaining it. | Required | |
| | Authorization and/or Supervision | Implement procedures for the authorization and/or supervision of employees that work with electronic protected health information and for authorization and/or supervision of areas where it could be accessed. | Addressable | |
| | Workforce Clearance Procedure | Implement procedures to determine that an employees access to electronic protected health information is appropriate. | Addressable | |
| | Termination Procedures | Implement procedures to end an employees access to electronic protected health information on termination or change to a job that no longer requires it. | Addressable | |
| Information Access Management | | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the requirements for use and disclosure of information under the Privacy Rule. | Required | |

| STANDARD | IMPLEMENTATION SPECIFICATIONS | DESCRIPTION | REQUIRED/ ADDRESSABLE | COMPLETED & DOCUMENTED |
|--|---|---|-----------------------|------------------------|
| | Isolating Health Care Clearinghouse Functions | If a covered entity is a sub-part of a larger entity, implement policies and procedures to protect electronic protected health information of the covered entity from unauthorized access by the larger organization. | Required | |
| | Access Authorization | Implement policies and procedures for granting access to electronic protected health information (e.g. through workstation access, transaction access, program or process access). | Addressable | |
| | Access Establishment and Modification | Implement policies and procedures that based on the covered entity's Access Authorization procedures establishes, documents and provides for review and modification of a employees right to access. | Addressable | |
| Security Awareness and Training | | Implement a security awareness and training program for all employees including management. | Required | |
| | Security Reminders | Sending of periodic security updates to employees. | Addressable | |
| | Protection from Malicious Software | Implement procedures for guarding against, detecting and reporting malicious software (i.e. a virus or other program designed to damage or disrupt a system). | Addressable | |
| | Log-in Monitoring | Implement procedures for monitoring log-in attempts and reporting discrepancies. | Addressable | |
| Security Incident Procedures | | Implement policies and procedures to address security incidents (i.e. attempted or successful, unauthorized access, use, disclosure, modification or destruction of information or interference with system operations). | Required | |
| | Response and Reporting | Implement procedures to identify and respond to suspected or known security incidents, to the extent possible mitigate any harmful effects and document each security incident and its outcome. | Required | |
| Contingency Plan | | Establish, and implement if necessary, policies and procedures for responding to an emergency or other threat (e.g. fire, vandalism, system failure, natural disaster) that damages systems that contain electronic protected health information. | Required | |
| | Data Backup Plan | Establish and implement procedures to create and maintain exact copies of electronic protected health information. | Required | |
| | Disaster Recovery Plan | Establish, and implement if necessary, procedures to restore any loss of data. | Required | |

| STANDARD | IMPLEMENTATION SPECIFICATIONS | DESCRIPTION | REQUIRED/ ADDRESSABLE | COMPLETED & DOCUMENTED |
|-------------------------------------|--|--|-----------------------|------------------------|
| | Emergency Mode Operation Plan | Establish, and implement if necessary, procedures to enable continuation of critical business processes that provide security to electronic protected health information while operating in emergency mode. | Required | |
| | Testing and Revision Procedures | Implement procedures for periodic testing and revision of contingency plans. | Addressable | |
| | Applications and Data Criticality Analysis | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Addressable | |
| Evaluation | None | Develop policies and procedures for performance of periodic technical and non-technical review to determine the extent to which current policies and procedures continue to meet the requirements of the Security Rule. | Required | |
| Business Associate Contracts | None | Obtain satisfactory assurance, in the form a written contract or agreement between the covered entity and the business associate, that the business associate will safeguard the information. | Required | |
| PHYSICAL SAFEGUARDS | | | | |
| Facility Access Controls | | Implement policies and procedures to limit physical access to electronic information systems and the facilities where they are housed, while ensuring properly authorized access is allowed. | Required | |
| | Contingency Operations | Establish and implement as necessary procedures to allow facility access in support of restoration of lost data under the disaster recovery plan and in support of emergency mode operations in the event of an emergency. | Addressable | |
| | Facility Security Plan | Implement policies and procedures to safeguard the facility and equipment inside from unauthorized physical access, tampering or theft. | Addressable | |
| | Access Control and Validation Procedures | Implement procedures to control and validate a person's facility and software access based on their role or function. Procedures must address visitor control and access control for purposes of testing and revising software programs. | Addressable | |
| | Maintenance Records | Implement policies and procedures to document repairs and modifications to the physical components of the facility that are related to security (e.g. hardware, walls, doors and locks). | Addressable | |

| STANDARD | IMPLEMENTATION SPECIFICATIONS | DESCRIPTION | REQUIRED/ ADDRESSABLE | COMPLETED & DOCUMENTED |
|----------------------------------|--------------------------------------|--|------------------------------|-----------------------------------|
| Workstation Use | None | Implement policies and procedures, by workstation or class of workstation that can access electronic protected health information, that specify the function to be performed at the workstation, the manner in which it is to be performed and the physical attributes of the workstation. | Required | |
| Workstation Security | None | Implement physical safeguards to restrict access to authorized users at all workstations that can access electronic protected health information. | Required | |
| 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. | Required | |
| | Disposal | Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media it resides on. | Required | |
| | Media Re-Use | Implement procedures for removal of electronic protected health information from electronic media before the media is made available for re-use. | Required | |
| | Accountability | Maintain a record of the movements of hardware, electronic media and any person responsible for hardware or media. | Addressable | |
| | Data Backup and Storage | Implement procedures to create, as necessary, a retrievable, exact copy of electronic protected health information prior to movement of equipment. | Addressable | |
| TECHNICAL SAFEGUARDS | | | | |
| Access Control | | 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. | Required | |
| | Unique User Identification | Assign a unique name and/or number for identifying and tracking user identity. | Required | |
| | Emergency Access Procedure | Establish, and implement as necessary, procedures for obtaining necessary electronic protected health information during an emergency. | Required | |
| | Automatic Logoff | Implement electronic procedures to terminate an electronic session after a predetermined time of inactivity. | Addressable | |

| STANDARD | IMPLEMENTATION SPECIFICATIONS | DESCRIPTION | REQUIRED/ ADDRESSABLE | COMPLETED & DOCUMENTED |
|--|---|---|------------------------------|-----------------------------------|
| | Encryption and Decryption | Implement a mechanism to encrypt and decrypt electronic protected health information. | Addressable | |
| Audit Controls | None | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Required | |
| Integrity | | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Required | |
| | Mechanism to Authenticate Electronic Protected Health Information | Implement electronic mechanisms to corroborate that information has not been altered or destroyed in an unauthorized manner | Addressable | |
| Person or Entity Authentication | None | Implement procedures to verify that the person or entity requesting access to electronic protected health information is the person or entity claimed. | Required | |
| 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. | Required | |
| | Integrity Controls | Implement security measures to ensure that electronic protected health information is not improperly modified without detection. | Addressable | |
| | Encryption | Implement a mechanism to encrypt electronic protected health information when appropriate. | Addressable | |
| ORGANIZATIONAL REQUIREMENTS | | | | |
| Requirements for Group Health Plans | None | If a group health plan is receiving electronic protected health information, other than summary health and enrollment/termination information as allowed under the Privacy Rule, it must amend its plan in relation to the Security Rule. | Required | |
| DOCUMENTATION | | | | |
| Documentation | | Maintain, in written or electronic form, the policies and procedures implemented to comply with the Security Rule. It is also required to document any action or assessment that is required under the Security Rule. | Required | |
| | Time Limit | Documentation of policies, procedures and actions under the Security Rule are to be maintained for 6 years from the later of the date they were created or the date they were last in effect. | Required | |
| | Availability | Documentation must be available to those persons responsible for | Required | |

Provided by UMR for informational purposes only.

| STANDARD | IMPLEMENTATION SPECIFICATIONS | DESCRIPTION | REQUIRED/ ADDRESSABLE | COMPLETED & DOCUMENTED |
|----------|-------------------------------|---|-----------------------|------------------------|
| | | implementing the procedures. | | |
| | Updates | Documentation must be reviewed periodically and updated as changes are made to the policies and procedures. | Required | |