DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Security and Standards Group (SSG)

CMS Information Security Acceptable Risk Safeguards (ARS)

Draft Version 1.1
March 14, 2003

Table of Contents

Preface

All federal systems require security controls to protect its information assets. These controls cover several areas of security from the physical environment to auditing and logging. The Centers for Medicare & Medicaid Services (CMS) developed the Acceptable Risk Safeguards (ARS) to define information security minimum requirements for CMS systems based on the system's designated system security level. (See CMS Information Security Levels [cms.hhs.gov/it/security]).

The ARS is based on industry-standards and past experience with large Federal government agencies and private-sector partners. It complies with the CMS Information Security Policy by providing a defense-in-depth security structure with all information access limited by a least-privilege approach and a need-to-know basis. It is not intended to be an all-inclusive list of security controls and will be regularly updated to reflect the changing technological environment. The ARS is not intended to replace a system owner's due diligence to incorporate controls to mitigate risk to CMS and its information assets. These controls must be considered through the risk management process and employed when appropriate and feasible.

The target audience for this standard is the System Owner and System Maintainer/Developer. They have primary responsibility for determining the system security requirements and ensuring their implementation. However, any entity involved in the System Development Life Cycle could use this information to understand the baseline security protections required by CMS. For additional information on how the ARS integrates into the CMS security life cycle refer to cms.hhs.gov/it/security.

The standards in the ARS reflect the minimum thresholds for information security controls. A system may be required to meet additional, higher-level or more rigorous, information protection requirements as mandated by specific Federal, legal, program, or accounting sources. For example, the CMS ARS, section 11.2 Application Auditing, states that for systems with a HIGH system security level, the logs will be retained for 90 days and then archived for 1 year. However, the National Archives and Records Administration has determined that Audit Files (NC1-440-78-1, Item B) be retained for 4 years after completion of the audit. The CMS system must be developed to meet these higher-level standards where applicable. **The CMS ARS shall not be construed to relieve or waive these other standards.**

How to Use This Document

The CMS ARS is divided into eleven security service areas:

1. Physical
2. Personnel

3. Organizational Practices
4. Security Management
5. Certification & Accreditation
6. Network
7. System
8. Application
9. Data
10. Vulnerability Assessments
11. Auditing & Logging

Each security service area contains the applicable security standards with the minimum controls by system security level i.e., HIGH, MODERATE and LOW. These standards are designed to assist the system owner and system maintainer/developer in defining the information security requirements for their system.

First, the system owner needs to determine the system's System Security Level based on the CMS Information Security Levels (cms.hhs.gov/it/security). Since the ARS controls are represented by System Security Level, the required controls for a particular system will be based on the designated level.

The controls within the ARS that may apply will depend on the scope of the system and its processing environment (e.g., a database on an Internet site as opposed to one on a non-public access mainframe, a General Support System [GSS] vs. a Major Application [MA] system). Another consideration is whether or not the system is covered by higher-level controls, (e.g., an MA that inherits the controls from the GSS on which it operates, or a GSS or MA that inherits the controls of a Master Plan).

Even though a system may need to be covered by a specific control, the system owner may not have to implement that control as long as it can demonstrate that the control is satisfied by a higher-level control. The system owner assisted by the system maintainer/developer is responsible for evaluating all information security areas within the ARS and determining the appropriateness for their system.

NOTE:
1) These standards are the minimum thresholds for the various controls defined. A system owner may choose to strengthen the controls ensuring the best possible protection of CMS information and information systems.

2) Sometimes controls cannot be implemented even at the minimum level due to resource issues such as funding and personnel constraints or hardware/software limitations. Alternative or compensating safeguards can be implemented to reduce the risk to CMS. This must be considered as part of risk management and the alternative or compensating controls must be documented in the information security risk assessment and system security plan.

1. Physical Security Standards

The physical security standards detailed in this section are intended to ensure protection of physical resources, and the information these resources contain. Security standards are included which focus upon both the protection of facilities and the protection of critical systems. Unauthorized physical access frequently results in the compromise of system security and information confidentiality. This section details methods for securing physical resources, including sensitive resources contained within and external to CMS facilities. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Physical Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
1.1 Physical Access to Data Centers and System Facilities	Control data center/facility access through door and window locks.	Control data center/facility access through door and window locks, and with security staff. Access can be gained using smart card/PIN combination.	Control data center/facility access through door and window locks, and with security staff. Access can be gained using physical authentication devices, such as biometrics and/or smart card/PIN combination.
1.2 Infrastructure Facility Access	Prohibit public access to infrastructure assets, including power generators, HVAC systems, and telephone/wiring closets.	Allow access to infrastructure assets, including power generators, HVAC systems, and telephone/wiring closets by authorized maintenance personnel only.	Allow access to infrastructure assets, including power generators, HVAC systems, and telephone/wiring closets by explicitly required authorized maintenance personnel only.

Physical Security Standards		System Security Level		
		Low	Moderate	High
1.3	Physical Complex Access	Restrict public access to public areas only.	Restrict access to grounds/facilities to authorized persons only.	Restrict access to grounds/facilities to authorized persons only.
1.4	Data Center Environment	Data center must meet the minimum requirements as established by the FISCAM.	Data center must meet the minimum requirements as established by the FISCAM.	Data center must meet the minimum requirements as established by the FISCAM.
1.5	Server Environment	Store and operate servers in physically secure environments protected from unauthorized access.	Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access must be monitored and recorded.	Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access must be monitored and recorded.
1.6	Off-site Physical Repair of Systems	Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel.	Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel.	Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel.
1.7	On-site Physical Repair of Systems	Access to system for repair must be by authorized personnel only.	Physical repair of servers must be within protected environments. Access to system for repair must be by authorized personnel only.	Physical repair of servers must be within protected environments. Access to system for repair must be by authorized personnel only.

Physical Security Standards	System Security Level		
	Low	Moderate	High
1.8 Power Surge Protection	Power surge protection must be implemented for all computer equipment.	Power surge protection must be implemented for all computer equipment.	Power surge protection must be implemented for all computer equipment.
1.9 Environmental Controls	Monitor specific control alarms. Evaluate level of alert and follow prescribed guidelines for that alert level.	Implement and monitor response procedures for specific control alarms. Alert component management of possible loss of service and/or media. Evaluate level of alert and follow prescribed guidelines for that alert level. Report damage and provide remedial action. Implement contingency plan.	Implement and monitor response procedures for specific control alarms. Alert component management of possible loss of service and/or media. Evaluate level of alert and follow prescribed guidelines for that alert level. Report damage and provide remedial action. Implement contingency plan.
1.10 Physical Ports	Disable any physical ports (e.g. wiring closets, patch panels, etc) not in use.	Disable any physical ports (e.g. wiring closets, patch panels, etc) not in use.	Disable any physical ports (e.g. wiring closets, patch panels, etc) not in use.

2. Personnel Security Standards

Due to the nature of personnel security, the standards are applied by the role of a person/persons and their corresponding duties and responsibilities (not by system security level). Personnel security is critical for the protection of CMS information asset. A complementary information security standards for personnel based on role will be developed at a future date.

The personnel security standards are intended to ensure protections of CMS resources, and the information contained within these resources. Information security standards are included which focus upon both CMS employees and contractor personnel that have access to CMS systems and CMS information. Inadequate personnel security protections frequently result in the compromise of system security and information confidentiality. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Personnel Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
2.1 Personnel Security	See CMS Information Security Handbook; Issue Specific Policies.	See CMS Information Security Handbook; Issue Specific Policies.	See CMS Information Security Handbook; Issue Specific Policies.

3. Organizational Practice Security Standards

This section focuses primarily on security standards at the organizational level. The standards included in this section enable CMS to implement security at an organizational level. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Organizational Practice Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
3.1 Acceptable Use & Sanctions for Violation (Rules of Behavior)	Define user roles, responsibilities and expectations for computer and network use. Develop, implement and enforce organizational sanctions for policy violations.	Define user roles, responsibilities and expectations for computer and network use. Develop, implement and enforce organizational sanctions for policy violations.	Define user roles, responsibilities and expectations for computer and network use. Develop, implement and enforce organizational sanctions for policy violations.
3.2 Information Sensitivity Assessment (ISA)	Prepare an ISA for the system prior to project initiation (See CMS Integrated IT Investment Roadmap, Section 10.5 of the CMS Business Case Analysis).	Prepare an ISA for the system prior to project initiation (See CMS Integrated IT Investment Roadmap, Section 10.5 of the CMS Business Case Analysis).	Prepare an ISA for the system prior to project initiation (See CMS Integrated IT Investment Roadmap, Section 10.5 of the CMS Business Case Analysis).
3.3 Acquisitions and Grants	All contracts and SOWs that require development or access to CMS information must include language requiring adherence to CMS security policies and standards.	All contracts and SOWs that require development or access to CMS information must include language requiring adherence to CMS security policies and standards.	All contracts and SOWs that require development or access to CMS information must include language requiring adherence to CMS security policies and standards.

Organizational Practice Security Standards	System Security Level		
	Low	Moderate	High
3.4 Commissioning and De-Commissioning of Equipment	Abide by CMS configuration management procedures, including testing, updating equipment inventory and system schematics.	Abide by CMS configuration management procedures, including testing, updating equipment inventory and system schematics.	Abide by CMS configuration management procedures, including testing, updating equipment inventory and system schematics.
3.5 Help Desk Support Procedures	Require user identification for any transaction that has information security implications.	Require user identification for any transaction that has information security implications.	Require user identification for any transaction that has information security implications.
3.6 Warning Banners at System and Network Logon	Notify users that CMS maintains ownership and responsibility for its computer systems, and users must adhere to CMS security policy. Describe legal requirements for data confidentiality and system use, and define organizational and legal sanctions for violation. Develop and implement warning banners in conjunction with legal counsel.	Notify users that CMS maintains ownership and responsibility for its computer systems, and users must adhere to CMS security policy. Describe legal requirements for data confidentiality and system use, and define organizational and legal sanctions for violation. Develop and implement warning banners in conjunction with legal counsel.	Notify users that CMS maintains ownership and responsibility for its computer systems, and users must adhere to CMS security policy. Describe legal requirements for data confidentiality and system use, and define organizational and legal sanctions for violation. Develop and implement warning banners in conjunction with legal counsel.

Organizational Practice Security Standards	System Security Level		
	Low	**Moderate**	**High**
3.7 Privacy Policy Display	Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.	Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.	Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.
3.8 Encryption	If used, a FIPS approved encryption method at a minimum of AES encryption with a 128-bit.	A FIPS approved encryption method at a minimum of AES encryption with a 128-bit key.	A FIPS approved encryption method at a minimum of AES encryption with a 128-bit key.
3.9 Passwords	Minimum of six alphanumeric and/or special characters.	Minimum of eight alphanumeric and/or special characters.	Minimum of eight alphanumeric and/or special characters with a number embedded in the password.
3.10 Passwords Changes	Automatically force users (including administrators) to change account and system account passwords every 60 days.	Automatically force users (including administrators) to change account and system account passwords every 60 days.	Automatically force users (including administrators) to change account and system account passwords every 60 days.
3.11 Password History	Automatically force users to select one unique password prior to reusing a previous one.	Automatically force users to select six unique passwords prior to reusing a previous one.	Automatically force users to select six unique passwords prior to reusing a previous one.

Organizational Practice Security Standards	System Security Level		
	Low	Moderate	High
3.12 System Administrator Password	System Administrators must use a unique UserID and password while performing administrator functions. This UserID cannot be shared with anyone and must be different from the administrator's own personal UserID.	System Administrators must use a unique UserID and password while performing administrator functions. This UserID cannot be shared with anyone and must be different from the administrator's own personal UserID.	System Administrators must use a unique UserID and password while performing administrator functions. This UserID cannot be shared with anyone and must be different from the administrator's own personal UserID.

Organizational Practice Security Standards	System Security Level		
	Low	Moderate	High
3.13 Documentation	Develop system documentation to describe the system's purpose, description, technical operations and access, maintenance, and required personnel training to include administrators and users. Maintain an updated list of related system's operations and security documentation. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Labeling and Securing Hard Copy Information" standard for security of hard copies depending on data sensitivity included in the documentation.	Develop system documentation to describe the system's purpose, description, technical operations and access, maintenance, and required personnel training to include administrators and users. Document the system's configuration, and procedures in support of system access administration and operations. Update documentation upon changes in system functions and processes. Maintain an updated list of related system's operations and security documentation. Must include date and version number on all formal system documentation. Refer to "Labeling and Securing Hard Copy Information" standard for security of hard copies depending on data sensitivity included in the documentation.	Develop system documentation to describe the system's purpose, description, technical operations and access, maintenance, and required personnel training to include administrators and users. Document the system's configuration, and procedures in support of system access administration and operations. Update documentation upon changes in system functions, processes, and configuration, performing annual contingency tests and/or system audits. Maintain an updated list of related system's operations and security documentation. Must include date and version number on all formal system documentation. Refer to "Labeling and Securing Hard Copy Information" standard for security of hard copies depending on data sensitivity included in the documentation.

Organizational Practice Security Standards	System Security Level		
	Low	Moderate	High
3.14 Security in the System Development Life Cycle	Must comply with the information security steps of IEEE 12207.0 standard for SDLC as defined by CMS and/or the CMS Roadmap	Must comply with the information security steps of IEEE 12207.0 standard for SDLC as defined by CMS and/or the CMS Roadmap	Must comply with the information security steps of IEEE 12207.0 standard for SDLC as defined by CMS and/or the CMS Roadmap

4. Security Management Standards

This section focuses primarily on security standards for the management and oversight of information security. The standards included in this section enable CMS to effectively manage its information security program. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Security Management Standards	**System Security Level**		
	Low	**Moderate**	**High**
4.1 Program and Functional Managers Security Awareness Training	Receive awareness training in computer security basics; implementation level training in security planning and management and computer security policy and procedures; and performance level training in contingency planning and systems life cycle management for information security.	Receive awareness training in computer security basics; implementation level training in security planning and management and computer security policy and procedures; and performance level training in contingency planning and systems life cycle management for information security.	Receive awareness training in computer security basics; implementation level training in security planning and management and computer security policy and procedures; and performance level training in contingency planning and systems life cycle management for information security.
4.2 Revocation of Access for Terminated Employees and Contractors	Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked within 8 hours of termination.	Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked within 1 hour of termination.	Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

Security Management Standards	System Security Level		
	Low	Moderate	High
4.3 End-User Security Awareness Training	Receive prior to access to systems: awareness training in computer security basics; security planning and management; systems life cycle management; and performance level training in computer security policies and procedures and contingency planning. Training is provided upon employment, promotion, when job responsibilities change, and when software upgrades impact end-user. Security awareness training must be refreshed once per year.	Receive prior to access to systems awareness training in computer security basics; security planning and management; systems life cycle management; and performance level training in computer security policies and procedures and contingency planning. Training is provided upon employment, promotion, when job responsibilities change, and when software upgrades impact end-user. Security awareness training must be refreshed once per year.	Receive prior to access to systems: awareness training in computer security basics; security planning and management; systems life cycle management; and performance level training in computer security policies and procedures and contingency planning. Training is provided upon employment, promotion, when job responsibilities change, and when software upgrades impact end-user. Security awareness training must be refreshed once per year.

Security Management Standards	System Security Level		
	Low	**Moderate**	**High**
4.4 Contractor Access	Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor’s ability to adhere to and support CMS security policy.	Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor’s ability to adhere to and support CMS security policy.	Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with only that system and physical access that is explicitly required, and must agree to and support the CMS security policy. The contractor selection process must assess the contractor’s ability to adhere to and support CMS security policy.
4.5 Review System Access during Extraordinary Personnel Circumstances	Reduce or disable system access level based upon the circumstance prior to user notification.	Reduce or disable system access level based upon the circumstance prior to user notification.	Reduce or disable system access level based upon the circumstance prior to user notification.
4.6 Designate an Information System Security Officer (ISSO)	Designate an ISSO for each component with roles and responsibilities of the position clearly defined.	Designate an ISSO for each component with roles and responsibilities of the position clearly defined.	Designate an ISSO for each component with roles and responsibilities of the position clearly defined.

Security Management Standards	System Security Level		
	Low	Moderate	High
4.7 Network Interconnection	Ensure remote location(s) follow all CMS information security policies and obtain a signed interconnection security agreement. Document interconnection in the System Security Plan for the CMS System that is interconnected to the remote location.	Ensure remote location(s) follow all CMS information security policies and obtain a signed interconnection security agreement. Document interconnection in the System Security Plan for the CMS System that is interconnected to the remote location.	Ensure remote location(s) follow all CMS information security policies and obtain a signed interconnection security agreement. Document interconnection in the System Security Plan for the CMS System that is interconnected to the remote location.
4.8 Incident Response	Implement system incident response procedures; assign lead for incident handling and develop chain of custody for forensic evidence, follow CMS Computer Security Incident Handling Procedures.	Implement system incident response procedures; assign lead for incident handling and develop chain of custody for forensic evidence; follow CMS Computer Security Incident Handling Procedures.	Implement system incident response procedures; assign lead for incident handling and develop chain of custody for forensic evidence; follow CMS Computer Security Incident Handling Procedures.

5. Certification and Accreditation Standards

This section focuses primarily on security standards for the certification and accreditation of CMS systems. The standards included in this section enable the authorizing official (CMS CIO) make a credible, risk-based decision on whether to place a system into operation. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Certification and Accreditation Standards	**System Security Level**		
	Low	**Moderate**	**High**
5.1 Assign Responsibility for Security within Each System	Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system	Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system.	Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system.
5.2 Information Security Risk Assessment (RA) for Each System	Document the risk and safeguards of the system according to the CMS Information Security RA Methodology.	Document the risk and safeguards of the system according to the CMS Information Security RA Methodology.	Document the risk and safeguards of the system according to the CMS Information Security RA Methodology.
5.3 Review of Security Controls	Review the security controls when significant modifications are made to the system, but at least every three years.	Review the security controls when significant modifications are made to the system, but at least every year.	Review the security controls when significant modifications are made to the system, but at least every year.

Certification and Accreditation Standards	System Security Level		
	Low	**Moderate**	**High**
5.4 System Contingency Plan	Contingency plan should be tested as needed.	Contingency plan must be current and executable. The plan must be tested once every two years or when a major change is made to ensure proper functionality.	Contingency plan must be current and executable. The plan must be tested once every year or when a major change is made to ensure proper functionality.
5.5 Disaster Recovery Plan	Disaster recovery plan tested as needed.	Disaster recovery plan must be current and executable. The plan must be tested once every two years or when a major change is made to ensure proper functionality.	Disaster recovery plan must be current and executable. The plan must be tested once every year or when a major change is made to ensure proper functionality.
5.6 System Security Plan for Each Major Application or General Support System	Document the in-place security controls of the system according to the CMS System Security Plan Methodology.	Document the in-place security controls of the system according to the CMS System Security Plan Methodology.	Document the in-place security controls of the system according to the CMS System Security Plan Methodology.

6. Network Security Standards

This section focuses upon preventive measures designed to reduce the risk of unauthorized access by external persons. The network security standards address perimeter security controls that maintain the capability to protect trusted networks from untrusted networks. Most organizations have perimeter security controls implemented, however a large majority of these controls are improperly designed or configured. The security standards detailed in this section are intended to provide a basis for implementing and adequately securing perimeter defenses.

This section also addresses the exposure of systems contained within the security perimeter to external sources. Specialized network technology may enable unauthorized persons to gain external access to internal systems, and effectively circumvent perimeter security defenses. This includes wireless network technology and modems. The security standards contained within this section provide guidance for the protection of such network technology. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Network Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
6.1 Firewall Hardware and Software	Utilize filtering hardware and software; although it is not required, it is recommended that stateful inspection hardware and software is utilized.	Utilize stateful inspection/application firewall hardware and software.	Utilize stateful inspection/application firewall hardware and software.

Network Security Standards	System Security Level		
	Low	**Moderate**	**High**
6.2 Packet Filtering on Firewalls and Routers	All traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.	All traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.	All traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.
6.3 Application Proxies	Access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.	Access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.	All proxies not explicitly required are disabled and removed. Proxy access is granted only to those hosts, ports, and services that are explicitly required.
6.4 Restrict the Use of Handheld Personal Computers	Restrict the connection of portable computing or portable network devices on the CMS network to CIO authorized devices.	Restrict the connection of portable computing or portable network devices on the CMS network to CIO authorized devices.	Restrict the connection of portable computing or portable network devices on the CMS network to CIO authorized devices.
6.5 Desktop Modems	Prohibit users from installing desktop modems.	Prohibit users from installing desktop modems.	Prohibit users from installing desktop modems.

Network Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
6.6 DMZ Architectures for Public Servers	DMZ architecture is implemented to separate internal network from public systems, and CMS servers from unnecessary public access.	All CMS servers allowing public access are placed within a DMZ environment, and direct access is not allowed to the internal network. DMZ servers cannot access the internal network. DMZ packet filtering and proxy rules provide protection for CMS servers.	All CMS servers allowing public access are placed within a DMZ environment, and direct access is not allowed to the internal network. DMZ servers cannot access the internal network. DMZ packet filtering and proxy rules provide protection for CMS servers.
6.7 Identify and Detect Unauthorized Modems	Examine a sample of network systems using an automated method on demand but no less than quarterly to determine if unnecessary network services (modems, etc.) are available.	Examine a sample of network systems on demand but no less than monthly using an automated method to determine if unnecessary network services are available. Perform a complete review on demand but no less than every six months.	Examine a sample of network systems on demand but no less than weekly using an automated method to determine if unnecessary network services are available. Perform a complete review on demand but no less than monthly.
6.8 Data Sent Via Wireless Media	No specific requirements.	Enable encryption protection (see Organizational Practice).	Enable encryption protection (see Organizational Practice.).

7. System Access Security Standards

The information security standards included in this section focus primarily upon methods to enable adequate operating system and platform security and contain security standards related to user account security and user account management. Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity, and availability. This section includes preventive measures intended to control system access and accordingly protect data confidentiality, integrity, and availability. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

System Access Security Standard	**System Security Level**		
	Low	**Moderate**	**High**
7.1 Authentication Protection for System Access	Use system and/or network password (see Organizational Practice).	Use system and/or network password (see Organizational Practice).	Use system and/or network password (see Organizational Practice). Additional authentication protection (token, biometric) not required but recommended.
7.2 Default User Accounts	Remove or disable default user accounts. Rename active default accounts.	Remove or disable default user accounts. Rename active default accounts.	Remove or disable default user accounts. Rename active default accounts.

System Access Security Standard	System Security Level		
	Low	Moderate	High
7.3 Operating System Access Controls	Configure operating system controls to disable public write access to files, objects, and directories that may directly impact system functionality or performance.	Configure operating system controls to disable public read and write access to files, objects, and directories that may directly impact system functionality or performance, or that contain sensitive information.	Configure operating systems controls to disable public read and write access to all system files, objects, and directories. Configure operating system controls to disable public read access to files, objects, and directories that contain sensitive information.
7.4 Privilege Restrictions	Enable privilege restrictions to limit public and employee access to administrative tools, scripts, and utilities.	Enable privilege restrictions to limit public and employee access to administrative tools, scripts, and utilities.	Enable privilege restrictions to limit non-administrative access to administrative tools, scripts, and utilities.
7.5 Unnecessary System Services	Disable all system services not explicitly required for system and application functionality.	Disable all system services not explicitly required for system and application functionality.	Disable all system services not explicitly required for system and application functionality.

System Access Security Standard	System Security Level		
	Low	**Moderate**	**High**
7.6 Administrative Rights	Maintain a limited group of administrators with full access. Limit distribution of certain administrative responsibilities and rights, such as the ability to reset user passwords or install software, to authorized groups and organizational units.	Maintain a limited group of administrators with full access. Limit distribution of certain administrative responsibilities and rights, such as the ability to reset user passwords or install software, to authorized groups and organizational units.	Maintain a limited group of administrators with full access. Limit distribution of certain administrative responsibilities and rights, such as the ability to reset user passwords or install software, to authorized groups and organizational units.
7.7 Administrators Accounts for Administrative and Non-administrative Activities	Use unique and separate administrator accounts for administrative and non-administrative activities.	Use unique and separate administrator accounts for administrative and non-administrative activities.	Use unique and separate administrator accounts for administrative and non-administrative activities.
7.8 Administrative Accounts Monitoring	Inspect administrative groups on demand but no less than every 30 days to ensure unauthorized administrative accounts have not been created. Verify that proper logging is enabled to audit administrative activities.	Inspect administrative groups on demand but no less than every 14 days to ensure unauthorized administrative accounts have not been created. Verify that proper logging is enabled to audit administrative activities.	Inspect administrative groups on demand but no less than every 7 days to ensure unauthorized administrative accounts have not been created. Verify that proper logging is enabled to audit administrative activities.

System Access Security Standard	System Security Level		
	Low	Moderate	High
7.9 File System Access	Disable all file system access not explicitly required for system, application, and administrative functionality.	Disable all file system access not explicitly required for system, application, and administrative functionality.	Disable all file system access not explicitly required for system, application, and administrative functionality.
7.10 Network Protocols	Disable all network protocols not explicitly required for system and application functionality.	Disable all network protocols not explicitly required for system and application functionality.	Disable all network protocols not explicitly required for system and application functionality.
7.11 Remote Access Connections	Implement password protection	Implement password protection.	Implement password protection in combination with certificate-based authentication or additional authentication protection, e.g. token-based, biometric.
7.12 Failed Logon Attempts	Configure systems to disable access for five minutes after five failed logon attempts.	Configure systems to disable access for ten minutes after three failed logon attempts. Lock out user account following three consecutive disable cycles, and require an administrative reset.	Configure systems to disable access for fifteen minutes after three failed logon attempts. Lock out user accounts following three consecutive disable cycles, and require an administrative reset.

System Access Security Standard	System Security Level		
	Low	**Moderate**	**High**
7.13 Virus Scanning	Enable real-time file scanning. Desktop virus scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and once a week.	Enable real-time file scanning. Desktop virus scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform full virus scans during system boot and every 24 hours.	Enable real-time file scanning. Desktop virus scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform full virus scans during system boot and every 12 hours.
7.14 System Boot Access	Boot access to removable media drives must be disabled if not explicitly required. System BIOS settings must be locked, and BIOS access must be protected by password (see Organizational Practice).	Boot access to removable media drives must be disabled if not explicitly required. Removable media drive functionality must be disabled if not explicitly required. System BIOS settings must be locked, and BIOS access must be protected by password (see Organizational Practice).	Boot access to removable media drives must be disabled if not explicitly required Removable media drives must be removed if not explicitly required. . System BIOS settings must be locked, and BIOS access must be protected by password (see Organizational Practice).
7.15 Inactive Mainframe Sessions	Mainframe sessions are forcibly disconnected after 15 minutes of inactivity.	Mainframe sessions are forcibly disconnected after 15 minutes of inactivity.	Mainframe sessions are forcibly disconnected after 15 minutes of inactivity.

System Access Security Standard	System Security Level		
	Low	Moderate	High
7.16 Desktop Locking Mechanism	Configure systems to disable desktop access automatically after 15 minutes of inactivity. Require a password (see Organizational Practice) to restore desktop access.	Configure systems to disable desktop access automatically after 15 minutes of inactivity. Require a password (see Organizational Practice) to restore desktop access.	Configure systems to disable desktop access automatically after 15 minutes of inactivity. Require a password (see Organizational Practice) to restore desktop access.
7.17 System Maintenance	Enforce consistent installation of vendor supplied service packs, hotfixes, security patches, and virus definitions. Ensure vendor-supplied security patches are obtained, analyzed for security and functionality in a test bed environment, and implemented on production equipment within one month.	Enforce timely and consistent installation of vendor supplied service packs, hotfixes, security patches, and virus definitions. Ensure vendor-supplied security patches are obtained, analyzed for security and functionality in a test bed environment, and implemented on production equipment within one week.	Enforce immediate (as required functionality allows) installation of vendor supplied service packs, hotfixes, security patches, and virus definitions. Ensure vendor-supplied security patches are obtained, analyzed for security and functionality in a test bed environment, and implemented on production equipment within 72 hours, or sufficient workaround procedures protect system assets.
7.18 Sensitive System Files	No specific requirements.	Encrypt sensitive system files.	Encrypt sensitive system files.

System Access Security Standard	System Security Level		
	Low	**Moderate**	**High**
7.19 Remote Access for Applications	Enable remote access through VPN links, using authorized VPN client software using encryption standard (see Organizational Practice).	Enable remote access through VPN links, using authorized VPN client software using encryption standard (see Organizational Practice).	Enable remote access through VPN links, using authorized VPN client software. Use encryption standard (see Organizational Practice) in combination with password authentication, certificate-based authentication or additional authentication protection, e.g. token-based, biometric.
7.20 Remote System Administration	Enable secure management protocols through a VPN link(s) if connected to network and use Remote Administration. Utilize encryption standard (see Organizational Practice).	Enable secure management protocols through a VPN link(s) if connected to network and use Remote Administration. Utilize encryption standard (see Organizational Practice).	Enable secure management protocols through a VPN link(s) if connected to network and use Remote Administration. Utilize encryption standard (see Organizational Practice), in combination with password authentication or additional authentication protection (e.g., token-based, biometric.)

System Access Security Standard	System Security Level		
	Low	Moderate	High
7.21 Callback Security for Remote Access Modems	Require callback capability with reauthentication to verify connections from authorized locations when MDCN cannot be used.	Require callback capability with reauthentication to verify connections from authorized locations when MDCN cannot be used.	Require callback capability with reauthentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log on, the vendor will be assigned a UserID and password and enter the network through the standard CMS authentication process. Access to such systems will be authorized and logged. UserIDs assigned to vendors will be renewed on a six-month basis.
7.22 User Access Administration	Implement centralized control of user access administrative functions.	Implement centralized control of user access administrative functions.	Implement centralized control of user access administrative functions.

8. Application Security Standards

The application security standards detailed in this section are focused on methods for enabling applications to operate securely. Applications deliver and process information, and are responsible in large part for maintaining the confidentiality, availability and integrity of critical data. The security standards presented in this section address the secure configuration of applications. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Application Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
8.1 Secondary Authentication and Encryption	No specific requirements but recommend enabling application security mechanisms, such as SSL and SSH and utilizing minimum encryption and password authentication (see Organizational Practice).	Enable application security mechanisms, such as SSL and SSH. Utilize minimum encryption and password authentication (see Organizational Practice).	Enable and force use of application security mechanisms, such as SSL and SSH. Utilize minimum encryption and password authentication (see Organizational Practice), in combination with certificate-based authentication or additional authentication protection, e.g. token-based, biometric.
8.2 Electronic Mail	No specific requirements but recommend encrypting outgoing e-mail messages and attachments.	Encrypt outgoing e-mail messages and attachments.	Encrypt outgoing e-mail messages and attachments. Digitally sign all outgoing e-mail messages, and verify digital signatures for received messages.

Application Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
8.3 Persistent Cookies	Requires approval by DHHS Secretary.	Requires approval by DHHS Secretary.	Requires approval by DHHS Secretary.

9. Data Security Standards

This section focuses on security standards for the protection of data at rest and in transit. It covers both electronic and hard copy forms of data. These standards will be used in conjunction with other standards described in this document, to augment data security and provide an acceptable level of confidentiality, integrity and availability of CMS data. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Data Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
9.1 Electronic Data at Rest	No specific requirements.	Data must be protected with system access controls.	Data must be protected with system access controls and must be encrypted.
9.2 Electronic Data in Transit	No specific requirements.	Encrypt data while in transit from source to destination. Data must be transmitted via secured communications.	Encrypt data while in transit from source to destination. Data must be transmitted via secured communications.
9.3 Labeling of Electronic Data Storage Media	Any magnetic media or compact disk must be labeled and retained according to business needs.	Any magnetic media or compact disk must be externally labeled (marked) with the appropriate security level classification. Off-line backup storage must be marked according to backup rotation schedule for ease of retrieval.	Any magnetic media or compact disk must be externally labeled (marked) with the appropriate security level classification. Off-line backup storage must be marked according to backup rotation schedule for ease of retrieval.

Data Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
9.4 Protection for Electronic Data Storage Media	No specific requirements.	Any magnetic media or compact disk must be kept in a secured area.	Any magnetic media or compact disk must be kept in a secured area.
9.5 Disposal of Electronic Data Storage Media	No specific requirements.	Any magnetic media, compact disk or hard drives must be sanitized before reuse or destroyed if it no longer can be sanitized for reuse.	Any magnetic media, compact disk or hard drives must be sanitized before reuse or destroyed if it no longer can be sanitized for reuse.
9.6 Disposal of Hard Copy Information	No specific requirements.	Fine shred documents when disposing of paper copies.	Fine shred documents when disposing of paper copies.
9.7 Labeling and Securing Hard Copy Information	No specific requirements needed for this classification beyond retaining a copy for the purpose the hard copy was created.	Hard copy must be marked with security level classification. Secure hard copies in a locked container. While in transit, store in a securable container such as a briefcase. Disseminate copies on a need-to-know basis and with management approval.	Hard copy must be marked with security level classification. Secure hard copies in a locked container. While in transit, store in a securable container such as a briefcase. Disseminate copies on a need-to-know basis and with management approval.

Data Security Standards	System Security Level		
	Low	Moderate	High
9.8 Validation of Data	Validate data prior to performing queries or updates on databases or any data repository. Use hypothetical data when executing test scripts. Employ parity checks, check-sums and error detection data validation techniques.	Validate data prior to performing queries or updates on databases or any data repository. Use hypothetical data when executing test scripts. Employ parity checks, check-sums and error detection data validation techniques.	Validate data prior to performing queries or updates on databases or any data repository. Use hypothetical data when executing test scripts. Employ parity checks, check-sums and error detection data validation techniques.
9.9 System Backups	Incremental backups are performed as needed. Backups stored on separate media.	Incremental backups are performed daily, and full backups are performed weekly. Three generations of backups must be stored off-site. Offsite and on-site backups must be logged with name, date, time and action.	Incremental backups are performed daily, and full backups are performed every other day. Three generations of backups are stored off-site. Offsite and on-site backups must be logged with name, date, time and action.

10. Vulnerability Assessment Security Standards

This section defines standards for intrusion detection implementation; network and system monitoring; collection and protection of security incident information, and forensic evidence; vulnerability assessment and security measures implementation; and security incident reporting.

Vulnerability assessment and analysis has been included in this section since it provides a proactive approach to minimize security gaps, which can lead to exposure and exploits that may be later detected with a real-time intrusion detection system. Vulnerability assessment and security posture evaluations will be performed by means of: a theoretical review of policies and procedures; by conducting penetration testing, given various levels of knowledge and access; and by analyzing and documenting a variety of test results. Standards for Incidence Response implementation are addressed in the Organizational Practices section. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Vulnerability Assessment Security Standard	**System Security Level**		
	Low	**Moderate**	**High**
10.1 Intrusion Detection System Devices and Software	Implement real-time Intrusion Detection System (IDS) devices to monitor network and system(s) and detect misuse and anomalies. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers. Generate notification to appropriate staff.	Implement real-time Intrusion Detection System (IDS) devices to monitor network and system(s) and detect misuse and anomalies. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers. Generate notification to appropriate staff.	Implement real-time Intrusion Detection System (IDS) devices to monitor network and system(s) and detect misuse and anomalies. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers. Generate notification to appropriate staff.

Vulnerability Assessment Security Standard	System Security Level		
	Low	**Moderate**	**High**
10.2 Network Traffic Monitoring for Anomalies	Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a 24-hour period. Generate alerts for technical staff review and assessment.	Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a 24-hour period. Generate alerts for technical staff review and assessment.	Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than twice within a 24-hour period. Generate alerts for technical staff review and assessment.
10.3 System Monitoring for Anomalies	Review system logs for initialization sequences, logons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a 24-hour period. Generate alert notification for technical staff review and assessment.	Review system logs for initialization sequences, logons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a 24-hour period. Generate alert notification for technical staff review and assessment.	Review system logs for initialization sequences, logons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a 24-hour period. Generate alert notification for technical staff review and assessment.

Vulnerability Assessment Security Standard	**System Security Level**		
	Low	**Moderate**	**High**
10.4 Inspection of Critical Files and Directories for Unexpected Changes	Review integrity of files and directories for unexpected and unauthorized changes at least once a day. Automate review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.	Review integrity of files and directories for unexpected and unauthorized changes at least twice a day. Automate review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.	Review integrity of files and directories for unexpected and unauthorized changes at least twice a day. Automate review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.
10.5 Security Incident Information	Document relevant information related to a security incident according to CMS Computer Security Incident Handling Procedures.	Document relevant information related to a security incident according to CMS Computer Security Incident Handling Procedures.	Document relevant information related to a security incident according to CMS Computer Security Incident Handling Procedures.

Vulnerability Assessment Security Standard	**System Security Level**		
	Low	**Moderate**	**High**
10.6 Forensic Evidence Protection	Document relevant information related to a security incident according to CMS Computer Security Incident Handling Procedures. Preserve evidence through technical means, including secured storage of evidence media and write protection of evidence media. Use sound forensics processes and utilities that support legal requirements means. Determine and follow chain of custody for forensic evidence.	Document relevant information related to a security incident according to CMS Computer Security Incident Handling Procedures. Preserve evidence through technical means, including secured storage of evidence media and write protection of evidence media. Use sound forensics processes and utilities that support legal requirements means. Determine and follow chain of custody for forensic evidence.	Document relevant information related to a security incident according to CMS Computer Security Incident Handling Procedures. Preserve evidence through technical means, including secured storage of evidence media and write protection of evidence media. Use sound forensics processes and utilities that support legal requirements means. Determine and follow chain of custody for forensic evidence.
10.7 Security Vulnerability Assessment and Analysis	Perform penetration testing and conduct enterprise security posture review as needed but no less than once a year. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.	Perform penetration testing as needed but no less than quarterly and conduct enterprise security posture review yearly. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.	Perform penetration testing as needed but no less than quarterly and conduct enterprise security posture review yearly. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Vulnerability Assessment Security Standard	**System Security Level**		
	Low	**Moderate**	**High**
10.8 System Protection upon Security Incident Occurrence or Vulnerability Discovery	Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk exposure to reduce vulnerability exploit exposure.	Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk exposure to reduce vulnerability exploit exposure.	Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk exposure to reduce vulnerability exploit exposure including isolation or system disconnect.

11. Auditing and Logging Security Standards

This section contains security standards related to auditing and logging methods. Proper implementation of audit and log mechanisms will enable CMS to inspect system and network activities, detect unauthorized access, trace and reconstruct intrusions, and process evidence related to unauthorized activities. The security standards included in this section address proper auditing and logging controls. **NOTE:** When a control for a system is subject to higher standards to meet specific Federal, legal, program, accounting or other requirements, the system must be developed to meet these higher standards. The CMS ARS shall not be construed to relieve or waive these other standards.

Auditing and Logging Security Standards	**System Security Level**		
	Low	**Moderate**	**High**
11.1 System Event Auditing	Log user account management activities, system shutdown, reboot, and system errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Log user account management activities, failed and successful logons, security policy modifications, use of administrative privileges, system shutdown, system reboot, and system errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Log user account management activities, failed and successful logons, security policy modifications, use of administrative privileges, system shutdown, system reboot, and system errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.

Auditing and Logging Security Standards	System Security Level		
	Low	Moderate	High
11.2 Application Auditing	Log user account management, application shutdown, application restart, and application errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Log user account management, use of access rights, security policy modifications, use of administrative privileges, application shutdown, application restart, and application errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Log user account management, use of access rights, security policy modifications, use of administrative privileges, application shutdown, application restart, and application errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.
11.3 Critical File Auditing	Log file creation and deletion. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Log file creation, deletion, and modification. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Log file access, creation, deletion, and modification. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.

Auditing and Logging Security Standards	System Security Level		
	Low	Moderate	High
11.4 Perimeter Protection Logging and Alerts	Enable logging on perimeter devices, including firewalls and routers. Log packet screening denials originating from untrusted networks, packet screening denials originating from trusted networks, user account management, modification of packet filters, application errors, system shutdown and reboot, and system errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Enable logging on perimeter devices, including firewalls and routers. Log packet screening denials originating from untrusted networks, packet screening denials originating from trusted networks, proxy use denials, user account management, modification of packet filters, modification of proxy services, application errors, system shutdown and reboot, and system errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.	Enable logging on perimeter devices, including firewalls and routers. Log packet screening denials originating from untrusted networks, packet screening denials originating from trusted networks, proxy use denials, user account management, modification of packet filters, modification of proxy services, application errors, system shutdown and reboot, and system errors. Retain logs for 90 days, and archive old logs. Retain log archives for 1 year.
11.5 Audit Log Reviews	Use automated utilities to review audit logs once every 14 days for unusual, unexpected, or suspicious behavior.	Use automated utilities to review audit logs every 7 days for unusual, unexpected, or suspicious behavior. Randomly perform manual reviews on demand but no less than once every 30 days.	Use automated utilities to review audit logs once daily for unusual, unexpected, or suspicious behavior. Randomly perform manual reviews on demand but no less than once every 30 days.

Auditing and Logging Security Standards	System Security Level		
	Low	Moderate	High
11.6 Log Information Disclosures	Record information disclosures. Log information type, date, time, receiving party, and releasing party. Retain logs for 90 days and archive old logs. Retain log archives for 1 year.	Record information disclosures. Log information type, date, time, receiving party, and releasing party. Retain logs for 90 days and archive old logs. Retain log archives for 1 year.	Record disclosures of personal information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Retain logs for 90 days and archive old logs. Retain log archives for 1 year.
11.7 Log Information Modifications and Updates	Record modifications to information. Retain logs for 90 days and archive old logs. Retain log archives for 1 year.	Record modifications to information. Retain logs for 90days and archive old logs. Retain log archives for 1 year.	Record modifications to personal information, including protected health and financial information. Retain logs for 90 days and archive old logs. Retain log archives for 1 year.