Managing Information Privacy & Security in Healthcare

Mayo Foundation

Information Security Policies and Standards With Guidelines and Cross References Revision 20, September 9, 2002

DEFINITIONS

Access control terms

Individual-based access control: Each user's information needs is individually evaluated and access is provided accordingly.

Role-based access control: Users with common jobs and/or access needs are grouped. For example, nurses, administrators, desk attendants, etc.

Context-based access control: Users who serve in a common context, such as a given discipline or legal entity are grouped. This method is most commonly implemented in conjunction with role-based access control. For example, a nurse [role] in Rochester [context] has access to X and a nurse in Scottsdale has access to Y.

Policy-related terms

Policy: a broad *statement of principle or intent* that presents Mayo's position. Policies are interpreted and supported by standards.

Standard: a *rule or regulation* that specifies conduct or a course of action. Standards are mandatory directives for implementing Mayo policy that ensure uniform compliance.

Guideline: *a recommended course of action or a response* to a given situation. Guidelines should be considered when determining how to implement standards.

Information classification terms

Mayo confidential information: information that is controlled on a need-to-know basis within the Mayo organization. This includes Protected Health Information and Individually Identifiable Health Information.

Mayo internal information: information that is kept within the Mayo organization but not subject to further controls.

Public information: information that is not subject to security controls and is shared freely within and outside Mayo.

Regulatory terms

Individually Identifiable Health Information: in general, a subset of health information, including demographic information, that is: 1) created by or received from a healthcare provider, health plan, employer, or healthcare clearinghouse; and 2) relates to the past, present, or future physical health, mental health or other condition that requires healthcare; or the past, present or future payment for the provision of healthcare, and

(a) identifies the individual, or

(b) could be used to deduce the identity of an individual

Protected Health Information (PHI): in general, all forms of Individually Identifiable Health Information that is or has been electronically transmitted or electronically maintained.

I. Information security

Mayo Foundation will protect its vital information from unauthorized access, modification, disclosure, or destruction. An information security program will exist to protect the interests of our patients and of Mayo Foundation.

II. Security administration

A group will exist to develop and maintain an information security program for Mayo Foundation entities. This group will monitor adherence to and enforce standards, promote awareness, and validate the program's effectiveness.

A. Standards: applicability and exceptions

1. The Mayo *Information Security Policies and Standards* apply to all Mayo Foundation entities.

2. Each Mayo practice site may add to, but not detract from, Foundation policies and standards. Any exceptions to Foundation policies and standards must be requested in writing and submitted to the Foundation Information Security Subcommittee.

A. Standards: Roles

1. The Foundation Information Security Office is responsible for implementing and monitoring a consistent information security program. The Foundation Information Security Subcommittee will monitor this responsibility. The Foundation Information Security Office will:

    - Serve as the single point of contact for matters of information security, both internally and externally
    - Coordinate the development and maintenance of information security policies, standards, and guidelines to include technology-specific implementation standards
    - Coordinate information security activities with Physical Security, Internal Audit Services, Information Services, the Legal Department, Treasury Services, and outside law enforcement.
    - Manage security risk by analyzing assets, threats, vulnerabilities and exposures, and recommending cost-effective countermeasures to reduce likelihood or impact of adverse occurrences
    - Monitor security activities and oversee the application of specified security standards
    - Enforce standards compliance
    - Assist information stewards in assessing their data classification and advise them of available controls to manage risk
    - Manage an information security education and awareness program in coordination with the training and education function.
    - Provide consulting services for information security throughout the Foundation

2. The information steward, or owner, is responsible for a particular set of information and for implementing information security policy and standards. The information steward will:

    - Assume responsibility for information
    - Recommend appropriate business use of information
    - Authorize information access and assign administrative responsibility
    - Communicate control and protection requirements to system administrators and

users

- Monitor compliance and periodically review requirements for information protection in coordination with the Foundation Information Security Office

- Review security violation reports and follow reporting procedures (If we assume that the information stewards are likely to not be technically oriented to clearly make this task a joint responsibility with the system administrators?) [editor's query: sense of preceding statement? Leave it as a question?]

3. The system administrator is responsible for operation and maintenance of information processing services. The administrator implements information security policy and standards, and will:

    - Administer business and information protection controls specified by the information steward

    - Administer access control

    - Provide backup and recovery of information

    - Detect and respond to violations and weaknesses

    - Monitor compliance with information security standards

4. The Foundation Information Security Subcommittee is comprised of members from the Mayo group practices and acts as a council for information security for all Foundation entities.

5. Internal Audit proactively reviews systems and services for compliance with information security standards, other internal standards and the requirements of external regulatory bodies.

C. Standard: information assessment

Information stewards will assess risks and threats to information under their purview and accordingly classify their information as *public*, *internal*, or *confidential.* Recommendations for handling information are outlined in the table below:

Information Classification

	Public	Internal	Confidential
Label	None	None	Mark "Confidential"
Access	No controls	No controls	Discretionary
Storage	No controls	Store out of sight of non-Mayo persons	Lock up
Communication	No controls	No controls	Confidential envelope; Secure transmission
Destruction	No controls	No controls	Shred paper Overwrite media

D. Standard: training and awareness

Each site will assign responsibility for information security awareness and training.

Guidelines:

1. The Department of Human Resources will describe data security to all new employees.

2. Awareness programs will provide instruction on good security practices.

3. Mayo will support specific technical and management training for system administrators and users as needed.

E. Standard: violations

Any deviation from the information security policies and standards is a violation. Everyone must report instances of noncompliance. Violations will be reviewed for appropriate disciplinary action in accordance with Human Resources policy and procedures. Corrective action may include termination of employment or criminal prosecution.

Guidelines:

1. The Information Security Office, the Department of Human Resources and an appropriate level of department management will review standards violations and recommend corrective or disciplinary action.

2. Users should report security violations to a supervisor, system administrator, steward, information security, physical security or Internal Audit Services, as appropriate.

F. Standards: computer crime

1. Computer crimes violate state and federal law. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; denial of computer services; theft of computer services; illegal copying of software; invasion of privacy; forging, altering or using another user's unique identifier; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both.

2. Mayo Foundation must comply with license agreements for copyrighted software and documentation.

3. Licensed software must not be reverse engineered or copied unless the license agreement specifically provides for it.

4. Copyrighted software must not be loaded or used on systems for which it is not licensed. This includes employee-owned home computers and other personal digital devices used for Mayo business.

G. Standard: exceptions to standards

All exceptions to these standards are to be requested in writing and approved by the Information Security Subcommittee.

H. Standards: Mayo systems administered by contractors

1. Contracts for system and/or application management must include security, confidentiality, and non-disclosure clauses. These clauses must specify adherence to the *Information Security Policies and Standards* and contain penalties or a mitigation process for noncompliance. Mayo's Information Security Office or designee will assess the contractor's security posture. This assessment may include a site visit.

2. Oversight of contractor operations is the responsibility of Mayo staff. On-site information

stewards and system administrators must be identified to oversee administrative duties performed by non-Mayo personnel and compliance with security policies and standards. The Mayo system administrator must have a working knowledge of the system or application and possess a level of administrative privilege equal or higher than the contractor's. Mayo must carefully consider several administrative aspects and ensure that checks and balances are in place to control and monitor contractor activities:

A. Secure authentication of contractors is required. This may include multiple levels of authentication such as at a remote access server or firewall *and* at host levels. Authentication may involve secure tokens, username/password combinations, and public/private key combinations. Device-to-device or firewall-to-firewall authentication is acceptable provided contractor demonstrates individual accountability for access to Mayo systems and applications. This may be verified on-site at the contractor's place of business.

B. Authorization of contractors is required. Mayo must limit contractor access to systems, services and information on a discretionary basis. Contractor user accounts must not allow more system or network privileges than necessary to meet contract requirements.

C. Logging and auditing system accesses and activity is required. Mayo administrators and contractors are jointly responsible for auditing system access and activity and will routinely examine the logs for adherence to standards and authorized activities. Contractors cannot have the ability to delete or alter system log files. System audit logs should be retained for at least 6 months.

3. Operating systems employed must provide a reasonable level of integrity. Use of newer operating system versions or the application of patches to fix known bugs and vulnerabilities is highly recommended. Information Security provides a vulnerability scanning service, which can identify operating system security weaknesses and other areas of concern.

4. System or application access by contractor personnel must be closely controlled. The access method must not provide functionality beyond that which is required for contract performance.

5. Secure communications with contractors who provide service from remote locations is necessary to preclude technical compromise of information and systems. Mayo technical staff will work with contractors to employ standard, secure methods whenever possible.

III. Standards for information use

Mayo will establish standards for ethical use of information to protect the interests of patients and to prevent misuse of vital information.

A. Standard: misuse of resources

Any action or misuse of information that harms the resources of the institution or adversely affects other individuals is prohibited.

B. Standard: appropriate use of resources

Use of the Mayo network, computers, Internet link, dial-in services, and information resources is primarily for Mayo business-related activity or professional development. Limited personal use is acceptable but discretion is necessary to ensure that individuals do not degrade Mayo's public image through their activities, adversely affect the availability of network resources, or demonstrate a lack of respect for the rights of others.

C. Standard: authorized usage

Users must not attempt to gain physical or logical access to information or systems for which they are not authorized.

D. Standard: medical information

Users must keep all medical information confidential. [Reference local policy that addresses access to medical information.]

IV. Information access control

Mayo will control physical and electronic access to its sensitive information and computing resources. The level of control will depend on user need and the level of risk and exposure to loss or compromise. Electronic access will be controlled through identification and authentication. Users are responsible and accountable for access under their personal identifiers.

A. Standards: physical access to computing facilities and equipment

1. The level of physical access control for any area containing *Mayo confidential* information is determined by the level of risk and exposure.

Guidelines:

1. Access control lists should be maintained to include ongoing review and update.

2. An administrative determination of trustworthiness should be made before allowing individual access to sensitive areas. This normally includes reference and records checks.

3. Maintenance personnel should be escorted and supervised by knowledgeable persons.

4. System administrators should provide initial and ongoing security awareness training for

those assigned to sensitive areas.

5. The Information Security Subcommittee or its delegate will review and approve the placement of, and physical access to, Mayo devices located in any authorized off-campus sites.

2. Highly sensitive areas, such as data centers, server areas and communications facilities will have separate control systems to limit access. [Reference local policies regarding lock location and installation.]

Persons granted access to areas or information are responsible for their actions. Additionally, they are responsible for the actions of others that are, in turn, allowed access

3. Physical security precautions for workstations, software, documentation and diskettes will be determined by the risk of loss or damage. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

Guideline: The senior manager of the area will specify the physical access controls based on information security and lock placement standards.

4. Workstations that access *Mayo confidential* information will be located and positioned to minimize the likelihood of unauthorized visual access.

5. System administrators will physically locate printers to minimize the risk of unauthorized access to printed materials or implement procedures to accomplish the same.

- System administrators will investigate and resolve instances of misdirected printouts.

Guideline: Users will notify system administrators when printing anomalies occur that may adversely impact security of information output.

B. Standard: media and hardcopy protection and transportation

Electronic media and hardcopy containing *Mayo confidential* information must have access controls during transportation and disposal.

Guidelines

1. Printed versions (hard copy) of *Mayo confidential* information should not be copied indiscriminately or left unattended and open to compromise.

2. Media containing *Mayo confidential* information should be placed in confidential envelopes and hand-carried by Mayo employees, transported by General Service couriers or sent through an approved outside carrier. These outside carriers may include, but are not limited to, the U.S. Postal Service, Federal Express, and United Parcel Service.

3. Magnetic media containing *Mayo internal* or *Mayo confidential* information that is released from

Mayo should first be processed to purge any information residing on that media.

5. Degaussing and overwriting are acceptable methods of purging information from magnetic media.

6. Responsible personnel should authorize the shipping and receiving of magnetic media and maintain appropriate records.

7. *Mayo confidential* information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

C. Standards: information access controls

1. Access to the Mayo network, the Internet and systems and applications that process, store or transmit *Mayo confidential* information will be controlled. Each user will be uniquely identified, and an accepted process will authenticate identity. Processes for verification may include unique tokens, card keys, biometric readers, or individual passwords. Passwords and tokens are the individual's responsibility and will not be shared.

Guidelines

1. All network access should be controlled through individual identification and authentication.

2. Each user should have a unique identification code.

3. Each user's identity should be authenticated through an acceptable verification process.

Acceptable processes include individual passwords, unique tokens such as cards with magnetic stripes, or biometrics.

- Where password authentication is employed, the following technical standards apply: Enact a six-attempt account lockout where technically feasible. Authorized personnel will reset locked accounts manually. Passwords must consist of at least six characters. Passwords must change at least every 180 days.

  A six-password history is required to disallow re-use where technically feasible. Enforcement of password complexity is required where technically feasible. For example, single repeated characters and passwords identical to user identifiers are unacceptable. Shared guest accounts are not allowed.

Guidelines

1. Passwords are the individual's responsibility and users should not share them.

2. Users should be able to select and change their own passwords.

3. Passwords should not include names or words that are easily guessed or found in a dictionary.

Use of numeric digits and non-alphanumeric characters in passwords is encouraged for protection of

Mayo confidential information.

4. Users should not write down passwords, store them on hard copy, or store them locally on workstations and laptop computers.

3. Access to *Mayo confidential* information is controlled in accordance with the need-to-know principle.

System administrators must implement discretionary access controls that permit each user access to all systems, services and information necessary to accomplish assigned tasks, and conversely, preclude unnecessary access.

4. System administrators must periodically review user accounts and inactivate them when access is no longer required.

Guideline: Stewards and system administrators should determine the necessity of changing locks and recovering card keys, tokens and other access control devices when users terminate employment or when work assignments change.

5. Each legal entity [a least common denominator where multiple legal entities may comprise a single Covered Entity under HIPAA] that employs shared electronic systems to store confidential information, to include Protected Health Information (PHI), in common repositories must control access to the information on a per-entity basis. Either separate databases or context-based access controls are required. The access control model must accommodate access by both the legal entity and Foundation personnel based on the need-to-know principle.

Guideline: For shared systems, the electronic storage of each legal entity's confidential information may reside on physically separate storage media, separate databases on shared media, separate tables within a database, in the same data repository, etc. In any case the data either must be physically separated or have a data identifier that allows controlled access at a per legal entity level.

D. Standard: authorization controls

System administrators must limit user privileges in accordance with the least privilege principle. Users may view, modify, create and delete information only to the extent required to accomplish assigned tasks.

E. Standard: audit controls

System Administrators must be able to audit access and access attempts to *Mayo confidential* information. Audits will be conducted when unauthorized accesses and attempts are identified. Audit records shall be kept at least six months, and administrators shall periodically review the audit records for evidence of violations or system misuse.

F. Standards: inactive sessions

3. System administrators must implement inactivity time-outs, where technically feasible, for terminals and workstations that access *Mayo confidential* information.

4. System administrators must implement automatic logoffs for systems and applications that process, store, or transmit *Mayo confidential* information.

Guideline: Implementation procedures are developed at the local and business unit levels. Stewards should specify time-out and automatic logoff intervals based on business needs and risk levels.

G. Standard: portable devices

1. Each group practice will determine the efficacy of storing *Mayo confidential* information on portable devices and, where permitted, will specify risk-appropriate security procedures and technical controls.

[Cross reference local guidance on personal digital assistants]

Guidelines:
1. Personal digital assistants containing *Mayo confidential* information should employ user authentication and data encryption.

2. Laptop/notebook computers containing *Mayo confidential* information should employ user authentication and data encryption when they are subject to heightened risk of loss or theft. Devices carried on travel, used offsite, employed by contractors and located in areas frequented by the public are at higher risk.

H. Standards: generic access to data

1. Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. A user does not directly initiate the task, nor is a user the direct recipient of the information.

2. Requests for generic access to information stored in databases are made to the database administrators. If the request meets standards, the database administrator will establish an account. If the request is not within the scope of the standards, the requestor may ask the Information Security Subcommittee for a variance. The subcommittee will render a decision and notify both the requestor and the database administrator.

3. Generic accounts and passwords are, in general, subject to standards and guidelines that pertain to individual user accounts. One exception is password expiration. Generic account passwords will expire every 180 days and application administrators will be notified of the expiration and will be prompted to change it. Application administrators will have seven calendar days to comply prior to revocation of access. There will be no exceptions to the expiration requirement.

4. Generic account passwords must be protected from unauthorized disclosure. Hard coded passwords that reside on the client machine or in an application must be afforded reasonable protection commensurate with risk and available platform or application security features.

5. Information access via generic accounts must be limited to the maximum practical extent and functionality must be limited to the specific task required.

V. Communication security

Mayo will protect sensitive information transmitted outside the organization. Methods employed will depend upon information sensitivity, technical risks, external regulations and available communication security controls.

A. Standard: internal transmission

Technical security features for systems and services vary. Stewards, system administrators and developers must consider these variances when they transmit *Mayo confidential* information internally from one system or service to another.

B. Standards: release of information that individually identifies Mayo patients

1. Individually Identifiable Health Information or information that identifies individual Mayo patients will not be released to any outside organization or individual except for patient care, legal, or reimbursement purposes. [cross-reference *Representing Mayo*]

Guideline: Individual identifiers include: names, addresses, birth dates, clinic numbers, Social Security numbers, telephone and fax numbers, electronic mail addresses, health plan beneficiary numbers, account numbers, certificate and license numbers, vehicle identifiers and serial numbers to include license plate numbers, device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers, biometric identifiers, full-face and comparable images, and any other unique identifying number, characteristic or code. The fact that information released does not specifically identify individuals *as* Mayo patients is immaterial.

2. Release of information for patient care will occur only in accordance with each site's medical information access policy and the Mayo *Information Security Policies and Standards.*

Guideline: *Release* is the physical movement or electronic transmission of information outside the physical boundaries of Mayo Foundation or the institutional network and supporting infrastructure that connects Foundation entities.

3. Exceptions to information release standards must be consistent with state and federal laws and regulations and approved by the Mayo Foundation Information Security Subcommittee, Foundation Information Management and Technology Committee and the Foundation Executive Committee.

Guideline: Project proposals and draft contracts for service must accurately identify the sources and flow of information, how it is stored and used, and detail security controls. Only endorsed standards exceptions are forwarded for consideration.

C. Standards: external transmission and remote access

1. The steward and appropriate policy setting groups make the business decisions regarding appropriateness of external transmission and remote access to Mayo network resources. Each group practice will provide guidance to system administrators concerning the provision of these services. Risk and countermeasure information is available from the Information Security Office. [cross-references: Standard for *Mayo systems administered by contractors* and Rochester CPC minute prohibiting remote access to patient-specific information, July 23, 2001]

2. Stewards must understand the risks of transmitting *Mayo confidential* information outside the institution, and will employ technical security services, such as encryption, where warranted by risk.

3. The Information Security Subcommittee or its delegate will review and approve technical security controls for external transmission and remote access.

   Guideline: Dial-up access should occur through an institutionally supported technical security service such as Remote Authentication Dial-In User Service (RADIUS).

4. If a secure, institutionally supported service is not used, a Mayo employee must either employ a security procedure, such as enabling and disabling the modem and supervising its use, or

implement a technical security controls such as authentication and dial-back.

5. Supervisors and administrators may authorize remote access accounts where beneficial to Mayo.

D. Standard: wireless devices

1. Encryption of wireless network data transmission and authentication of wireless devices to the network is required. Each group practice will provide guidance to system administrators concerning the provision of these services.

E. Standards: electronic mail [cross-references: 1. Mayo Foundation e-mail policy; 2. Local guidance regarding e-mail usage, clinical usage and communicating patient-specific information; 3. Foundation Information Technology policies; 4. Human Resources policy. These standards pertain to both internal messages and Internet e-mail.]

1. Mayo Foundation owns the electronic mail service, and considers electronic mail private, direct communication between sender and recipient. However, employees cannot expect absolute confidentiality. The contents will not be monitored, observed, viewed, displayed or reproduced in any form by anyone other than the sender or recipient unless specifically authorized by an officer of Mayo Foundation, a law enforcement representative or the Information Security Office.

Guideline: The local Information Security Office may authorize second party access to electronic mailboxes.

2. Electronic mail is considered official correspondence of Mayo Foundation, and users must avoid the inclusion of inappropriate or derogatory language in their messages. Electronic mail is maintained in computer systems and on backup media for varying lengths of time and may be recovered subsequent to deletion. The messages may be disclosed in the same manner as paper records. Reasons for recovery of electronic mail messages may include legal discovery, external investigations and internal security investigations.

3. Work-related mail is forwarded to the most appropriate employee in the case of employment termination or when an employee is absent for an extended period of time. A recipient may designate another employee to receive and read work-related mail for business reasons. Personal messages are forwarded to the intended recipient. If that is not possible, they are destroyed. Messages are not examined further than is necessary to determine the category into which they fall.

Guideline: The local Information Security Office may authorize supervisor access to staff electronic mailboxes for business reasons when individuals are unexpectedly absent and/or unreachable.

F. Standards: e-mail host security

1. Hosts that run e-mail routing applications must support and employ security functions such as authentication and logging at the system and e-mail application administrative levels.

Guideline: Most single user PC-based operating systems, such as Windows 95, do not provide acceptable security functionality. E-mail hosts must run on operating systems capable of identification, authentication and other security functions such as logging and discretionary access controls.

Examples of such operating systems are Windows NT, Unix, and VMS. Administrators must employ these security features to prevent and detect unauthorized access to system and application administrative accounts.

- Administrators must actively manage e-mail hosts to minimize security risk.

Guidelines: Operating system security vulnerabilities exist and are well documented. Tools exist to assist administrators evaluate risk and correct vulnerabilities. Information sources, such as the National Security Agency's Computer Emergency Response Team (CERT), publish threat information and prescribe technical courses of action to neutralize those threats. The persons, groups or departments that own and operate systems are ultimately responsible for security. System administrators will actively monitor authoritative security sources, perform risk assessments and employ available countermeasures as risks and threats are identified. Specific security guidance includes:

Hosts should preferably run the most current version of e-mail routing applications. Minimally, the routing software used must incorporate applicable security patches.

E-mail gateways/mailers must not automatically execute attachments or message bodies, such as those found in Multipurpose Internet Mail Extensions (MIME), ActiveX, SML, or Java.

Administrators of E-mail routers that perform some non-MIME auto-execute functions such as "vacation," must configure their systems to automatically invoke programs deemed secure and/or required for the business function of the system.

- E-mail hosts and e-mail users must be Internet "good neighbors."

Guidelines: Administrators who configure e-mail hosts as relay hosts must take measures to detect and prevent delivery of unsolicited broadcast E-mail, or "spam," bywatching for messages coming to their machines from non-Mayo sites that are destined for other non-Mayo sites. Spammers sometimes attempt to hide their tracks by bouncing e-mail off intermediate sites to obscure the source.

Senders of e-mail may not hide or disguise the origin of their messages for illicit or illegal purposes. Forging or altering e-mail messages to impersonate other individuals or entities is forbidden. Violators are subject to corrective action.

- No employee may automatically forward mail outside of Mayo.

Guidelines: For security reasons, it is inappropriate for users to indiscriminately route all incoming email from a Mayo-designated email account to an account outside the Mayo intranet, without specific permission from the Information Security Subcommittee. Only under exceptional circumstances will such permission be granted. Terminated employees, with supervisory approval, may have all inbound Internet email routed from their Mayo-designated email in-box to an external Internet email account for up to six (6) months as a courtesy.

G. Standards: Internet

1. Use of the Internet via the Mayo network must be primarily for Mayo business or professional development. Limited personal use is acceptable but discretion is necessary to ensure that individuals do not degrade Mayo's public image through their activities or adversely affect the availability of network resources. Use of the Internet via the Mayo network for personal business is not permitted. [cross references: 1. local Human Resources policy on computer and Internet use; 2. FIIPC policy on web usage and content filtering]

   Guideline: Internet access should be limited to those with business need.

2. All access and communication to or from the Internet must occur through an actively managed Internet firewall service

3. Internet services available via Mayo's internal network will be limited to those required for business or professional development.

4. Access via Internet to Mayo'sinternal network must be approved by the Information Security Officer or designate. External entities must have contractual agreements with Mayo that address information security, nondisclosure and indemnification. Access methods must employ strong authentication and encryption. Access must be limited to the minimum systems and services required, and activity must be logged.

5. Internet access by non-Mayo persons (i.e. patients and guests) via Mayo network services is not allowed. A non-networked system with dialup service to commercial Internet service providers is the preferred method of providing Internet access to non-Mayo persons.

VI. Information integrity controls

Vital information must remain consistent, complete, and accurate. Serious errors and unauthorized or inappropriate duplications, omissions and intentional alterations will be investigated.

A. Standard: separation of duties and functions

Where feasible, responsibilities of application programmer, system programmer, system administrator, and database administrator must not overlap.

B. Standard: application software

Only tested and controlled software should be installed on networked systems. Use of unevaluated and untested software outside an application development environment is prohibited.

C. Standard: change controls

Change control management must exist for software development where deemed appropriate.

Guideline: Revision procedures should be designed to minimize the likelihood of information loss or corruption.

D. Standards: anti-virus controls

1. All systems connected to the network will have virus protection.
   Guideline: Controls may include real-time or periodic scans.
2. System Administrators are responsible for oversight and implementation of these procedures. A consistent approach will be employed across the Foundation.
3. Foundation Information Services will maintain and update a list of approved software for virus protection.
4. Where technically feasible, users will employ approved anti-virus software.
5. A Foundation-wide educational and technical approach will exist to raise user awareness of virus hazards in the computing environment and to detect and purge viruses.
6. Where necessary, Mayo will provide and help maintain anti-virus software on networked personal systems. To the extent practical, users are responsible for the integrity of their personally owned devices used for remote access and will employ adequate anti-virus software that is updated regularly via central security control, as practical, or via manual download.

Guideline: Mayo should provide anti-virus software protection, where necessary, for personally owned systems used for remote access.

VII. Preventive measures, backup, and recovery

Mayo will prevent loss of vital information, provide backup and recovery, and provide continuous operation consistent with business needs.

A. Standards: prevention

1. Frequent testing of preventive methods as they apply to fire, utility services, and other environmental hazards must occur.

Guideline: Combustibles should not be stored in data centers, network hub rooms, network points of presence, or other areas critical to the computing base.

2. Users must not connect unauthorized devices to the Mayo network. Network Services or its designee will evaluate requests to attach devices to the network.

B. Standard: backup

All information must have sufficient backup and be recoverable.

Guidelines:

1. Multiple levels of backup and storage should be used for critical information.

2. Backup should provide for the loss of multiple cycles.

3. Users of personal computers and other personal digital devices are responsible for backup and recovery of locally stored information.

4. Files and programs should be properly labeled and indexed to facilitate recovery.

5. Alternate fire zone storage facilities should be used for media containing vital data that, if lost or destroyed, would be difficult to recreate.

6. Alternate fire zone storage facilities should be used for files containing patient care programs, program changes, or data that could be used to reconstruct essential systems in the event of a disaster.

7. Backup and recovery procedures should be tested.

c. Standard: emergency mode of operation

Alternate modes of operation, that may include manual methods, must exist to ensure continuity of critical services in the event a natural disaster, fire, or act of vandalism or terrorism occur.

D. Standards: disaster recovery planning

1. All Mayo data centers and computerized systems critical to Mayo Foundation must have written operationally-tested disaster recovery plans.

2. Information stewards will prioritize the recovery of applications and associated databases to ensure critical services are recoverable in a timely fashion.

Guidelines:

1. Information processing management will maintain teams to execute recovery procedures for data centers, systems, networks and databases.

2. The disaster plan should include procedures to facilitate an immediate, planned response to emergency situations.

3. All areas of data processing are required to maintain recovery documentation consisting of a system recovery overview, systems chart and job-level recovery documentation.

4. Recovery procedures should address computers, peripheral equipment, environmental systems, supplies, and anything else essential to the data processing operation.

5. Stewards, system administrators and users should all be involved in disaster recovery planning.

6. Specific personnel should be assigned recovery tasks. Each person should have an alternate. Recovery plans must allow alternate personnel to access the necessary instructions and procedures to accomplish recovery tasks.

7. Testing of recovery plans should be an ongoing activity. All activity during a test must be recorded and reviewed for the purpose of improving the plans. Tests should include alternate site processing where applicable.