

UNIVERSITY OF MISSISSIPPI MEDICAL CENTER

Information Policy

Table of Contents

1.0 PURPOSE	3
2.0 SCOPE	3
3.0 RESPONSIBILITIES.....	3
3.1 Information Systems Strategic Planning Committee (ISSPC)	3
3.2 Chief Information Officer (CIO).....	4
3.3 Office of Information Security (OIS).....	4
3.4 Information Systems Internal Auditor.....	4
3.5 Information Owner (Owner).....	5
3.6 Security Administrator	5
3.7 Individual	6
4.0 STANDARDS	6
4.1 Access Security and Controls	6
4.1.1 System Access Set-up	6
4.1.2 Passwords	7
4.1.3 Physical Security	8
4.1.4 Log-In/Log-Off.....	8
4.1.5 Remote Access	8
4.1.6 Revoking System Access	8
4.1.7 Termination	8
4.1.8 Departmental Transfer.....	9
4.1.9 System Changes.....	9
4.1.10 Viruses.....	9
4.1.11 Encryption	10
4.1.12 Expectation of Privacy	10
4.1.13 Electronic Mail	10
4.1.13.1 Disclaimer	10
4.1.14 Electronic Protected Health Information (EPHI).....	10
4.1.15 Institutional Publications	121
4.2 Appropriate Use.....	11
4.2.1 Personal Use	11
4.2.2 Nondisclosure.....	11
4.2.3 Intellectual Property	11
4.2.4 Software Agreements.....	12

4.3 Web Environment	12
4.4 Contingency Planning	12
4.4.1 System Backup and Recovery	13
4.4.2 Data Backup	13
4.5 Disposal of Information	13
5.0 POLICY INVESTIGATIONS	14
6.0 SANCTIONS	14
7.0 POLICY EXCEPTIONS	14
8.0 DEFINITIONS	14
9.0 CONTACT INFORMATION	16
SUPPLEMENTAL INFORMATION	16
Examples of Inappropriate Use	16
Electronic Information Transfer Guidelines	18

1.0 PURPOSE

The purpose of the University of Mississippi Medical Center (UMC) Information Policy is to establish management direction and requirements to ensure the accomplishment of the UMC mission through the appropriate protection of all UMC information from accidental or intentional misuse or unauthorized access, modification, destruction or disclosure.

2.0 SCOPE

The UMC Information Policy applies to all UMC-related information in all forms, whether observed, written, spoken, electronic or printed. It also applies to UMC electronic resources, including hardware, software and networks. All electronic equipment that is connected in any manner, directly or indirectly, intermittently or continuously, to the campus network or any computer subnet is subject to the UMC Information Policy.

The UMC Information Policy applies to all individuals accessing UMC information on or off campus, including but not limited to employees, contractors, consultants, volunteers, temporaries, students, faculty, third-party affiliates, business associates, affiliated campus organizations, authorized visitors and nonprofit groups.

Departmental or other institutional policies may further define certain aspects of information access and use, but may not be less restrictive than the UMC Information Policy.

3.0 RESPONSIBILITIES

All individuals and organizations that come in contact with UMC information are responsible for its appropriate management and protection. Levels of accountability facilitate compliance with the UMC Information Policy. To achieve a more secure environment, appropriate segregation of responsibilities must be established.

3.1 Information Systems Strategic Planning Committee (ISSPC)

Responsibilities of the ISSPC include, but are not limited to:

- reviewing current resource allocation;

- receiving requests from the various units for new technology needs;
- submitting a five-year information technology strategic plan;
- reviewing issues related to the UMC Web environment; and
- submitting recommendations to the vice chancellor for approval.

3.2 Chief Information Officer (CIO)

Responsibilities of the CIO include, but are not limited to:

- directing informational integrity and security initiatives;
- defining and managing the strategic direction of all electronic information resources;
- managing the information technology affairs of the institution;
- designating owners in cooperation with senior management;
- interacting with internal and external clients to ensure continuous customer satisfaction; and
- enhancing technology use through education and training.

3.3 Office of Information Security (OIS)

Responsibilities of the Office of Information Security include, but are not limited to:

- monitoring, evaluating, maintaining and recommending security systems and procedures to protect electronic information resources from accidental or intentional misuse, or unauthorized access, modification, destruction or disclosure;
- identifying security threats, responding to suspected or reported security violations and recommending corrective actions; and
- providing education and ongoing orientation and support on system security and confidentiality.

3.4 Information Systems Internal Auditor

Responsibilities of the information systems internal auditor include, but are not limited to:

- verifying compliance with federal, state and local laws, regulations and rules, accreditation criteria and all institutional policies;
- identifying and resolving security breaches in conjunction with OIS;
- serving as the UMC HIPAA security officer to manage UMC's HIPAA security program; and

- assisting management or other individuals in evaluating information systems and security procedures, and recommending corrective action.

3.5 Information Owner (Owner)

Responsibilities of owners include, but are not limited to:

- organizing, authorizing, acquiring, creating and maintaining accurate and current information and information systems within their assigned areas of control;
- identifying and reporting major risks to their information;
- maintaining controls that ensure information confidentiality and integrity;
- identifying their sensitive, confidential and critical information;
- selecting and adhering to data retention requirements for their information in accordance with advice from the UMC legal counsel;
- specifying supplementary control measures to protect their information, including system backup and recovery;
- evaluating the cost-effectiveness of controls;
- approving and reviewing access privileges to their information based on the need-to-know;
- designating a backup owner to act if they are unavailable;
- refraining from delegating their responsibilities to third-party individuals or organizations; and
- serving as the Web Site Owner.

3.6 Security Administrator

Responsibilities of a security administrator include, but are not limited to:

- recommending and/or implementing physical and procedural safeguards to comply with UMC policies;
- administering access to information;
- reporting security vulnerabilities and violations to OIS or the Office of Compliance;
- monitoring access control logs and performing similar security actions;
- initiating appropriate actions when problems are identified;
- following supplemental instructions of owner(s) for information handling and control; and

- providing owner(s) with periodic reports showing access levels of all individuals accessing the system.

3.7 Individual

Responsibilities of individuals include, but are not limited to:

- protecting all sensitive or confidential information at all times;
- complying with controls specified by UMC, the owner and the security administrator;
- securing access to UMC systems when logged on, whether unattended or not;
- reporting information errors, anomalies and security vulnerabilities and violations to their supervisor, the security administrator, OIS or the Office of Compliance;
- completing required training;
- complying with the UMC Information Policy, Rules and Procedures for the UMC Web Environment and the Compliance Plan, as well as federal, state and local rules, laws and regulations, accreditation criteria and all other institutional policies; and
- signing the Information Policy Agreement Form.

4.0 STANDARDS

UMC authorizes and reserves the right to restrict or limit the use of and access to any information. These standards are required for compliance with federal, state and local laws, regulations and rules, accreditation criteria and the UMC Statement of Purpose.

4.1 Access Security and Controls

Access to information resources is granted on a need-to-know basis and must have controls to protect UMC information from accidental or intentional misuse, or unauthorized access, modification, destruction or disclosure.

4.1.1 System Access Set-up

All electronic information systems must:

- employ individual assigned accounts and passwords;
- provide a password-protected screen saver invoked either manually or automatically after a period of inactivity;
- mask or suppress password entry;

- immediately require all vendor-supplied default passwords to be changed;
- require immediate change of initial or reset passwords;
- limit consecutive unsuccessful logon attempts to three before suspending for reset or temporarily disabling for no less than three minutes - for external network connections, the session must be disconnected;
- incorporate automatic controls to suspend application sessions delivering sensitive or confidential information that have been inactive for 15 minutes or less;
- require all relevant passwords to be changed whenever system security is believed to be compromised;
- require administrative passwords to be changed at least every 90 calendar days;
- disable individual accounts with 40 calendar days of inactivity - if no request is received to reactivate the account within an additional 80 calendar days, the account must be deleted;
- deny access to all individuals while system security is not functioning properly;
- prevent the non-repudiation of system processes;
- include tools to verify and log system activity and be secured for a period in accordance with federal, state and local laws, regulations and rules, accreditation criteria and institutional policies; and
- display a network log-in banner during system authentication that must state the system is for authorized use by authorized individuals only; all system use is logged and subject to be monitored; and there are consequences for access violations.

4.1.2 Passwords

Passwords are the primary method of access security and are a major key to the success of information security at UMC. Under Mississippi law, it is a crime to use another person's password or disclose passwords to another person for the purpose of obtaining unauthorized access to information. Passwords must:

- be difficult to predict;
- be a combination of at least six alphabetic and numeric characters;
- be changed frequently, but at least once every 180 calendar days, when initially assigned, and on first use after reset;

- never be reused; and
- be kept secure and not shared with anyone.

4.1.3 Physical Security

All UMC electronic resources, including all forms of media containing UMC sensitive or confidential information, must be physically and environmentally secured to prevent theft, destruction or unauthorized access. Individuals must protect information in a manner that minimizes the possibility of damage or destruction from hazards, such as fire and water.

4.1.4 Log-In/Log-Off

Individuals must:

- access secured systems by using their assigned logon ID;
- assume responsibility for anything that occurs under their assigned logon ID;
- log off or secure systems when a system is unattended; and
- refrain from using information or systems unless authorized.

4.1.5 Remote Access

Individuals needing any remote access, such as modems, virtual private network (VPN) or peer-to-peer protocol (PPP), must register their request with DIS. DIS must certify all remote access accounts annually.

4.1.6 Revoking System Access

System access must be revoked by designated security administrators when any of the following occurs:

- inappropriate use;
- termination;
- suspension;
- security breach;
- change in enrollment status; or
- change in need-to-know.

4.1.7 Termination

Termination refers to the conclusion of an association between UMC and an individual. Prior to the effective date of termination, individuals must contact the Department of Human Resources for the appropriate exit processing procedures and appropriate disposal of all UMC sensitive and/or confidential information from all personally owned electronic devices.

In the case of a suspension or involuntary termination, the individual's supervisor or department chair must immediately notify OIS by e-mail (dis-ois@dis.umsmed.edu) and telephone (984-1790) with the effective suspension or termination date; the individual's name; his or her employee number, if applicable; and the department account number.

When the deans in the various schools certify students for graduation, the appropriate dean's office must notify the Division of Student Records and Registrar in a signed written document and notify OIS by e-mail, listing both the students' names and their date of graduation. When students are suspended or discharged, the appropriate dean's office must notify the Division of Student Records and Registrar in a signed written document and notify OIS by telephone and e-mail.

4.1.8 Departmental Transfer

Prior to transferring to another UMC department, all individuals must:

- make all department-specific information available to the current department manager or his/her designee who determines appropriate methods of disposal, destruction or redistribution of that information;
- submit an Information Resources Request Form to the Division of Information Systems (DIS) Help Desk to establish an e-mail account with the new department; and
- transfer individually created e-mail shared folders and specific departmental e-mail to the current department manager or his/her designee.

UMC does not automatically transfer an individual's information related to e-mail, hard drives and network drives when an individual transfers to another department. Prior to transferring, all individuals should follow the [Electronic Information Transfer Guidelines](#) to avoid loss of information.

4.1.9 System Changes

Any system changes, such as software, hardware, and data, must be approved or sanctioned by the Change Management Committee.

4.1.10 Viruses

Antivirus software must be approved by UMC and properly installed, maintained and used on networks as well as on all devices connected in

any manner, directly or indirectly, intermittently or continuously, to the UMC network.

4.1.11 Encryption

The transmission or storage of any electronic confidential information outside of the UMC network must be encrypted. Encryption products must be approved by DIS and all encryption keys must be kept confidential.

4.1.12 Expectation of Privacy

Individuals expressly waive any right of privacy in their use of UMC information resources, including e-mail and the Internet. All information, including personal information, may be subject to inspection or disclosure when required by and consistent with federal, state and local laws, regulations and rules, accreditation criteria, institutional policies or time-dependent critical circumstances.

4.1.13 Electronic Mail

When conducting UMC-related business, education, research or health care services, individuals must use only authorized UMC electronic mail (e-mail) accounts.

After a specified time, non-archived e-mail is automatically deleted in the order in which it is received or generated.

When requested by the department chair or senior management, UMC may extend e-mail access for a limited time to terminated individuals.

4.1.13.1 Disclaimer

Individuals must add the following disclaimer to all external communications containing sensitive or confidential information:

Individuals who have received this information in error or are not authorized to receive it must promptly return or dispose of the information and notify the sender. Those individuals are hereby notified that they are strictly prohibited from reviewing, forwarding, printing, copying, distributing or using this information in any way.

4.1.14 Electronic Protected Health Information (EPHI)

DIS, the Office of Compliance and UMC legal counsel must approve all EPHI contracts and agreements.

4.1.15 Institutional Publications

All UMC institution-wide announcements and all official institutional communications, announcements and publications must be approved by the Division of Public Affairs before distribution.

4.2 Appropriate Use

Access to UMC information resources, including communications, is provided for use in activities relating to business, education, research and health care services. Individuals must use these resources only when authorized and only to accomplish their assigned duties. Individuals must protect UMC information from accidental or intentional misuse or unauthorized access, modification, destruction or disclosure.

See supplemental information for examples of inappropriate use.

4.2.1 Personal Use

Limited personal use is permitted, provided that such use does not:

- interfere with UMC operations;
- generate incremental identifiable costs to UMC;
- negatively impact job performance;
- involve any activities not sanctioned by UMC;
- violate UMC codes of conduct, bylaws or policies;
- violate federal, state and local laws, regulations and rules;
- display, print or transmit information that is offensive;
- disrespect the rights of others; or
- compromise the integrity of the systems and related physical resources.

4.2.2 Nondisclosure

Individuals must not disclose any sensitive or confidential information unless the release of such information is directly related to the performance of their assigned responsibilities.

4.2.3 Intellectual Property

Intellectual property refers to all patentable materials, copyrighted materials, trademarks, software and trade secrets. Individuals must assume that all intellectual property is protected by copyright.

Information must be:

- reproduced only after permission has been obtained from the source;
- properly identified when quoted from other sources; and
- approved by the appropriate owner and the Division of Public Affairs prior to public release.

Individuals must comply with all applicable laws and regulations, including those for electronic access licenses or any other legal binding agreements, when conducting UMC business. For more information about copyright issues, see the [UMC Copyright Portal](#). Patentable materials, such as tangible innovations, inventions and know-how (non-patented technology), are governed by the UMC [Patent and Invention Policy](#). All information published on the Web is protected by copyright laws unless specifically stated to the contrary.

In keeping with academic freedom and tradition, all faculty **own and control** instructional materials and scholarly works created at their own initiative with usual UMC resources. Some examples are lecture notes, transparencies, digital media, slides, case examples, articles, books and CD-ROMs, regardless of the form in which the ideas or processes are disseminated. Intellectual property protections for all UMC non-faculty individuals are interpreted by the UMC legal counsel.

4.2.4 Software Agreements

Software must be used only in accordance with its license agreement. Individuals are responsible for registering all software licenses with the Office of Software Compliance for any software deployed or installed on their computers. Individuals must obtain and produce upon request a license for any software either delivered or installed on their computer, excluding site licenses.

4.3 Web Environment

All Web sites containing information related to UMC business must be authorized or registered by the [ISSPC Web Subcommittee](#). All UMC schools, departments, divisions and other recognized services are required to maintain a presence in the UMC Web environment.

The [Rules and Procedures for the UMC Web Environment](#) establish requirements and provide instruction for all UMC-related Web sites.

The UMC Web environment must be strategically integrated with all aspects of the UMC mission. All information published on the Web must promote the purpose of the Web site and must be appropriate for

public distribution. Web sites in the UMC Web environment must include links to the [UMC Web Privacy Statement](#) and the [UMC Web Legal Disclaimer](#).

4.4 Contingency Planning

Controls must be established to enable UMC to restore electronic information from any hardware, software or other electronic media. These controls must include a recovery plan that prioritizes contingency procedures by identifying critical information and its impact on the organization.

4.4.1 System Backup and Recovery

System backup and recovery controls include, but are not limited to:

- maintaining and securing copies of original operating systems, applications and documentation at on-site and off-site locations; and
- maintaining and annually testing the UMC disaster recovery plan, including all department/unit plans.

4.4.2 Data Backup

Data backup and recovery controls include, but are not limited to:

- establishing data retention requirements;
- backing up data in a frequent and synchronized manner; and
- maintaining and securing copies of critical data at on-site and off-site locations.

To avoid loss of information, individuals should archive UMC electronic information, including important e-mails, on the UMC network for systematic back-ups. When this is not possible, individuals must back-up UMC information residing on their hard drives in a frequent manner that ensures accurate and complete recovery of information. These back-ups must be protected and stored away from the original source.

UMC is not responsible for any lost, incorrect, non-delivered or processing-delayed personal data.

4.5 Disposal of Information

To prevent unauthorized use of UMC resources, sensitive and confidential information and licensed software must be secured until appropriate disposal. Information must be removed from electronic devices before they are sold, transferred or discarded, according to

UMC and OIS standards. Appropriate methods of disposal include, but are not limited to, shredding appropriate hard copies and rendering data files unreadable on any storage media or electronic equipment.

UMC-authorized documentation explaining the method of rendering data files unreadable must accompany any electronic equipment that is disposed and must include the name of the person responsible for taking the action.

5.0 POLICY INVESTIGATIONS

Any external investigations of UMC information must be referred to the UMC legal counsel for appropriate action. Internal investigations of UMC information must be referred to the Department of Internal Audit.

6.0 SANCTIONS

Individuals violating the UMC Information Policy are subject to disciplinary action, up to and including termination. All violations must be reported to the Department of Internal Audit and OIS. Employee violations also must be reported to the Department of Human Resources; student violations also must be reported to the dean of the appropriate school. The intentional reporting of false violations will be treated as a violation. UMC strictly prohibits retaliatory action against individuals reporting violations.

7.0 POLICY EXCEPTIONS

In rare circumstances, exceptions to the UMC Information Policy may be permitted. Owners must submit a Policy Exception Agreement Form in advance to OIS requesting approval.

8.0 DEFINITIONS

- **Change Management Committee:** a campuswide committee that protects the entire UMC information technology environment by establishing standard procedures for the implementation of all changes.
- **Compromise:** accidental or intentional misuse or unauthorized access, modification, destruction or disclosure of information or systems.

- **Confidential Information:** information that must be protected by law, ethical practice, or UMC business practice/policy, or that represents competitive market data, legal, contractual and financial aggregate data.
- **Critical information:** any information vital to UMC's operations.
- **Electronic mail (e-mail):** any electronic document created and/or associated with an electronic mail system.
- **Encryption:** a process involving data coding to achieve confidentiality, anonymity, time-stamping and other security objectives.
- **Encryption Key:** a password used to control the algorithm governing an encryption process.
- **Individual:** one who has access to UMC information.
- **Information system:** an interconnected set of information resources under the same direct management control that shares common functionality.
- **Media:** anything that stores UMC information.
- **Need-to-know:** the individual's qualification for access to only that information which is required to conduct his or her assigned responsibilities.
- **Network:** the interconnectivity of all UMC information resources.
- **Non-repudiation:** a feature of a security control or application that prevents individuals using a system from denying involvement in an event with which they are associated.
- **Password:** a confidential string of characters used to identify or authenticate access to information resources.
- **Peer-to-peer protocol (PPP):** electronic communications between parties that have the same capabilities that allow either to initiate a communication session.
- **Remote access:** a connection to the UMC network from an off-site location.
- **Screen Saver:** a program which displays either a completely blank screen or a constantly changing image on a computer monitor.
- **Security Administrator:** individuals charged with safeguarding information access and use as directed by the owner.
- **Senior Management:** the highest level of management within the applicable organizational unit.
- **Sensitive Information:** information that must be protected because its accidental or intentional misuse or unauthorized

access, modification, destruction, or disclosure will cause perceivable damage to someone or something.

- **Virtual Private Network (VPN):** a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the UMC network.

9.0 CONTACT INFORMATION

For questions about the UMC Information Policy or for more information, send an e-mail to OIS (dis-ois@dis.umsmed.edu), call the chief information officer at 984-1140, or call the Office of Compliance at 815-3944.

SUPPLEMENTAL INFORMATION

Examples of Inappropriate Use

Individuals who engage in inappropriate use of UMC information resources, including but not limited to the following, are subject to disciplinary action, up to and including termination:

- accessing or soliciting information without the need-to-know;
- allowing others, such as family members and friends, to perform activities on the UMC network or any secured system under one's own logon ID;
- performing or requesting to perform any activities in a secured system under someone else's logon ID;
- attempting to access a secured system without proper authorization;
- attempting to obtain proper authorization through fraudulent means;
- disclosing or compromising confidential access codes;
- discussing confidential information in public areas;
- leaving sensitive or confidential information, such as patient charts or secured systems, unattended;
- forwarding or distributing sensitive information to any party outside UMC without prior approval;
- making unauthorized changes (electronic or written) on a patient chart, student record or personnel file;

- impersonating someone else to obtain a grade, help others obtain a grade or to provide falsely identified materials;
- conducting activities not sanctioned by UMC, such as for-profit, fund-raising, gain-making or political activities;
- creating or intentionally releasing a computer virus;
- copying all or part of copyrighted material, such as electronic books, journals, graphics, Web content and software, without permission from the publisher, other than for private study, scholarship, research or classroom purposes (Copyright Portal – Fair Use);
- distributing or transmitting any copyrighted material, including Web content such as class information or PowerPoint files on BlackBoard, without permission from the publisher;
- making any public representation about UMC without the approval of the Division of Public Affairs, such as advertisements, Web pages, electronic bulletin board postings, e-mail or voice mail;
- misrepresenting UMC or perpetrating fraud;
- using personal e-mail accounts with an Internet Service Provider (ISP) or any other third party for any UMC business communications;
- obtaining or attempting to obtain an unauthorized access code;
- providing UMC information to the lay media without approval from the Division of Public Affairs;
- refusing or delaying to sign the Information Policy Agreement form;
- removing any sensitive or confidential information from UMC premises unless there has been prior approval from the owner;
- using UMC resources to harass, inflame, intimidate or threaten others;
- publishing or publicly displaying information that would place UMC in an embarrassing or an uncomplimentary position;
- sending or forwarding chain letters;
- using, sharing or reproducing sensitive or confidential information for unauthorized purposes or personal reasons;
- storing non-UMC-related information on network servers, such as music, videos or games;
- engaging in peer-to-peer file-sharing without proper authorization from the department and DIS;
- storing any sensitive or confidential information with personal non-UMC information on any removable data storage media;

- destroying UMC information with malicious or fraudulent intent;
- using UMC resources to access, view, publish or transmit sexually explicit materials unrelated to legitimate academic purposes;
- modifying, altering or tampering with UMC systems hardware or software without authorization;
- intentionally reading sensitive or confidential information, such as patient charts, student records or personnel records, without authorization; or
- using any device, such as camera phones, camcorders and scanners, to record or transmit images of sensitive or confidential information without authorization.

Electronic Information Transfer Guidelines

To avoid loss of information, **PRIOR TO** transferring to another UMC department, all individuals should follow these guidelines:

- export items, such as personal e-mail address books and frequent contact lists, to a removable storage device;
- contact the DIS Help Desk to make transfer arrangements for personal and archived e-mail messages to be moved to the new e-mail account; and
- copy needed personal information from hard drive(s) or network drive(s) to a personal removable storage device.

APPROVALS

Ada M. Seltzer	Date
Chair, Academic Information Services	
Chair, Information Systems Policy Subcommittee	

Dr. David Powe	Date
Associate Vice Chancellor for Administrative Affairs	
Chairman, ISSPC	

Dr. Daniel Jones
Vice Chancellor for Health Affairs

Date

Approval dates: August, 2004; 2006