Charles E. Schmidt College of Medicine

INFORMATION AND DATA SECURITY POLICIES

COM IT

JUNE 2015

BACKGROUND

This document is designed to provide All FAU College of Medicine workforce members (including faculty, staff, students, residents, temporary, volunteers, and other persons who perform work for FAU College of Medicine) with the mandatory standards and policies to protect information systems, confidential and sensitive data from internal and external threats.

Implementation of common information, data security and confidentiality policies which allow for a continuity of operations, without being burdened or obstructed, is both reasonable and feasible. COM personnel will benefit from enhanced security protocols and the protection of key data elements and information systems.

These policies will be consistently implemented and enforced. Adoption of each policy and best practices for securing and protecting data will provide a critical foundation towards safeguarding COM information systems, assets, electronic records and research studies with human subjects.

FAU'S Office of Information Technology (OIT)

FAU's Office of Information Technology (OIT) Information Security Team – governed by legal, privacy requirements and policies – is responsible for protecting information resources that are critical to the academic and research mission of FAU.

The COM policies and standards contained in this manual will augment existing FAU policy and are aligned with University's strategy for the protection of information system and data assets.

CONTENTS

I. INTRODUCTION

What is Information and Data Security?

Information and Data Security (IS) is the protection of information, information systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- Information security is achieved through implementing technical, management, and operational measures designed to protect the confidentiality, integrity and availability of information.

- The goal of an IS program is to understand, manage, and reduce the risk to information under the control of the organization.

Guiding Principles

Many information systems are electronic; however a media-neutral policy towards information will be adopted for the COM, meaning that **any data whether in electronic, paper, or oral format must be protected**. This standard will be systematically instituted across all levels of information and data management at the COM.

The guiding principle and strategy for the COM's Information and Data Security policy is *Security by Default* – meaning that the default configuration settings for any system, research study or initiative are set to **maximum** and methodically scaled down based on either 1) risk analyses 2) usability tests for the most user friendly settings 3) business requirements 4) unacceptable operational burden.

Reviews and Assessments

A review of the COM's data security, confidentiality, and sharing policies and procedures will be conducted at least annually or sooner if improved technologies, University policy, legislative or regulatory changes occur; revisions will be made as necessary.

In addition, a quarterly assessment will be conducted to ascertain whether other changes in personnel, programs, organizations, or priorities require changes in policies and procedures. For example, changes in standards for encryption could affect existing policies and procedures and require software updates or other revisions.

Tracking the security and confidentiality training of staff members authorized to access data, including documenting and storing their signed confidentiality agreements, will also be part of ongoing assessment activities.

Definitions

CONTROLLED VOCABULARY - DEFINITIONS	
Asset	An asset is any tangible or intangible thing or characteristic that has value to an organization. There are many types of assets. Some of these include obvious things like machines, facilities, patents, and software. But the term can also include less obvious things like services, information, and people, and characteristics like reputation and image or skill and knowledge.
Availability	Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users.
Breach	A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter. A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
Confidentiality	Protecting information from unauthorized disclosure to people or processes.
Controls	Any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.
HIPAA	Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
Incident	An incident is the act of violating an explicit or implied security policy, whether knowingly or unknowingly. These include but are not limited to: - Attempts (either failed or successful) to gain unauthorized access to a system or its data

	- Theft or loss of an information system asset or property - Unwanted disruption or denial of service - The unauthorized use of a system for the processing or storage of data - Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
Integrity	To preserve the integrity of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it.
PHI (ePHI)	Protected health information (PHI) / electronic protected health information is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. HIPAA regulations allow researchers to access and use PHI when necessary to conduct research. However, HIPAA only affects research that uses, creates, or discloses PHI that will be entered in to the medical record or will be used for healthcare services, such as treatment, payment or operations.
PII	"Personally identifiable information" (PII), as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
Privacy	Information privacy is the privacy of personal information and usually relates to personal data stored on computer systems. The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business related information or website data. Information privacy is also known as data privacy.
Risk	The likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; hence, it is vulnerable to a threat, such as a thunderstorm, which creates a risk.
Sensitive	Sensitive information is defined as information that is protected against unwarranted disclosure. Access to sensitive information should be

	safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations. Sensitive information also includes any information that is protected by University policy from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.
Threats	The potential to cause unauthorized disclosure, changes, or destruction to an asset. –Impact: potential breach in confidentiality, integrity failure and unavailability of information –Types: natural, environmental, and man-made
Vulnerabilities	Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.

Responsibilities

In general, all COM workforce members have a responsibility to:

1. Collect, use, and disclose personal information only for reasons that are for a legitimate job function, support the mission of COM or FAU, and are allowed by law.

2. Minimize information or data collected and accessed for authorized purposes only. Data must be collected or accessed on a "need to know" or "minimum necessary" standard. Only data needed to answer research questions must be collected and access should only be provided only to those who need it. Data will be limited to the minimum amount needed to do their job.

3. Safeguard personal information in your possession, whether it be in paper or electronic format.

4. Report suspected privacy violations or incidents to the COM Privacy Officer / IT Director.

5. Shred documents containing PII or PHI; NEVER place them in the trash. Contact the COM IT Office for proper disposal of equipment like copy machines and computers.

DATA SECURITY RESPONSIBILITIES	
IRB	Assures the Covered Entity that health information will be protected under the research protocol and that researchers protect data; IRBs must conduct periodic reviews of such research.
FAU OIT Security	Manage the information security incident response and investigation
FAU Privacy Officer	Coordinating with the Office of General Counsel and the OIT Security Officer to ensure that an appropriate Business Associate Agreement is in place with a third-party, prior to conducting business that involves the handling of PHI applicable to the Primary Component.
COM IT	Maintain the software and hardware used to protect the information
FAU General Counsel	Issue policy and guidance with regard to the use of protected health information

II. POLICIES

The following security controls and policies will be enforced with all COM IT information systems. Failure to adhere to these directives increases vulnerability and risk to the user, the College of Medicine and FAU while compromising the integrity of operations.

Non-compliance or violations of these policies will be documented and reported to the appropriate supervisory officials for resolution. These officials include, but are not limited to: COM IT Director, COM Privacy Officer, FAU OIT Security, COM Chief Business Officer, COM Dean and Executive Director of Medical Affairs, FAU Privacy Officer, FAU Office of General Counsel.

POLICY 1.1 - User Access to Computer Resources

Standard Access – All College of Medicine faculty (paid or affiliate), staff, students, researchers and personnel who are given access to computing resources, application systems and the FAU network will be granted 'standard access.' Individual passwords and access to these information systems may not be shared, copied or distributed with others for any purpose. COM IT are the only authorized entity to request passwords on a temporary basis for specific troubleshooting tasks.

Remote access – VPN and other remote access to systems will be based on the established OIT approval processes and managed by OIT. Any change in the user status related to access rights will be managed by the OIT workflow process. Devices used for remote access must conform to the security and privacy requirements in this policy document.

Access reports – COM IT and OIT will review user access reports on a periodic basis on systems which stores (or can access) PHI or PII to determine if the appropriate need-to-know standards have been applied and if policies and procedures are adhered to. Annual reviews will be conducted on network information resources to verify access rights.

Need-to-Know checklist – All new College of Medicine faculty (paid or affiliate), staff, students, researchers and personnel must complete a COM IT checklist to determine required access to systems. COM IT will work with administrative staff during the onboarding process to determine the level of access based on necessity.

Portable media access – Any user who accesses any COM system which stores (or can access) PHI or PII are prohibited from using unencrypted portable media devices, such as portable USB Flash drives or CD/DVD.

In addition to those times where access to work files and FAU devices (including, but not limited to, desktops, laptops, tablets, mobile devices and phones) are necessary, in accordance with IT policies, authorized administrators shall have full access to employee's files on all FAU-issued devices during the time of employment or education

with the Charles E. Schmidt College of Medicine and upon resignation, separation or termination.

POLICY 2.1 - User and Administrator Permissions

Standard User Permissions – All faculty, staff and students at the COM will be granted standard "user" permissions by default to their approved computing resources. These users will be restricted from installing software or altering their secured computer configuration settings. All installations of new software applications, software patches or plugins will be managed through COM IT.

Administrator Permissions – COM IT staff will be the only authorized group of users with Administrator rights to any desktop or laptop. A valid business justification and undue burden justification for granting administrator rights to any faculty or staff computer resources must be submitted to the COM IT Director and COM Chief Business Officer.

POLICY 3.1 – Software Management

Software Catalogue – COM IT will maintain a comprehensive software and licensing catalogue of OIT and COM approved applications for all COM faculty, staff and students. FAU has agreements with various vendors to provide discounted licenses for FAU owned computers. COM IT will manage the distribution, installation, and implementation of software products across all COM computing resources.

All requests for currently unapproved software, open source, shareware and freeware will be submitted to OIT though the formal approval process.

POLICY 4.1- System Lockouts (timeout)

Desktop Lockout – All COM faculty, staff and student desktops and laptops will adhere to an automatic desktop lockout and timeout system after 5 minutes of inactivity. When stepping away from their desks, all users must activate the lockout for their system (Ctrl+Alt+Delete for PCs, then Enter). When leaving the office for the day, all users must save their work and completely logoff from their workstations.

Screensavers – will be automatically activated and password protected after 5 minutes without regard to traffic flow or sensitivity of data. Personal screensavers, music and other activities that "fool the system" into thinking there is activity cannot be used. Screensaver time limits will be set to no more than 2-3 minutes in certain high traffic areas.

POLICY 5.1 - Encryption and Backup

Full Device Encryption – All COM mobile devices, desktops and laptops (regardless of Operating System or Platform), servers, USB drives that store, collect, process data will

be fully encrypted using OIT-approved encryption methods and software. Full disk/FIPS-2 (drive) encryption will be used where possible on all COM devices. All data being sent will be encrypted. Software-specific file passwords (such as Microsoft Word or Adobe PDF passwords) cannot be used as a substitute for encryption or protection.

Secure Encrypted Email – All emails involving ePHI (Electronic Personal Health Information) will be sent securely using OIT-approved, end-to-end encrypted email technologies.

Encrypted Backup Process – All COM desktops and laptops are required to use the file and document backup storage solution implemented by COM IT. All COM devices using the file backup solution will be fully encrypted to protect both PHI and ePHI in motion and at rest. The files and data stored on these backup servers are restricted on a need-to-know basis.

POLICY 6.1 - Anti-Virus and Malware

Standard Software – All COM computing resources are required to use the anti-virus and anti-malware solution implemented by COM IT.

POLICY 7.1 - Mobile Device Management (MDM)

Standard Software – All FAU/COM issued mobile and tablet devices are required to enroll in the MDM solution implemented by COM IT.

POLICY 8.1 - Bring Your Own Device (BYOD)

Acceptable Usage – COM faculty, staff and students may choose to bring their own mobile or laptop device and connect to the FAU network for official business, educational or research purposes. The following provisions will be adhered to when using your own device for official business, education or research:

- Jailbroken and rooted devices are not allowed
- Enrollment in MDM is mandatory when on the FAU network
- FAU email accounts may not be added onto personal devices without MDM, nor may FAU emails be forwarded to personal accounts.
- Devices must be protected by screen lock passwords, enabled after 5 minutes of inactivity
- Devices must have a vendor supported operating system and be regularly updated with latest OS and patches
- Anti-Virus software from an OIT-approved vendor must be installed with current definitions in place
- Business data and personal data must be kept separate
- All COM or FAU-related data (ie, non-personal) must be encrypted
- Custom profiles for each device type and manufacturer

- VPN (Application or Device) required for connectivity
- Periodic re-authorization and re-verification with COM IT is required

POLICY 9.1 - Physical Security for Devices

All COM faculty, staff and students must adhere to best practices concerning the physical security of their computing devices.

General Security – The general recommendations for physical security are the same for all devices, particularly smaller devices like laptops, hard disks, smartphones, music players, and flash drives:

- Never leave your laptop or small device unattended, even for a moment, even in your office. Most laptops are stolen from their owner's office, while the owner is at a quick break or meeting.

- If you must leave your laptop in a car, stow your bag in the trunk before you reach your destination, so potential thieves don't see you doing so. Make sure your car is locked.

- Do not leave portable electronic equipment unattended when traveling. Monitor it closely while checking in at an airport or hotel counter and while passing through airport security checkpoints. If you must leave the equipment briefly unattended in a hotel room, secure it to a desk or table with a cable lock or keep it in a hotel provided safe if available.

- When leaving your office space, lock your computing resources in a desk or an office that can be locked.

- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

- Whiteboards containing Restricted and/or Sensitive information should be erased.

POLICY 10.1 – Printers, Scanners, Copiers, Fax and Shredders

Document security – Every time you scan, copy, or email a document, an image of the original document may remain in storage on the device. Without any additional protective measures such as encrypting the document while in storage or securely wiping the data, individuals with some technical capability can recover such information.

All COM faculty and staff using a desktop, multifunction printer (MFP) or multifunction device (MFD) that incorporates the functionality of multiple devices (e.g., printer, scanner, photocopier, fax, email) used to manage unencrypted data must contact COM IT for help in protecting the data stored in these devices.

Tracking and Analytics – All network printers must be password protected and firmware updates applied on a regular basis. Print jobs must be securely managed and tracked through a document management and financial accounting solution.

Destruction of confidential/sensitive documents – All confidential and sensitive documents containing PHI, EHRs, EMRs or PII of any kind must be destroyed using a high quality, high volume, cross-cut industrial grade shredder.

POLICY 11.1 – Safe and Secure File Sharing

Acceptable Services – The following tools can be used to allow secure collaboration and document/file transfers:

- Microsoft OneDrive – When logging in with FAU authorized account
- Network Share Drives – Only for non-sensitive information
- SharePoint sites
- OIT FileLocker

Prohibited Services – The following services cannot be used for document/file transfers:

- Any cloud storage provider not listed under the acceptable services (i.e. “Google Drive, Box.net, Dropbox”).

POLICY 12.1 – Cloud Storage and Services

All COM faculty, staff and students must adhere to FAU and OIT acceptable use policies on cloud storage and cloud services.

POLICY 12.2 – Secured Servers and Applications

Research and Data Storage – All COM studies and research requiring the need for secure servers, secure access and storage of data will coordinate their projects with the COM IT Office prior to initiating the study. Sensitive research data will remain encrypted at rest at all times.

Applications for Curriculum or Management – All COM users who access educational applications used in the curriculum and COM-developed Web applications must adhere to complex password requirements, privacy and security requirements, and user access definitions defined by COM IT.

POLICY 14.1 - OIT CyberSecurity

FAU IT Security policies – All COM faculty, staff and students must adhere to OIT's CyberSecurity and Information Security processes which include, but are not limited to:

- Acceptable Operating Systems, Software and Version Numbers
- Enforced password complexity and strength audits
- Enforced password resets
- Electronic filing and protection of passwords
- Intrusion detection / scanning
- Network and WiFi standards
- Banned 'rogue' devices
- Penetration (Pen) Testing standards and remediation
- Identity Theft and Phishing Protection
- Illegal File Sharing policies
- VOIP encryption policies for ePHI

All COM faculty, staff and students must adhere to FAU's Acceptable Use of Technology Resources policy: http://www.fau.edu/security/policies.php and overall University policies on conduct: http://www.fau.edu/policies/.

III. HIPAA / HITECH

All College of Medicine faculty (paid or affiliate) workforce members -- staff, students, researchers and personnel -- will adhere to the highest standards in HIPAA compliance, training and accountability in preserving the integrity of its assets, medical/health records and research data.

Please refer to the FAU HIPAA Privacy and Security website for additional guidance and information: http://fau.edu/hipaa/

IV. INCIDENT RESPONSE PLAN (IRP)

The COM will adhere to FAU's Emergency Response Policy, which includes amendments to address HIPAA provisions and coordination with the Incidence Response Team (IRT).

A security incident is an event that compromises or has the potential to compromise:

- the operation of covered core systems or
- confidentiality or integrity of covered data assets

A security incident may involve any or all of the following:

- a violation of campus computer security policies and standards
- unauthorized computer/mobile device or data access
- presence of a malicious application, such as a virus
- presence of unexpected/unusual programs
- a denial of service condition against data, network or computer
- misuse of service, systems or information
- physical or logical damage to systems
- computer or mobile device theft

An Incident Response Plan (IRP) is a set of written instructions for adequately detecting, responding to and limiting the effects of an information security incident, an event that may or may not be an attack or threat to computer system or corporate data security. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

According to the SANS Institute, there are six steps to handling an incident most effectively:

Preparation: The organization educates users and IT staff of the importance of updated security measures and trains them to respond to computer and network security incidents quickly and correctly.

Identification: The response team is activated to decide whether a particular event is, in fact, a security incident. The team may contact the CERT Coordination Center, which tracks Internet security activity and has the most current information on viruses and worms.

Containment: The team determines how far the problem has spread and contains the problem by disconnecting all affected systems and devices to prevent further damage.

Eradication: The team investigates to discover the origin of the incident. The root cause of the problem and all traces of malicious code are removed.

Recovery: Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for any sign of weakness or recurrence.

Lessons learned: The team analyzes the incident and how it was handled, making recommendations for better future response and for preventing a recurrence.

a. Reporting Lost or Stolen Data and Devices

Any lost or stolen data and/or devices must immediately be reported by phone to the following COM IT Helpdesk, who will follow up with reporting to the COM Building Manager and Campus Police if necessary.

If COM users suspect there has been an incident that might involve the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA, it must be promptly reported.

Following the notification, an incident intake report will be included which lists:

- Contact person name and phone number
- Device or data which was breached, compromised, lost or stolen
- IP address, hostname and physical location of breached system
- Name of the covered system
- What types of covered data was available on/from the breached host?
- Impact of the incident (e.g. the number of data records are compromised or the number users that are affected by unavailable system)

For each file containing personal information:

- Name of the file
- Size of the file
- Location of (full path to) the file
- Was the data encrypted, and if so, how?

Additional details which may be included on the intake form include:

- Description of the security incident, including the timeline of activities, how the incident was detected, impact (business and technical) of the incident, details of mitigating controls in place such as what data encryption mechanism was used.

- Action being taken on the breached system (what's the state of the system now, etc.)

b. Detection and Analysis

- Lost or stolen devices will be verified that full disk encryption was applied. Devices should be disabled by technical means, when possible. A police report will be filed through the University Police.

- COM will follow direction from University Office of Information Technology Information security office for detection and analysis of threats and vulnerabilities. Should a threat be found, the Containment, Eradication & Recovery policy will be applied.

- COM IT will use best efforts to monitor any logs available to detect threats introduced to university owned devices. Should a threat be found, the Containment, Eradication & Recovery policy will be applied.

c. Containment, Eradication & Recovery

- Containment – Users who are identified to have an incident should have their accounts temporarily disabled until the eradication process has been completed. Devices which have been identified as having an incident should have network access removed from the system.

- Eradication – Systems which have been compromised by a virus or malware should be wiped, data backed up, and be re installed.

- Recovery – Data from affected machines

d. Post-Incident Activity

- Users who have had an incident should be referred for additional information security training.

- If a cause of an incident has been determined, steps should be taken in the future to try and mitigate the risk from happening.