THE UNIVERSITY OF ALABAMA®

# UA HIPAA CORE SECURITY PROCEDURE

**Unit:** Office of Information Technology (OIT)
**Effective Date:** 4/20/2005
**Revision Date:** 10/22/2020

**Contact:** UA HIPAA Security Officer
**Title:** Chief Information Security Officer

## Purpose:

The purpose of this policy is to make sure that covered entities within The University of Alabama meet the requirements of HIPAA 45 CFR Part 160 and Subparts A and C of Part 164.

## HIPAA Security Rule General Requirements

This entire Policy applies to UA Designated Health Care Components, UA departments serving as Business Associates for non-UA covered entities, covered health plans of The University of Alabama (a Covered Hybrid Entity) and to the administrative departments at The University of Alabama that provide legal, billing, auditing, or other administrative support for the above, including but not limited to The University of Alabama Office of Counsel, The University of Alabama System auditors, the University's HIPAA Privacy and Security Officers, Office of Information Technology, Human Resources, and Risk Management. For purposes of this Policy, these UA entities and their affiliated administrative support departments shall be referred to as "covered entity or entities"

A HIPAA covered entity is any entity that furnishes, bills or receives payment for health care in the normal course of business, maintains ePHI and transmits covered transactions (such as insurance billing) electronically.

Covered entities must ensure the confidentiality, security, integrity, and availability of electronic protected health information (hereinafter referred to as "ePHI") that it creates, receives, maintains, or transmits. Covered entities must protect against any reasonably anticipated threats or hazards to the security or integrity of such information. Covered entities must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.

Workforce compliance is required by all employees, volunteers, physicians, residents, interns, trainees, contracted individuals, and other persons whose conduct, in the performance of work for a covered entity is under the direct control of the covered entities, whether or not they are paid by the covered entities.

Covered entities may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications. In deciding which security measures to use, covered entities should consult with its support organization and consider its size, complexity and capabilities. Covered entities should also consider its technical infrastructure, hardware and software capabilities along with the cost of the security measures. Covered entities should consider the probability and criticality of potential risk to ePHI.

Covered entities must comply with administrative, technical and physical safeguards with respect to all ePHI.

### Policies and Procedures Documentation Requirements

Covered entities will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security regulations.

All Security Rule policies and procedures will be documented in writing either in paper records, or electronically. The documentation will be retained for at least six years from the date of the creation of the documentation, or the last date that the document was in effect, whichever is later.

Covered entities will disseminate all official updates of policies and procedures to its workforce as applicable in a reasonably prompt time period, while also ensuring the security of information.

Covered entities will review periodically, and update as needed, its policies, procedures, and documentation in response to environmental or operational changes affecting the security of the ePHI.

**Violations of Policy**

Violations of these policies may result in disciplinary action, up to and including dismissal, and civil and criminal penalties.

Vendors or contractors who do not follow the above policies may be subject to breach of contract penalties.

Business Associates must comply with UA policies applicable to the nature of their work with UA. Business Associates who do not follow applicable requirements could be subject to breach of contract penalties, possible legal prosecution, civil and criminal penalties, and other legal remedies/ramifications as are available to UA.

# Risk Analysis and Management of ePHI

Covered entities who maintain or transmit ePHI shall:

- Conduct and document a thorough risk analysis a minimum of every two years by the covered entities' HIPAA Privacy and Security Officer(s) in coordination with the UA HIPAA Privacy and Security Officers.
    - Exceptions to the two-year analysis include:
        - When changes to the environment could affect the confidentiality, integrity, or availability of sensitive or business-critical information, a risk analysis or impact analysis must be conducted.
        - The occurrence of an event or incident warranting the reevaluation of risks requires an immediate risk analysis.
        - Regulatory requirements that necessitate a more frequent risk analysis.
- Conduct and document risk analysis, consisting of the following minimal components:
    - Risk assessment,
    - Asset inventory,
    - Data criticality analysis,
    - Threat assessments,
    - Determination of risk exposures, and
    - Development of a risk mitigation strategy.
    - Maintain a written record of the analysis/assessment for 6 years.
- Submit the risk analysis findings to the UA Privacy and Security Officers without unreasonable delay and in no event later than 30 days of concluding their analysis.
- In collaboration with the appropriate covered entity leadership, document risk acceptance decisions, and implement measures to remediate vulnerabilities and sufficiently reduce risk exposure within a reasonable timeframe after concluding their assessment.
- Document the remediation activities.
- Submit the final risk remediation plan to UA HIPAA Privacy and Security Officers.

- Provide written exemption or extension requests for any vulnerability that, due to business or technology constraints, cannot be remediated in the allotted time. All such requests must be approved by the OIT security office, HIPAA Privacy and Security Officers and Risk Management.

Data produced from the risk analysis shall be kept confidential.

All business associates shall be required to sign a business associate agreement reviewed by UA Legal Counsel and approved by the UA HIPAA Privacy Officer, UA HIPAA Security Officer, Entity Privacy Officer, and the covered entity's senior manager.

# Information Systems Account Management

**Background Information**

Access is determined by position, role, and/or responsibility. If an employee's position, role, and/or responsibility change, system access shall be reevaluated as to its applicability. If the user believes that his/her account has been compromised, the user must contact their information systems help desk to report the occurrence and change his/her account information.

**Unique User Identification**

All users must have a standard unique identifier (user ID) assigned for accessing UA information resources.

Whenever possible, UA information resources shall prohibit concurrent or simultaneous access by the same user ID except in cases where business use has been deemed necessary and appropriate and authorized by management.

Generic user IDs shall only be allowed where the functions accessible or activities carried out by the ID do not need to be traced or audited.

Service accounts used for communications between systems and to operate services within a server environment shall be unique and shall be held confidential by the system administrators. OIT shall establish auditable procedures to securely maintain and access service accounts by systems administrators.

A user's account shall be promptly deactivated upon notification of separation of their relationship with UA.

Users shall be given the minimal necessary access privileges to perform their duties. If a user's position, role, and/or responsibility changes the user's account privileges shall be reevaluated and modified (if necessary) by their manager to match the minimum necessary for the current position's responsibilities.

All systems and applications are required to use at least a user identifier (typically a user ID) and an authentication mechanism, i.e. password, token, biometrics, smart card.

Minimally each department or clinical area shall have a designated written authorization process for granting access to UA information resources. This process shall include a procedure for validating a

user's identity and notifying the user's supervisor. Such a process shall include how the person granting access is identified. This person shall be a specifically identified individual who grants others access to resources.

- All account requests shall at least include the last four digits of a user's social security number or an equivalent, such as employee CWID.
- All users requesting an account shall be required to provide their name as it appears on their personnel records (if applicable), department, title, phone number, and their supervisor's name and email address.

A process to document initial account requests shall be in place for each system.

Personnel shall notify the appropriate information systems help desk of any account violations.

Newly implemented systems and current systems with the capability shall comply with the following policies. Existing systems without the capability shall use their maximum available security features and work to comply with the following policies as systems are upgraded.

- Multi factor authentication should be used in all cases where appropriate to the business function
- All systems shall enforce strong password selection.
- All systems shall have audit trail capabilities that provide documented evidence of user access.
- Passwords shall not be viewable to users or system administrators.
- Passwords shall be stored encrypted on the system.
- Default passwords and PINs shall be changed.
- Guest accounts shall be disabled.
- The system shall prompt a user to choose a new password upon initial access to the system or after his account has been reset.

**User Responsibilities**

Users shall protect account information and prevent use of their IDs, passwords, PINs, and tokens by others.

Users shall access information appropriately – with individually-assigned accounts and in compliance with UA standards and policies.

Users shall not re-use expired passwords for at least 4 password-expiration cycles.

Users shall choose a new password upon initial access to the system and each time the password is reset by the administrator – to the extent that password change capabilities are supported by the system.

Users shall choose strong passwords – to the extent that strong password capabilities are supported by the system.

Users have a responsibility to close or log off applications or lock the workstation immediately after use.

Users shall provide account administrators with their manager's contact information (name, e-mail and phone number) when directly requesting access to information resources.

Vendors and contractors shall not be granted access without approval of the UA sponsoring department. Access requests shall be submitted by the vendor's/contractor's assigned UA management contact.

Users shall contact the appropriate system administrator for password resets and user account issues.

Users shall not verbally reveal their password to the helpdesk or any other person asking for the password. If the helpdesk needs the password, it will be a reset.

**Account Administrator Responsibilities**

Account administrators shall notify the user's manager when the user submits a direct request for access.

Account administrators shall add, modify, and disable user accounts upon notification from the appropriate manager.

Account administrators shall periodically analyze system logs to determine accounts that may have been compromised.

Account administrators shall not accept access requests from vendors or contractors. Access requests for vendors and contractors shall be submitted by UA management with oversight for the vendors'/contractors' activities.

Account administrators shall ensure that systems are configured to comply with this policy.

**Manager Responsibilities**

Managers shall ensure and justify appropriate access for those under their supervision – including employees, vendors, contractors, interns, volunteers, and other third parties.

Managers shall provide account administrators with a projected separation date or contract termination date when requesting user accounts for temporary employees, vendors, contractors, and other third parties.

Managers shall ensure that access rights are the minimum necessary and commensurate with current job responsibilities for all individuals under their supervision.

Managers shall review, approve, and submit requests for the user accounts of those individuals under their supervision.

Managers shall ensure that individuals under their supervision are trained to access and use UA information resources.

Managers shall enforce standards, policies, and procedures associated with the use of UA information resources.

Managers shall notify relevant account administrators upon an employee's separation of employment, reassignment of duties, or transfer and upon completion of service by an intern, volunteer, vendor, contractor, or another third-party.

# Internet and eMail Use

All email messages, documents, correspondence and data obtained through UA network resources are considered UA property.

Users shall have no expectation of privacy in email and internet use and shall comply with all applicable UA policies regarding use of email and the internet.

UA may monitor messages and internet use without prior notice.

Users are responsible for reporting any suspected or confirmed violations of this policy to their department manager or to any one of the following officers, Entity Security Officer, Entity Privacy Officer, UA HIPAA Privacy Officer, or UA HIPAA Security Officer.

Users shall not misuse their internet privileges, e.g. spending excessive time on the internet for non-work-related business or accessing inappropriate sites.

Users shall not misuse their email privileges, i.e., sending and forwarding non-business-related mass emails.

Users shall delete chain and junk email messages without forwarding or replying to them. Electronic chain letters and other forms of non-business-related mass mailings are prohibited.

Personnel shall not use UA resources to view, record, or transmit materials which violate UA policies. Inappropriate messages, pictures, and/or other visual images/materials include, but are not limited to:

- **Fraudulent messages** - Messages sent under an anonymous or assumed name with the intent to obscure the origin of the message.
- **Harassment messages** - Messages that harass an individual or group for any reason, including race, sex, religious beliefs, national origin, physical attributes, or sexual preference.
- **Obscene messages** - Messages that contain obscene or inflammatory remarks.
- **Pornographic materials** -This includes, but is not limited to pictures, audio/video files, literature, or newsgroups.

Users shall not engage in spamming activities. Electronic chain letters and other forms of non-business-related mass mailings are prohibited.

Users shall not photograph, post, or transmit patient images or information, electronically or otherwise, unless doing so is in accordance with an approved use or disclosure, and approved methods for doing so are utilized.

Users shall contact the UA Information Security Office for a list of approved cloud service providers before storing, sharing, or processing sensitive, restricted, or protected health information (PHI) in the cloud. The use of cloud storage services must be reviewed by the HIPAA Security and Privacy Officers involved to determine the need for a Business Associate Agreement as well as any other privacy protection agreements required.

Users shall not send or forward email containing sensitive, restricted, or protected health information (PHI) to a public email system, e.g., Hotmail.com, gmail.com, without a current BAA or approval from the Entity Security Officer and the UA HIPAA Security Officer .

Users shall not forward sensitive information, PHI, or other UA business information to non-business-related email accounts, including but not limited to Gmail, Yahoo, iCloud,etc.

Personal email accounts shall not be used for official UA business.

UA reserves the right to block access to non-business-related material.

Email transmission of ePHI, if necessary, shall be conducted with the highest level of security applied and only in situations where the email is necessary for the treatment of the patient, payment, and health care operations. Encryption of electronic health information via email is optional for internal only recipients (sent on UA's secure email environment). This includes email between UA covered entities and the employees of the University of Alabama System Office in Tuscaloosa. To send email transmissions over the Internet (outside the UA secure email environment), ePHI and other sensitive information shall be encrypted. Email shall not be transmitted over the Internet from any other email system unless/until an encryption method is approved for that email system. Detailed instructions for secure email can be found here.

Users shall comply with all laws related to copyright, intellectual, and personal property.

Users shall check their email regularly and delete unneeded email.

Users shall not knowingly download non-work-related executable files from the Internet.

Users shall not establish peer-to-peer connections to external parties.

Users shall not knowingly enable anyone to gain unauthorized access or control of any device, application, or system to the data networks.

Users shall report suspicious emails to their covered entity Security Officer, and forward the suspicious email to the UA Information Security Office at: security@ua.edu. Do not open any attachments in the suspicious email.

For the UA HIPAA network, the use of any software or service that hides the identity of the user or the location of the user while using the Internet is prohibited (including but not limited to proxy bypass, anonymization networks such as TOR, and VPN connections).

Individuals may be granted access to the email account of their former employee or vendor with the covered entity's HIPAA Privacy Officer approval, then Human Resources approval. This may require written approval from requestor's supervisor.

- The account shall be used only for the retrieval of existing email and shall not be used to impersonate the former personnel or send email communications on their behalf.
- Access shall be granted for 7 days and any extension must be approved by Human Resources.

Users shall not utilize their UA passwords on any non-corporate systems (i.e., banking, personal email, etc.).

Users shall not circumvent UA technical security controls.

Users shall not transfer restricted or sensitive information to an unencrypted or unapproved device.

Users shall log off application, workstations, laptops, and devices after use.

Users shall not store restricted or sensitive information on non-UA equipment such as personally-owned devices unless properly authorized to do so.

Users shall not provide personal or official UA information solicited by unknown individuals or suspected phishing email or websites.

Users shall follow the same security policies at any alternate workplaces as those required on the UA networks.

# Information Systems and Network Access

Requests for access to UA's ePHI shall be granted only to individuals with a direct need to know.

Approval will be based upon minimum necessary privileges and the direct need to know for a specific job function.

For UA systems containing ePHI and requiring the services of a non-HIPPAA workforce member, the system owner is responsible for signing an internal sponsor agreement and monitoring the individual's activities on the system. Additionally, if access to ePHI is a possibility, the system owner must make sure there is a current Business Associate Agreement with the non-HIPAA workforce member.

Transmission of ePHI or other sensitive information over an electronic communication network shall be encrypted. This does not include traditional facsimilie (Fax) transmissions.

Network personnel shall not open ports through any firewall without pre-approval from appropriate management or UA Information Security Office. Approved requests shall be documented.

Use of portable devices to store ePHI must be pre-approved by the covered entity's Privacy and Security Officer(s) and must be properly secured with proper physical and software controls in accord with the HIPAA Security Core Policy, "Use of Portable Devices."

All requests for phone lines shall be approved by UA Telecommunications.

Any external access to a UA network containing ePHI (i.e., VPN) or internal access to outside networks (i.e., DSL lines) that bypasses the UA firewalls shall be approved by the covered entity's Privacy and Security Officer(s).

Access for non-UA personnel must be uniquely identifiable and submitted in writing to the covered entity's Privacy and Security Officer(s) prior to receiving access. The written request for access shall describe the reason and duration of the need (to include an anticipated termination date). This written request must describe the nature of access, reference the Business Associate Agreement (BAA) if needed, contain sufficient information to identify potential risk, and meet the minimum necessary requirement. If granted, the access must be documented, noting the date when granted.

Requests for access to ePHI systems utilized for Institutional Review Board-approved research shall be reviewed against the above established criteria on a case by case basis.

All networks containing ePHI shall utilize measures to prevent unauthorized devices from connecting to the network.

**User Responsibilities**

Shall follow UA and their department's system security procedures, i.e., security patches, anti-malware protection, anti-spam protection. Exceptions shall be approved by the covered entity's Privacy and Security Officer(s).

Shall not implement systems that function as a bridge between UA HIPAA network containing ePHI/sensitive information and an external network, i.e., split tunneling.

Shall log off applications containing ePHI/sensitive information when not in use. Also, shall lock the computer screen or log off windows when not in use.

Shall not share their access codes or passwords with other individuals.

Shall not perform unauthorized scanning on a UA network. Scanning activities must be pre-approved by the covered entity's Privacy and Security Officer(s). Examples include but are not limited to Nmap scans, Nessus assessments, port scans, phone sweeps, probing tools, and other similar scanning activities.

Shall not attempt unauthorized or inappropriate access to any UA system including those containing ePHI or other sensitive information.

Shall apply the same security policies and procedures as is required in the workplace when accessing UA resources containing ePHI regardless of the location (i.e., applying necessary access lists, software or network firewalls, access controls, etc., when at home or other off-site location).

**System Administrator Responsibilities**

Shall report unapproved portable devices to the covered entity's security officer.

Shall implement and maintain the latest security patches on the systems under their management.

Shall implement and maintain anti-malware software on the systems under their management.

Shall apply automatic logoff/lockout features for inactive user sessions (i.e., 15 minutes logoff in high volume/traffic areas as per industry best practices or local policy).

Shall use separate, unique user accounts to ensure individual accountability.

Shall establish user accounts and accounts with higher privilege, i.e., system administrator, supervisor, root, superuser, in a manner that ensures individual accountability.

Shall not establish group user accounts.

Shall grant minimum necessary and direct need-to-know access rights as applicable to the person's documented job function. The covered entity's Privacy and Security Officer(s) shall approve additional access rights.

Shall establish emergency access procedures for the systems they manage.

Shall keep and monitor logs in order to detect and document attempts to compromise accounts, password brute force, and other types of abuse.

**Manager/Supervisor Responsibilities**

Shall ensure users follow policies for use of portable devices in accord with the HIPAA Security Core Policy, "Use of Portable Devices".

Shall routinely monitor to ensure users are aware of and in compliance with the security policies including those addressing portable devices and home workstations.

Shall establish procedures in written or electronic form to comply with this policy and if action, activity, or assessment is required by this policy to be documented, maintain a written or electronic record of the action, activity, or assessment.

Shall ensure Business Associates are aware of and in compliance with all of the HIPAA and HITECH security requirements.

**Business Associates' Responsibilities**

All Business Associates shall be required to sign an approved Business Associate Agreement.

Business Associates must comply with UA policies and standards applicable to the nature of their work with UA.

**Remote Access**

Requests for remote access must be reviewed and approved. Security control used to safeguard sensitive information will be evaluated. Remote access accounts should be periodically reviewed. Examples of minimum-security controls include unique user ID, strong password, two-factor authentication, session timeout, and secure connection.

Remote users when accessing ePHI systems shall use a UA-approved Virtual Private Network (VPN) solution.

# Use of Portable Devices

**Background Information**

The use of mobile device and mobile device applications related to patient care must be approved by entity HIPAA Security and HIPAA Privacy Officer as well as the entity leadership.

There is a growing number of applications, both commercial and institutionally developed, that allow individuals to store, view, and interact with sensitive data on a portable device. This includes personal assistance such as Siri, Alexa, etc.  Many Federal regulations and guidelines require institutions to develop policies and protections to secure electronic information stored on or accessed from any computing device, including portable devices. This policy addresses this requirement when portable devices are used to access and/or store UA ePHI or other sensitive information. Such devices pose great risk to UA if not adequately safeguarded and appropriate handling techniques are not utilized. Therefore, any portable electronic device or storage mechanism that may contain ePHI or other sensitive information or interface with a system containing ePHI or other sensitive information, are subject to this policy.  Note that many portable/mobile devices utilize cloud storage services.

**User Responsibilities**

All ePHI or other sensitive information must be stored in secure server environments only, as in a directory on a secure network file server. In addition, analysis and research work shall be conducted in the secure server environment. Storing ePHI or other sensitive information in any other environment requires documented permission from senior management.

No workforce member should copy or download ePHI or other sensitive information to a local hard drive, CD, DVD, flash drive, laptop, non UA approved cloud service or other storage device without documented prior approval from senior management.

Workforce member must disable personal assistant devices or applications such as Siri, Alexa, etc., to prevent unintended “listening” and “recording” of conversations that include discussions about health information unless required by approved mobile applications.

In the event prior approval has been granted for downloading ePHI or other sensitive information, workforce members shall be responsible for the protection from improper use or disclosure of all ePHI or other sensitive information contained on their portable device and personal computer.

- Security of data maintained and stored on such devices is subject to the provisions of relevant local, state, and federal statutes and regulations, including the provisions of the UA HIPAA core policies and other UA policies.

Workforce members shall not use personally owned portable devices for work related purposes unless such use is specifically approved by senior management. If use of a personal portable device is approved by senior management, then the device must comply with all applicable policies and standards and must be made available to UA for routine or special analyses. In addition, the device must be set-up in English.

In the event senior management authorizes the use of a portable device for the transfer or use of ePHI or other sensitive information, the device must be purchased by UA or receive approval from the covered entity’s Privacy and Security Officer(s)prior to operation.

ePHI or other sensitive information stored on portable devices shall be protected from unauthorized access in accordance with applicable UA policies through the use of effective and necessary approved measures. These shall include, but are not limited to, the following:

- **Password protection** using approved strong password techniques.
    - Portable devices such as cell phones and portable storage that support the clearing of memory/storage after a number of failed login attempts shall erase their contents after a minimal of 10 failed login attempts.
    - BIOS and/or boot passwords shall be used for all portable devices incapable of meeting password complexity.
- **Encryption software** shall be approved by UA’s Information Security Office.
- **Up-to-date antivirus/anti-malware software** shall be installed and maintained with frequent updates to detect and prevent malicious software.
- **Appropriate hardware or software firewall protection** shall be utilized if the portable device containing sensitive information is connected to the Internet via an “always on” broadband connection.

If ePHI or other sensitive information is uploaded from the portable device to a computer, the workforce member shall be responsible for safeguarding such ePHI or other sensitive information on that computer in accordance with all applicable policies and procedures including the UA HIPAA core policies and the requirements of the HIPAA security rule.

Use of portable devices shall employ approved UA VPN technology when establishing connection to the UA HIPAA network via public networks.

Portable devices accessing wireless networks must meet the following criteria:

- Portable devices must use encryption for secure information transfers.
- Portable devices using only WEP encryption technology will not be approved for the transfer of ePHI or other sensitive information.
- Portable devices using publicly accessible wireless infrastructures and accessing ePHI or other sensitive information shall employ two factor authentication as defined in the HIPAA Guidance for Remote Access and in accordance with UA practices.

Sanctioned use of email on portable devices is only approved if the device employs UA mobile device management software and configurations. Access to email systems in any other method is prohibited.

- Portable devices storing email locally within the device shall have mechanisms that encrypt the email stored on the device, encryption of the email during transport, and the ability to erase the device after a number of failed login attempts.

Portable devices using a browser or other software for Internet access/activity shall follow UA policies and standards for securing the browser and appropriate use policies.

Portable devices shall be backed up on a routine basis. The workforce member shall work with the appropriate IT department to maintain these backups in conformance with UA, and HIPAA policies and standards. Workforce members shall not backup or synchronize devices on public workstations, servers, or home computers (including laptops).

Prior to disposal or transfer to a new owner, all ePHI and other sensitive information on that device must be destroyed. See the UA HIPAA core security policy, "Media Allocation and Disposal."

Portable devices shall not be shared among family members or outside parties.

Removal of portable device hardware and electronic media from a UA facility shall follow the guidelines below:

- Workforce members shall not remove from a UA facility any hardware or electronic media containing ePHI or other sensitive information (portable device), nor download ePHI or other sensitive information to any computer, device, or network that is not located in a UA facility without documented senior management approval.
- Workforce members shall promptly (within 2 hours of the discovery of the loss) report the loss or theft of any portable device, hardware, electronic media, or any ePHI or other sensitive information data stored on the portable device or electronic media to their appropriate supervisor, UA Police, the covered entity HIPAA Privacy and Security Officers, and the UA Information Security Officer.

**System Administrator Responsibilities**

Final Disposal of Electronic sensitive information.

- System Administrators shall ensure that ePHI or other sensitive information subject to final disposition is disposed of by using a method that ensures the ePHI or other sensitive information

cannot be recovered or reconstructed. See the UA HIPAA security core standard regarding media disposal and reallocation.

- System Administrators shall maintain a log of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general description of the ePHI or other sensitive information (if available), and the identity of the workforce personnel performing the destruction.
- System Administrators shall provide assistance in backing up portable devices according to applicable UA, and UA HIPAA core policies and standards. Backups should not be made from a portable device to another portable device as the sole backup. Backups shall (at a minimum) be made to a secure server environment.
- System administrators shall report to the covered entity HIPAA Security Officer (within 2 hours) the loss or theft of any portable device containing or possibly containing ePHI or other sensitive information.
- Devices containing hard drives shall use UA approved encryption technologies.
- Disposal of the portable device containing a hard drive shall follow UA policies.

**Covered Entity Senior Management Responsibilities**

Senior management, as defined by each covered entity, shall maintain the following information when granting approval of a workforce member's ability to copy or download ePHI or other sensitive information to a local hard drive, CD, DVD, flash drive, laptop, non UA approved cloud service or other storage device:

- Date of request.
- Purpose of and rationale for request.
- Date of approval.
- Name of workforce member.
- Type of device.
- Date to reevaluate need of ePHI or other sensitive information.
- Date ePHI or other sensitive information on device removed/destroyed.
- Tracking information of device.
- Data sources being utilized on device.
- Date device is expected back or to be reviewed by responsible IT department.

If senior management consents to allowing contractors, business associates, or workforce members under contract to copy, download, or remove UA ePHI or other sensitive information to any portable device, then senior management shall record the following minimal information about the approval:

- Date of request.
- Purpose of and rationale for request.
- Date of approval.
- Name of workforce member, contractor, or business associate.
- Type of device.
- Date to reevaluate need of ePHI or other sensitive information.
- Date ePHI or other sensitive information on device removed/destroyed.
- Tracking information of device.
- Data sources being utilized on device.
- Confirm appropriate contract language and Business Associate Agreements are properly executed.
- Confirm appropriate confidentiality agreements and policy acknowledgements are properly executed and copies are retained within the department.
- Document safeguards present on the device.

**Contractor, Business Associates, and Other Temporary/Contract Workforce Members Responsibilities**

Contractors, business associates, or workforce members under contract may not copy, download, or remove UA ePHI or other sensitive information to any portable device or non UA approved cloud service without documented consent from the appropriate UA senior management. In the event UA senior management consents to allow a contractor or business associate to use ePHI or other sensitive information on a portable device, the consenting party is responsible for the tracking, retrieval, and removal of the ePHI or other sensitive information materials and conformance to the policy statements in this policy.

Contractors, associates, and workforce members under contract shall employ safeguards equivalent to UA safeguards prior to removal of any material.

Contractors and associates shall not share ePHI or other sensitive information with other parties or internal to their company without written approval from UA.

This policy applies to workforce members within this class as it does to all UA employees.

# Media Reallocation and Disposal

**Reallocation**

Media containing PHI/ePHI may only be dropped off in designated, secured containers or directly to a member of the Information  covered entity's Privacy and Security Officer(s) or UA Information Security Team.

Media containing PHI/ePHI information shall not be placed in trash receptacles.

**Storage**

ePHI shall be stored on media that is approved by the covered entity's Privacy and Security Officer(s) or the HIPAA Privacy and Security Officer, which includes, but is not limited to, computers and electronic storage systems owned and leased/contracted by the organization. Exceptions to this may be approved by submitting a risk assessment request via email: riskassessments@ua.edu.

Media PHI/ePHI information shall be stored in a secure location prior to sanitization and/or disposal.

**Sanitization**

Media containing ePHI shall be sanitized prior to being reallocated, transferred, or disposed of.

Approved sanitization methods are included in NIST Special Publication 800-88.

Media containing ePHI shall be sanitized by authorized personnel approved by the covered entity's Privacy and Security Officer(s) or the UA HIPAA Security Officer

**Disposal**

Vendors shall be used for the disposal of media. Please contact the covered entity's Privacy and Security Officer(s) or the UA Information Security Team for a list of authorized vendors.

Vendors shall not remove any PHI/ePHI without a contractual agreement in place.

Service providers who host ePHI must provide a way of destroying the data as requested by UA or upon termination of the relationship.

**Enforcement**

Employees or vendors shall report policy violations to the appropriate Information Security Team.

Requesting or performing reallocation or disposal activities in an effort to eliminate evidence that may incriminate UA or staff in civil or criminal litigation is strictly prohibited.

# Information Privacy and Security Incident Response

HIPAA Security Officer shall maintain the UA Incident Response Plan.

HIPAA Security Officer shall periodically test the UA Incident Response Plan.

HIPAA Privacy Officer shall manage the UA HIPAA Compliance Privacy Complaint, Incident Response and Breach Notification Procedure.

HIPAA Privacy Officer shall maintain the incident log and incident details and outcomes related to the UA HIPAA Compliance Privacy Complaint, Incident Response and Breach Notification Procedure for a period of no less than six years.

Covered entities shall coordinate response efforts under the direction of an Incident Response Team (IRT) as defined by the UA Incident Response Plan.

All Workforce Members shall report suspected privacy and information security incidents.

All Workforce Members shall cooperate with incident response investigations and resolutions.

Management shall ensure workforce members are trained in incident response procedures appropriate for their roles.

Covered Entity Privacy Officer shall:

- Serve as covered entity's primary privacy resource,
- Follow information privacy incident procedures,
- Investigate information privacy incidents,
- Request audit trails,
- Contact the proper areas regarding incidents,
- Complete incident reports and distribute to appropriate parties,
- Document and distribute the privacy incident resolutions within a timely manner, and
- Track privacy incidents via the Request Tracking Spreadsheet.

Covered Entity Security Officer shall:

- Serve as covered entity's primary security contact and information resource.
- Follow information security incident procedures.
- Aid or assist in the investigation of information security incidents.
- Immediately contact the UA HIPAA Security Officer if an incident is suspected.
- Assist in the completion of incident reports and distribute to the appropriate parties.

# Contingency Planning

A contingency/disaster recovery plan shall be developed and published for every in-scope system used in each operational area.

- The operational area shall develop downtime procedures in conjunction with other departments that maintain information systems
- The procedures shall address both short-term and long-term downtime events.
- The procedures shall be given to the Covered Entity Security Officer for inclusion in the covered entity's contingency plan.
- The procedure shall be reviewed periodically and updated as business practices change within the operational area.

All system users shall be trained on downtime procedures so that they know how to respond appropriately and in a timely manner in the event of actual downtime. NOTE: Downtime procedures should be reviewed before a downtime is experienced.

All downtime procedures shall be published and available within the individual covered entity.

The covered entity contingency plan shall be reviewed by the appropriate management periodically and whenever significant system changes are implemented

All downtime procedures shall be tested for accuracy and ease-of-use prior to publication and annually.

All downtime procedure tests shall be documented.

All downtime procedures shall be reviewed and approved by the affected management prior to publication.

Systems containing sensitive data shall be backed up at least once per business day. Backup media should be encrypted where possible and securely stored (onsite or offsite) at all times. The backup shall contain the sensitive data and all necessary software required to process the data.

- Full backups to support business operations and recovery shall be maintained at all times.
- A restoration procedure must be able to restore the system to a state as specified by the recovery objectives.

At least three copies of a covered entity's contingency/disaster plan will be kept, one in each of the following locations:

- Secure offsite storage
- Covered Entity Security Officer's office
- UA HIPAA Information Security Office

UA HIPAA Information Security Office Responsibilities

- Verify that covered entities have proper contingency plans.
- Collect and store contingency plans from covered entities.
- Verify that contingency plans are tested and revised as needed.
- Provide annual reports to the HIPAA Advisory Committee regarding HIPAA contingency plan compliance.

**User Responsibilities**

During contingency operations, do not store sensitive information on a workstation. Use a secure network file server..

**System Administrator Responsibilities**

Document vendor contacts (with approved BAA), system configuration, backup procedures, and restoration procedures including required hardware and software for inclusion in the covered entity's contingency plan

Provide documentation to management on any system backup failure, i.e. a backup process failed due to broken tape.

**Management Responsibilities**

Ensure that users are trained on downtime procedures.

Ensure that contingency plan is tested and reviewed as needed.

Ensure that the contingency plan is updated as business procedures change or following an activation of the contingency plan.

Provide mechanisms for secure backup of non-electronic forms and data.

Ensure creation, maintenance, and adherence to core policies and procedures including:

- Emergency contact lists that include managers and system administrators
- Critical system inventory and configuration
- Vendor contact lists (i.e. hardware, software, forms, supplies)
- Alternative working procedures for all critical business functions
- Backup procedures
- Restoration procedures
- Recovery procedures
- Testing procedures
- Revision procedures.

Ensure that all published procedures, test results, and other documentary evidence shall be archived for no less than six years.

**Entity Security Officer Responsibilities**

Maintain the covered entity contingency plan including:

- Emergency contact lists that include managers and system administrators
- Critical system inventory and configuration
- Vendor contact lists (i.e. hardware, software, forms, supplies)
- Alternative working procedures for all critical business functions
- Backup procedures
- Restoration procedures
- Recovery procedures
- Testing procedures
- Revision procedures.

Collect updates to the covered entity contingency plan from covered entity system administrators.

Ensure that recovery time and contingency plan are reviewed and approved by the affected management. Note that contingency planning may cross standard departmental boundaries.

Periodically test the contingency plan, including contacting vendors, to ensure replacement system availability.

Provide the UA HIPAA Information Security Office with an updated covered entity contingency plan if/when revised.

All business associates shall be required to sign a business associate agreement.

## References:

National Institute of Standards & Technology (NIST) Special Publication 800-88, "Guidelines for Media Sanitization."

National Institute of Standards & Technology (NIST) Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations."

45 CFR Parts 160 and 164 HIPAA Administrative Simplification: Enforcement; Final Rule

The University of Alabama Core HIPAA Policy

The University of Alabama Incident Response Plan

## Contacts:

For questions regarding the requirements, implementation, and enforcement of this policy, contact one of the following:

Your departmental HIPAA Covered Entity Security Officer

The OIT Help Desk at 205-348-5555 or itsd@ua.edu

UA HIPAA Privacy Office

UA HIPAA Security Office

UA IT Information Security Office at 205-348-5610 or security@ua.edu

## Scope:

These procedures apply to UA Designated Health Care Components, UA departments serving as Business Associates for non-UA covered entities, covered health plans of The University of Alabama (a Covered Hybrid Entity) and to the administrative departments at The University of Alabama that provide legal, billing, auditing, or other administrative support for the above, including but not limited to The University of Alabama Office of Counsel, The University of Alabama System auditors, the University's HIPAA Privacy and Security Officers, Office of Information Technology, Human Resources, and Risk Management.

For purposes of these procedures, these UA entities and their affiliated administrative support departments shall be referred to as "covered entity or entities" Compliance with these procedures is required by all employees, volunteers, physicians, residents, interns, trainees, contracted individuals, and other persons who work for a covered entity or is under the direct control of a covered entity, whether or not they are paid by the covered entity.

These procedures do not apply to, but provide a sound security foundation: Psychology Clinic, Student Health Center/Pharmacy, ODS records, Counseling Center, WGRC, Athletic Department health records

## Definitions:

**Account Administrator**: Individuals who are charged with adding, disabling, and modifying access granted to users and other types of accounts such as service accounts.

**Entity Security Officer (SO):** The covered entity's SO who acts in conjunction with the UA HIPAA Security Office for UA.

**Authentication mechanism:** Items including, but not limited to, passwords, tokens, biometrics, and smart cards used for confirming a user's identity.

**Backup procedure**: A detailed step-by-step method for saving data and, if appropriate storing it securely offsite that includes hardware, software, and configuration information.

**Business Associate (BA)**: A person or entity (other than an employee of a UA Covered Entity) who performs a function or activity involving the use or disclosure of protected health information, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, for or on behalf of a UA Covered Entity. A Business Associate of one UA Covered Entity does not become a Business Associate of any other UA Covered Entity simply by virtue of the UA Affiliation.

**Business Associate Agreement (BAA)**: A legal agreement between UA and the Business Associate that outlines how the Business Associate will protect the ePHI that they store, process, or transmit on behalf of UA. This is an additional document separate from the contract.

**Cloud Service Provider:** Off campus hosted services that provide storage of data such as Box, One Drive, Google Docs, etc. Also includes cloud hosting and storage services such as Azure, Amazon Web Services (AWS), etc. Use of cloud storage for ePHI requires a BAA with the cloud provider.

**Contingency plan**: A set of strategies that coordinates processes and procedures for the recovery of information systems containing ePHI or other sensitive information following an emergency or disruptive event.

**Direct Need-to-Know:** Those persons or classes of persons, as appropriate who need access to specific protected health information to carry out their work-related duties.

**Disaster recovery plan**: The combination of a recovery procedure and a restoration procedure.

**Disposal**: The permanent destruction of media.

**Downtime procedure**: A detailed step-by-step workflow description that ensures continuity of the business and the security of data for use in a recovery procedure. This is equivalent to an emergency mode operation plan.

**Electronic Communication Network:** This includes things such as the Internet, wireless, or wired network.

**Electronic Protected Health Information (ePHI or electronic PHI)**: Health information, including demographic information, collected from an individual and created or received by a health provider, health plan, employer, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual, and that is created, maintained, received or transmited in any electronic format or media.

The following identifiers of an individual or of relatives, employers, or household members of the individual, are considered PHI:

1. Name
2. Geographic subdivisions smaller than a state; (street address, city, county, precinct, zip code, and equivalent geocodes)
3. All elements of dates (except year) including birth date, admission and discharge dates, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age
4. Telephone numbers
5. Fax numbers
6. Electronic mail address
7. Social security number
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/License numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locator (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code, except as allowed under the re-identification specifications (164.514(c)).

**Email**: The electronic transmission of information through a mail protocol such as SMTP, POP, or IMAP.

**HIPAA Security Officer:** A designated individual responsible for HIPAA related information security issues.

**HIPAA:** Health Insurance Portability and Accountability Act.

**Information security incident:** Any event or series of events that violates or threatens to violate information security policies, confidentiality, integrity, or availability related to a system or systems within the UA infrastructure.

**Long-term downtime**: Any downtime greater than anticipated system recovery time.

**Malicious code:** Any program that is intended to circumvent security measures, destroy data, collect data for unauthorized third parties, or propagate data onto another system, i.e., exploits, viruses, worms, spyware.

**Media/Portable Storage**: Include, but are not limited to, removable or external hard disk drives, DVDs, CDs, flash drives, pen drives, USB drives, tapes, and other portable storage devices capable of acting as a transport agent for digital information.

**Minimum Necessary**: To make reasonable efforts to limit the use or disclosure of, and requests for, ePHI to the minimum necessary to accomplish the intended purpose.

**Mobile Device/Portable Devices:** Include, but are not limited to, hand held devices, pen pads, cell phones, smart phones, iPhones, Android devices, iPads, portable workstations on wheels and carts, biomedical devices that collect patient information or provide life support and medical treatment, and pagers that store data. Portable devices are battery operated (though they may support direct connection to utility power), freestanding devices used for the purposes of data storage, retrieval, analysis, and exchange. Such devices may interact with other networked systems, the Internet, desktop personal computers via some form of interconnection and/or synchronization process.

**Privacy incident:** Suspected breaches of confidentiality of PHI.

**Reallocate**: The assignment of media from one party within UA to another party within UA.

**Recovery procedure**: A detailed step-by-step method for recovering data or transactions that occur during a system downtime.

**Recovery time**: The amount of time that it takes to restore information systems to normal operations following a disaster. This includes the amount of time it would take for vendors to replace hardware, installation time, restoration from backup, and the implementation of the recovery procedure.

**Remote Access:** Users outside of a covered entity's network accessing data on the covered entity's network.

**Restoration procedure**: A detailed step-by-step method for recovering a system from backup media. It shall also include details on necessary hardware, software, licensing keys, and system information.

**Risk Analysis:** An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by a UA covered entity.

**Risk Management:** The implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

- Ensure the confidentiality, integrity, and availability of all ePHI the UA covered entity creates, maintains, receives, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the HIPAA Privacy Rules;
- Ensure compliance with the HIPAA Security Rule and HITECH Act; and
  Ensure Meaningful Use requirements are met.

**Risk:** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact on confidentiality, integrity and availability of confidential information.

**Secure Location:** Any area or place with restricted and monitored physical access through card key or physical lock.

**Secure offsite location**: A physically and environmentally safe storage area that is separated from where the originating information systems reside.

**Senior Management:** Persons in the positions of dean, chair, or division or program director, or persons specifically designated by a dean, chair, or division or program director, that make executive decisions and are authorized to accept risks for the administrative unit in the area of information security.

**Sensitive Information or Data**: Data that should be kept confidential. Access to these data shall require authorization and legitimate need-to-know. It includes Protected Health Information, financial information, personnel data, trade secrets, and any information that is deemed confidential or that would negatively affect UA if inappropriately handled.

**Separation**: The cessation of an individual's authority to occupy any role and perform any responsibilities on behalf of UA. This may occur through the resignation of personnel, the dismissal of personnel or the termination of contractual agreements.

**Short-term downtime**: Any downtime less than the anticipated system recovery time.

**Strong passwords**: Current industry best practices identify this as a minimum of eight alphanumeric characters with at least one upper case and one special character.

**Transfer:** To transmit media (internally or externally in compliance with HIPAA or other applicable regulatory guidance) and the data contained therein from one party to another party that has the appropriate authorization to access and maintain the data.

**User account**: An established relationship between a user and a computer network, service, or application. User accounts are assigned a user ID and are uniquely identifiable and traceable to one user or entity.

**User Account:** Information used by a user to gain access to UA ePHI resources. This includes, but is not limited to, user IDs, passwords, personal identification numbers (PIN), tokens, certificates, biometrics, and smart cards.

**User ID**: An individual ID used to identify a unique individual when logging into an information resource such as a computer, network, service, or application. synonymous with sign-on code.

**User:** Any individual who accesses UA electronic protected health information assets.

**Workforce members:** Any individual (physician, resident, employee, student, volunteer, contracted employee, visiting faculty, or clinical or research fellow) who accesses UA electronic protected health information or is considered a UA workforce member within the federal HIPAA regulations.

## Approved by:

The University of Alabama HIPAA Compliance Committee