UADA Policy 915.3
Division Data Protection:
PHI Security and Clean Desk Policy and Procedure

Purpose

The University of Arkansas System, Division of Agriculture (UADA) policies regarding privacy and security of protected health information (PHI) reflect its commitment to protecting the confidentiality of employee's medical records or information from management information systems, confidential conversations, and any other sensitive material as a result of doing business. While a commitment to the privacy and security of PHI is an expectation, there remains a possibility that an inappropriate or unintended disclosure of PHI may result in a privacy breach. This policy will determine the procedure to mitigate all breaches, both willful violations and unintended actions, consistent with the guidance described by the HIPAA rules.

Scope

This policy applies to all members of the UADA workforce:

- Employees (including faculty and staff)
- Volunteers
- Students and Residents
- Extra Help workers
- Contingent workers

Policy

PHI is confidential and must be treated with respect and care by anyone with access to this information. As an employer, UADA is entrusted with demographic, financial, and clinical information regarding our employees. Any violation or breach of confidentiality by workforce members is subject to formal discipline up to and including termination, as outlined in this policy. The organization's personnel shall observe policy guidelines and sanctions applied fairly and consistently to all individuals violating the policies.

This policy covers the following:

- Definition of breach
- Required reporting process for breaches
- Investigation process followed
- Disciplinary sanctions and appeals
- UADA's duty to mitigate damages created by breaches
- Documentation requirements of these processes
- Other Examples

Breach Defined:

A "breach" is the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, which compromises the security or privacy of that information.

There are three exceptions to the definition of "breach."

- Unintentional acquisition or use in good faith within the course and scope of employment by someone authorized to access PHI, and the information is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA Privacy rule, or
- Inadvertent disclosure by an authorized person to another authorized person within the same Covered Entity or Business Associate, and the information is not further used or disclosed in a way that is inconsistent with the requirements of the HIPAA Privacy rule, or
- A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person who receives the information would not reasonably have been able to retain such information.

Examples of a breach (this is not an all-inclusive list):

- Authorized user accesses an employee's information without a functional "need to know"
- Release of employee information to an outside party for any unauthorized purpose – examples may include releases to the media, to relatives or friends of an employee, or sale of PHI
- Electronic hacking or theft of employee files or database
- "Dumpster diving" to find PHI
- Unauthorized user using another authorized person's ID/password to access employee information
- Unauthorized access to PHI, paper or electronic, that is neither protected by encryption nor properly destroyed.

Under the Department of Health and Human Services Final Breach Rule, an acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA's Privacy Rule is presumed to be a breach unless UADA demonstrates that there is a "low probability that the protected health information has been compromised."

Initial Reporting Responsibilities:

1. Anyone who is aware of or suspects a violation of privacy/security policy or a breach of employee information is required to report it immediately to:
    - Chief Financial Officer
    - Chief Human Resources Officer
    - Chief Information Officer

2. Once the initial report is made, others should be informed, including:
    - Immediate supervisor
    - Department Head or Manager of the area in which the individual works
    - Senior Associate VP

3. Bad Faith Reports: Reporting a violation or breach of bad faith or for malicious reasons may be interpreted as a misuse of the reporting mechanism(s) and may result in disciplinary action.

Investigations of Reporting Breaches:

1. The appropriate officials will assess all reported violations.
2. When applicable, the Incident Response Team (IRT) will invoke the Information Technology Security: Incident Response Procedures which outlines the necessary steps to take if any confidential or restricted data is compromised.
    - This protocol includes assembling key personnel to perform a full assessment of the compromise of the PHI.
    - If the PHI in question is not indecipherable, unreadable, or unusable and falls into unauthorized hands, UADA will determine through a risk assessment whether there was a low probability that the protected health information had been compromised.
    - Outcomes of the analysis are documented and acted upon accordingly, as outlined in the Information Technology Security: Incident Response Procedures.

3. Information about investigations of breaches will only be shared with those who need to know. Confidentiality of all participants in the reported situation shall be maintained to the extent reasonably possible throughout any resulting investigation. The investigator(s) will conduct the necessary and appropriate investigation commensurate with the level of the breach and the specific facts. This investigation may include, but is not limited to, interviewing the individuals involved, interviewing other individuals, obtaining specific facts surrounding the violation/breach, and reviewing pertinent documentation.

Disciplinary Sanctions and Appeals:

1. When a violation/breach is verified, existing UADA procedures for disciplinary action shall be utilized.
2. Sanctions may include, but are not limited to:
   - Verbal Warning
   - Written Warning
   - Suspension
   - Termination
3. Disciplinary sanctions and appeals are handled per applicable UADA procedures, depending on the type of workforce member being disciplined.
4. If the individual responsible for the violation/breach is a contractor, UADA will take reasonable corrective steps to implement sanctions. While UADA is not required to monitor the activity of our contractors, we will address problems as we become aware of them and request that our contractors remedy their behavior. UADA reserves the right to terminate contracts if it becomes clear that the contractor cannot be relied upon to maintain the privacy/security of the information we provide.

Duty to Mitigate Valid Breaches:

1. UADA will mitigate, to a practical extent, harmful or injurious effects of unauthorized access, use, or disclosure of all forms of protected health information (paper, electronic, or oral). The appropriate officials or the Data Security Team make recommendations to the appropriate department manager/administrator for corrective action.
2. The manager of the area responsible for the breach is required to develop and implement a corrective action plan to address valid breaches.

Reporting and Tracking of Breaches:

1. UADA officials will contact state agencies, law enforcement, regulatory, accreditation, and licensure bodies as necessary to report and mitigate policy and or law violations properly.
2. A summary of reported privacy and/or security breaches is prepared by the Privacy Office and/or Security Office at least once per year and reported to upper management.
3. All information documenting the process required under HIPAA Privacy and Security regarding the violation or breach will be retained for a period of six years by Human Resources.

Other Examples of Privacy and Security Incidents:

Other examples of violations of privacy and security of PHI are included below. (This is not an all-inclusive list):

- Individuals discussing employee information in public areas where those who do not need to know the information can overhear.
- Individual leaves a paper copy of any employee medical information in a public area.
- Unauthorized access to medical records areas and medical records.
- Individual leaves a computer unattended in a publicly accessible area with medical record information unsecured.
- Failure to log off the computer.
- For purposes unrelated to job duties:
  - An individual improperly acquires, accesses, uses, reviews, and/or discloses records of any employee or requests another individual to do so.

    - An individual acquires, accesses, reviews, and/or discloses an employee's record with the intent of giving or selling information outside of UADA.
    - An individual improperly acquires, accesses, uses, reviews, and/or discloses the confidential information of another member of the UADA workforce.
- Stealing or sharing passwords or not reporting a known lost password.
- Introduction of viruses, worms, Trojan horses, or other malicious software into the organization's computer systems.
- Unauthorized access to networks, computer systems, or facilities/equipment rooms housing the computer systems.
- Unauthorized destruction/changing of PHI.
- Improperly discarding PHI (not physically destroying it), whether paper or electronic media.
- Loss or theft of any Mobile Computing Device with PHI that is discoverable and not properly protected/encrypted.

Related Links

Data Lifecycle and Management Policy-Procedures (UADA)
Information Technology Security: Incident Response Policy
Information Technology Security: Incident Response Procedure
Information Technology Security: Incident Escalation Guideline

---

Clean Desk and Clear Screen Policy (UADA)

Purpose

The purpose of a Sensitive Data Clean Desk and Clear Screen policy is to establish a culture of security and trust for employees at the University of Arkansas System, Division of Agriculture (UADA). An effective clean desk and clear screen effort involving the participation and support of UADA employees can greatly protect paper and electronic documents containing sensitive data about our employees, donors, alumni, parents, volunteers, and stakeholders. All employees that handle sensitive data should familiarize themselves with the guidelines of this policy.

Scope

This policy applies to all UADA employees that handle sensitive data. This policy covers any papers, screen displays, removable storage media, and any computing devices that contain or display UADA sensitive data, regardless of location.

Policy

When away from your desks, such as during lunch breaks or meetings, working papers containing sensitive data should be placed in locked drawers or a locked office, and screen displays should be placed in a locked screen state.

At the end of the working day, an employee should tidy his or her desk and put away all office papers that contain sensitive data, secure all screens, and lock his or her office. UADA provides locking desks and filing cabinets for this purpose.

Actions

- Allocate time in your calendar to clear away your sensitive data paperwork.
- Always clear your workspace of sensitive data paperwork before leaving for long periods of time.
- Whenever unattended or not in use, all computing devices that can be used to display sensitive data must be logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism, (devices include laptops, tablets, smartphones, and desktops).
- Paper containing sensitive data must be removed from printers and faxes immediately. Faxes and printers used to print sensitive data should not be in public areas. Any time a document containing sensitive data is being printed the user must make sure they know the proper printer is chosen and go directly to the printer to retrieve the document.
- If in doubt, check with your supervisor. If you are unsure of whether a duplicate piece of sensitive data documentation should be kept or even produced, discuss it with your supervisor before shredding.
- Sensitive data on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled at a later time and must be secured until the time that they can be shredded.
- Destroy sensitive data documents when they are no longer needed through crosscut shredders or locked shredder boxes.
- Lock your office, desk, and filing cabinets that contain sensitive data at the end of the day. Don't keep the keys in the lock or drawer.
- Portable computing devices such as laptops, smartphones and tablets that can be used to display sensitive data should be secured in a locked office or cabinet at the end of the day.

Reference Documents

UADA 910.1 - Division Acceptable Use Policy

Accountability

The Chief Information Officer for UADA is charged with the responsibility to review the policy and propose changes as needed periodically.