THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: AU-001-Auditing & Logging Accountability	
Version 3	**Effective Date: 06/17/2020**

Responsible Office: Office of Cybersecurity	Last Review: 01/11/2023 Next Review: 01/11/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The University of Tennessee Health and Science Center (UTHSC) ITS office and Office of Cybersecurity must establish a comprehensive level of security controls through an audit and accountability policy and standards. This document establishes the UTHSC 's Audit and Accountability standard which enables the management of risks and provides guidelines for security best practices regarding audit record retention.

Scope

The scope of this standard applies to all colleges within UTHSC, all business owners or designees that may include internal staff, contractors, and vendors, temporary personnel, third party providers under contract with a UTHSC, and other entities that interact with UTHSC information related resources. This standard covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the UTHSC to request exceptions to this standard.

UTHSC coordinates with third-party organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with UTHSC are subject to follow requirements outlined within this standard.

Compliance

As the official guidance domain for this standard, UTHSC colleges and business departments abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within federal organizations such as the Department of Health & Human Services (HHS), Centers for Medicare & Medicaid Services (CMS), Internal Revenue Service (IRS), and Social Security Administration (SSA).

Definitions

Audit Log Failure: Defined by UTHSC as events defined by federal and state guidelines in which logs being captured show issues or errors. Audit log failures can include but are not limited to software/hardware errors, failures in the audit capturing mechanisms, audit storage capacity being reached or exceeded, location of access, and severity of captured information.

Auditable Events: Defined by UTHSC as events defined by federal, state, and UTHSC guidelines, requiring audit and retained for the defined period. Auditable events can include but are not limited to the number of failed system log-on attempts, password changes, system errors, printing, changes, updates, deletions to the system, and application errors.

Level 3 Data: The security level needed for data defined by UTHSC Standards whose unauthorized disclosure could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UTHSC students, patients, research subjects, employees, guests/program participants, UTHSC reputation, or the overall operation of the Location or essential services. This classification level also includes lower risk items that, when combined, represent increased risk. per GP-002-Data & System Classification. Minimum security requirements are explained on the webpage https://uthsc.edu/its/cybersecurity/requirements.php.

Coordinated Universal Time (UTC): Defined by UTHSC as the time standard commonly used across the world, basis for civil time today. Unlike GMT, UTC is the world time standard and is not a time zone. This 24-hour time standard is kept using highly precise atomic clocks combined with Earth's rotation.

Electronic Protected Health Information (ePHI): Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Identifiable protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g.

Third Party: Defined by UTHSC as any contracted or government organization that is not a part of the UTHSC's organizational structure. This may include state or federal auditing agencies, approved security contract vendors or other external organization whose capabilities can be determined sufficient to conduct assessment needs.

Vendor Staff/Personnel: Defined by UTHSC as an employee contracted through an approved agreement, or other formal agreement, to provide temporary work for UTHSC.

Responsibilities

Chief Information Security Officer (CISO) is responsible for providing strategy and direction for assessment, planning, and implementation of all security standards, practices, and ensuring compliance to same.

Chief Privacy Officer (CPO) is responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the University's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual ensures compliance with HIPAA notification and reporting requirements in the event of an identified breach.

HIPAA Security Officer conducts Health Insurance Portability and Accountability Act (HIPAA) risk assessments.

Security/Privacy Lead - Individuals are designated by the campus/business area leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of all sensitive information under their assigned control.

UTHSC Contract, State, and Vendor Staff/Personnel All UTHSC contract, state, and vendor staff/personnel must adhere to this procedure. All staff/personnel must comply.

System Data Owner and System Data Administrators Management/lead who works with the application's development team, to document components that are not included in the base server build and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

Standard

Auditable Events UTHSC Office of Cybersecurity or designee will ensure that the information system or components are capable of auditing events defined by federal and state regulations. The office designee will coordinate security functions and controls with other organizational entities to ensure required auditable events or related data are being captured. UTHSC shall follow the UTHSC Audit and Accountability Procedure for additional information on audit logs, events, and more.

Content of Auditable Events The information system will generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit Storage Capacity UTHSC ITS will allocate audit storage capacity in accordance with all federal and state regulations and guidance.
Response to Audit Processing Failures The information system and/or its components will alert designated personnel in the event of an audit log failure where appropriate action is taken.

Audit Review, Analysis, and Reporting UTHSC Office of Cybersecurity will work with System Data Owners, or delegate(s), who receive and analyze audits and reports, per UT Policy, UTHSC standards, or as directed by federal and state regulations.

Findings of the reviewed information system audit records, and or issues, is reported to management.

Audit Reduction and Report Generation The information system provides an audit reduction report generation capability that supports functions for on demand audit review, analysis and reporting requirements, and after the fact investigation of security incidents. The information system will not alter the original content or time ordering of any audit records.

Time Stamps Information systems will use internal system clocks that can be mapped to Coordinated Universal Time (UTC) to generate time stamps. UTHSC will meet federal and state defined granularity of time measurements on audit logs.

Protection of Audit Information Audit information will be protected from unauthorized access, modifications, and deletions. The system will have compensating controls in place to prevent any unauthorized action to be taken on audit information.

Audit Record Retention The system will retain audit records to provide support for after action reviews, investigations of security incidents, and assisting troubleshooting measures. Retention requires shall meet all, UT, UTHSC, and state and federal regulatory retention requirements.

Audit Generation Auditable events will be generated by the information system. Security personnel or designee may have the ability to select which events are to be audited.

References

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
2. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
3. Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
4. Social Security Administration (SSA) Security Information

5. U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)
6. UTSA Policy IT0127 Audit and Accountability
7. GP-002-Data & System Classification