IS-8 AUDITING POLICY

**8.1** **Auditing Policy**

<COMPANY NAME> shall audit access and activity of electronic protected health information (ePHI) applications and systems in order to ensure compliance. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit activities may be limited by application, system, and/or network auditing capabilities and resources. <COMPANY NAME> shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

It is the policy of <COMPANY NAME> to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, <COMPANY NAME> shall audit access and activity to detect, report, and guard against:

* Network vulnerabilities and intrusions;
* Breaches in confidentiality and security of patient protected health information;
* Performance problems and flaws in applications;
* Improper alteration or destruction of ePHI;
* Out of date software and/or software known to have vulnerabilities.

This policy applies to all <COMPANY NAME> Add-on systems that store, transmit, or process ePHI.

**8.2 Auditing Policies**

1. Responsibility for auditing information system access and activity is assigned to <COMPANY NAME>'s Security Officer. The Security Officer shall:
	1. Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
	2. Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
	3. Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).
	4. All connections to <COMPANY NAME> are monitored. Access is limited to certain services, ports, and destinations. Exceptions to these rules, if created, are reviewed on an annual basis.
2. <COMPANY NAME>'s auditing processes shall address access and activity at the following levels listed below. In the case of Customer System Access, Customers, Application and User level auditing is the responsibility of the Customer; <COMPANY NAME> provides software to aggregate and view User and Application logs, but the log data collected is the responsibility of the Customer. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
	1. User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
	2. Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
	3. System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions. <COMPANY NAME> utilizes file system monitoring from <AUDIT TOOL NAME> to assure the integrity of file system data.
	4. Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.
3. <COMPANY NAME> shall log all incoming and outgoing traffic to into and out of its environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and other relevant details that are available to <COMPANY NAME>.
4. <COMPANY NAME> utilizes <TOOL NAME> to scan all systems for malicious and unauthorized software every 2 hours and at reboot of systems.
5. <COMPANY NAME> leverages process monitoring tools throughout its environment.
6. <COMPANY NAME> uses <TOOL NAME> to ensure the integrity of log files by centrally collecting and storing all logs.
7. <COMPANY NAME> shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. The "events" may be applied to the entire <COMPANY NAME> Platform or may be specific to a Customer, partner, business associate, Platform Add-on or application (See Listing of Potential Trigger Events below).
8. In addition to trigger events, <COMPANY NAME> utilizes log correlation functionality to proactively identify and enable alerts based on log data.
9. Logs are reviewed weekly by the Security Officer.
10. <COMPANY NAME>'s Security Officer and Privacy Officer are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:
	1. Scanning tools and devices;
	2. Password cracking utilities;
	3. Network "sniffers."
	4. Passive and active intrusion detection systems.
11. 12. The process for review of audit logs, trails, and reports shall include:
	1. Description of the activity as well as rationale for performing the audit.
	2. Identification of which <COMPANY NAME> workforce members will be responsible for review (workforce members shall not review audit logs that pertain to their own system activity).
	3. Frequency of the auditing process.
	4. Determination of significant events requiring further review and follow-up.
	5. Identification of appropriate reporting channels for audit results and required follow-up.
12. 13. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.
	1. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services - separation of duties).
	2. Testing shall be done on a routine basis, currently monthly.
13. 14. Software patches and updates will be applied to all systems in a timely manner.

**8.3 Audit Requests**

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, Security Officer, Customer, Partner, or an Application owner or application user.
2. A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by <COMPANY NAME>'s Privacy or Security Officer.
3. A request for an audit must be approved by <COMPANY NAME>'s Privacy Officer and/or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.
	1. Should the audit disclose that a workforce member has accessed ePHI inappropriately, the minimum necessary/least privileged information shall be shared with <COMPANY NAME>'s Security Officer to determine appropriate sanction/corrective disciplinary action.
	2. Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by <COMPANY NAME>'s Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that <COMPANY NAME> consider seeking risk management and/or legal counsel.

**8.4 Review and Reporting of Audit Findings**

Audit information that is routinely gathered must be reviewed in a timely manner, currently monthly, by the responsible workforce member(s). On a quarterly basis, logs are reviewed to assure the proper data is being captured and retained. The following process details how log reviews are done at <COMPANY NAME>:

1. The Security Officer initiates the log review by creating an Issue in the <COMPANY NAME> ticketing system.
2. The Security Officer, or a <COMPANY NAME> designee, is assigned to review the logs.
3. Relevant audit log findings are added to the request; these findings are investigated in a later step. Once those steps are completed, the request is then reviewed again.
4. Once the review is completed, the Security Officer approves or rejects the request. Relevant findings are reviewed at this stage. If the request is rejected, it goes back for further review and documentation. The communications protocol around specific findings are outlined below.
5. If the request is approved, the Security Officer then marks the request as Done, adding any pertinent notes required.

The reporting process shall allow for meaningful communication of the audit findings to those workforce members, Customers, or Partners requesting the audit.

1. Significant findings shall be reported immediately in a written format. <COMPANY NAME>'s security incident response form may be utilized to report a single event.
2. Routine findings shall be reported to the sponsoring leadership structure in a written report format.

Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.

Security audits constitute an internal, confidential monitoring practice that may be included in <COMPANY NAME>'s performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable ePHI shall not be included in the reports).

Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.

Log review activity is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.

**8.5 Auditing Customer and Partner Activity**

1. Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between <COMPANY NAME> and the 3rd party. <COMPANY NAME> will make every effort to assure Customers and Partners do not gain access to data outside of their own Environments.
2. If it is determined that the Customer or Partner has exceeded the scope of access privileges, <COMPANY NAME>'s leadership must remedy the problem immediately.
3. If it is determined that a Customer or Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, <COMPANY NAME> must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

**8.6 Audit Log Security Controls and Backup**

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.
3. Audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges.
	1. Separate systems are used to apply the security principle of "separation of duties" to protect audit trails from hackers.

**8.7 Workforce Training, Education, Awareness and Responsibilities**

1. <COMPANY NAME> workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. <COMPANY NAME>'s commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. <COMPANY NAME> workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.
2. <COMPANY NAME> Customers are provided with necessary information to understand <COMPANY NAME> auditing capabilities, and PaaS Customers can choose the level of logging and auditing that <COMPANY NAME> will implement on their behalf.

**8.8 External Audits of Information Access and Activity**

Prior to contracting with an external audit firm, <COMPANY NAME> shall:

1. Outline the audit responsibility, authority, and accountability;
2. Choose an audit firm that is independent of other organizational operations;
3. Ensure technical competence of the audit firm staff;
4. Require the audit firm's adherence to applicable codes of professional ethics;
5. Obtain a signed HIPAA business associate agreement;
6. Assign organizational responsibility for supervision of the external audit firm.

**8.9 Retention of Audit Data**

The Company must analyze storage needs and storage capacity of the centralized audit record storage system on at least an annual basis.

Systems generating audit logs may be configured to overwrite the oldest event logs if there is no more audit log storage space, however appropriate log storage facilities should be provided to ensure the following:

* A central audit log processing resource must store aggregate audit log data for at least one year with at least three months (or 90 days) available for immediate analysis.
* Audit trails must be secured so they cannot be altered where ever possible, and file integrity monitoring should be used to alert when they are altered. This is especially true for individuals who are responsible for managing user accounts and privileges.

**8.10 Potential Trigger Events**

The following table provides a list of audit events including the level of response that should be applied:

|  |  |  |
| --- | --- | --- |
| **Event Description**  | **Information System**  | **Real time notifications**  |
| Invalid logon attempt (unprivileged user)  | All systems  | No  |
| Invalid logon attempt (privileged user)  | All systems  | Yes  |
| Account lockout (unprivileged user)  | All systems  | No  |
| Account lockout (privileged user)  | All systems  | Yes  |
| Invalid logical access attempt to file or folder containing Client Confidential Data (CI)  | All servers  | Yes  |
| Valid logical access attempt to file or folder containing Client Confidential Data (CI)  | All servers  | No  |
| Successful malware infection  | All servers & workstations  | Yes  |
| Unsuccessful malware infection  | All servers & workstations  | No  |
| DoS attack (successful and unsuccessful)  | All servers, networking & security devices  | Yes  |
| Unplanned system shutdown  | All servers, networking & security devices  | Yes  |
| System or log file integrity check failure  | All servers  | Yes  |
| Failed Backup creation logs  | All Systems to be Backed up  | Yes  |
| Antivirus signature out of date  | All servers & workstations  | Yes  |
| Initialization of Audit Logs  | All servers  | Yes  |
| Valid logical access to Audit Logs  | All servers  | No  |
| Invalid logical access to Audit Logs  | All servers  | Yes  |
| Creation and deletion of system-level objects  | All servers  | Yes  |
| User Added/Deleted/Modified  | All Systems where Available  | No  |
| User Logon Failure on VPNs  | Network  | Yes  |
| Network/Firewall Policy/Configuration Changes  | Networking & security devices  | Yes  |
| Detection of unauthorized wireless access points  | Network  | Yes  |
| Critical IDS alerts  | Network  | Yes  |

**8.11 System Time Keeping**

Accurate time keeping is essential to effective and accurate event analysis. Systems should have their time sources synchronized to an authoritative time source to ensure a reasonable level of accurate time is used to “time stamp” event logs across all information processing resources. The following time source hierarchy should be employed:

* All applications must use their host systems for time keeping
* All host systems must use an approved/authoritative time source located at their hosting site for time keeping (i.e. Microsoft Domain Controller or equivalent)
* The approved/authoritative time sources must use an approved external source of time (i.e. pool.ntp.org).
* An alternate external time source should be considered in the event the primary time source becomes inaccessible.

**Purpose**

The purpose of this policy is to set forth the authority and outline the need, usage and limits to perform electronic and other forms of audit logging on <COMPANY NAME> networks, firewalls, and/or any other Company systems or resources. On-going system monitoring and audit logging should allow timely detection of and response to unauthorized information processing activities.

**Scope**

This policy covers any information or information processing resources owned or operated by the Company.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 00.a Information Security Management Program
* 01.a Access Control Policy
* 01.b User Registration
* 01.c Privilege Management
* 09.aa Audit Logging
* 09.ac Protection of Log Information
* 09.ab - Monitoring System Use
* 06.e - Prevention of Misuse of Information

Applicable Standards from the HIPAA Security Rule

* 45 CFR §164.308(a)(1)(ii)(D) - Information System Activity Review
* 45 CFR §164.308(a)(5)(ii)(B) - Protection from Malicious Software & Log-in Monitoring
* 45 CFR §164.308(a)(8) - HIPAA Security Rule Periodic Evaluation
* 45 CFR §164.312(b) - Audit Controls
* 45 CFR §164.312(2) - Mechanism to Authenticate ePHI
* 45 CFR §164.312(e)(2)(i) - Integrity Controls

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |