



Essent HealthCARE, INC.

Section:	Information Systems	Effective Date:	04/20/05
Subject:	IS Activity Audit Review Policy	Revision Date:	04/20/05
Policy #:	ISP-019	Review Date:	6/26/08
Approved By:	Chief Information Officer	Revision #:	1

Scope:

This policy is applicable to all Essent Healthcare, Inc. ("Essent"), facilities.

Purpose:

The purpose of this policy is to set forth the guidelines on how Information Systems policies will be monitored and audited by the Corporate Information Systems Department (CISD). This policy will provide the necessary tools for Essent to monitor all activities and provide assurance that all confidential and sensitive data is being accessed for the intent of necessary business practices.

Policy:

It is the policy of Essent to implement an audit process to monitor unauthorized access of electronic Protected Health Information (ePHI). Each facility FSO is responsible for auditing all policies and procedures within their organization. CISD will conduct a quarterly audit to ensure that the process is being done. A formal report of the audit will be delivered to the Chief financial Officer of the facility and the Chief Security Officer (CSO).

PROCEDURES:

The following functions must be monitored and audited at each facility by the FSO or designee. A quarterly audit of the same functions will be performed by a member of the CISD team.

User Activity Log (all systems):

FSO is required to maintain a proper log of all user activities within every system (MEDITECH or non MEDITECH) that have ePHI. These logs have to be kept for a period of six (6) years. FSO must review these logs in a monthly basis to ensure the validity and the integrity of the logs. The FSO must test 5 random accounts per patient type each month against unauthorized access. If unauthorized access is discovered, the FSO must report the incidents in accordance to Security Incident reporting policy (**ISP-012**) to the CSO. Disciplinary actions can be taken against unauthorized users in accordance to the Sanctions policy (**ISP-010**).

CISD will be responsible for reviewing these audits in a quarterly basis to ensure an accurate process at each facility. If CISD member, performing the audit, discovers issues or breaches in the auditing functions of the facility, they must report the findings immediately to the CSO in writing. Appropriate steps will be taken to correct the functions.



Essent HealthCARE, INC.

Section:	Information Systems	Effective Date:	04/20/05
Subject:	IS Activity Audit Review Policy	Revision Date:	04/20/05
Policy #:	ISP-019	Review Date:	6/26/08
Approved By:	Chief Information Officer	Revision #:	1

Backups:

FSO must ensure that systems that contain critical and ePHI data are backed up in accordance to the Essent backup policy (**ISP-005**). The policy requires the facility to maintain a backup log for period of six (6) years. During the quarterly audits, CISD will check the validity and integrity of these logs. Any failures must be corrected and reported in detail to the CSO.

Security Patches:

The FSO must ensure that every workstation and servers within the facility are updated to the latest Microsoft security patches in accordance with the Software and Hardware maintenance policy (**ISP-018**). As part of the quarterly audits, CISD will verify the compliance of this policy by testing minimum of 15 workstations and three (3) servers. The findings must be corrected and reported to the CSO.

Computer room environment/Physical safeguard:

FSO must ensure that all physical locations where computing infrastructure devices (routers, switches, and servers) are located will be kept in a controlled and secure environment. An inventory of individuals who have access to such location must be kept updated. Temperature in computer rooms must be checked daily and recorded. Temperature logs must be maintained for a period of one (1) year.

FSO must work with the facility maintenance personnel to ensure the proper testing of the backup generators. A log of these tests must be kept in the facility. In addition, all UPS backup system at every computer room within Essent that includes servers with ePHI DATA must be checked and kept under maintenance agreement.

During the Quarterly audits, CISD will audit the logs and maintenance agreements to ensure compliance with the policy. Any breaches must be reported in writing to the facility CFO and the CSO.

Work Station Security and Usage:

FSO must maintain a current inventory of workstations used within the facility to obtain ePHI data. The usage and security of the work station must be in accordance with workstation us policy (**ISP-007**) and workstation security (**ISP-008**). CISD will perform audits to ensure the compliance of these policies and will report any breaches in writing to the facility CFO and the CSO.



Essent HealthCARE, INC.

Section:	Information Systems	Effective Date:	04/20/05
Subject:	IS Activity Audit Review Policy	Revision Date:	04/20/05
Policy #:	ISP-019	Review Date:	6/26/08
Approved By:	Chief Information Officer	Revision #:	1

Content Filtering:

FSO must ensure that all Internet traffic from the facility is passed through a web content filtering system in accordance to the content filtering policy (**ISP-004**). During the quarterly audit, CISD will verify the existence of such system and its integrity.

References:

HIPAA Section 164.308(a)(2)
NIST Special Publication 800-12
NIST Special Publication 800-53