



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Security Incident Reporting & Response	Revision Date:	4/20/05
Policy #:	ISP-012	Review Date:	6/26/08
Responsible Party:	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 guidelines for identifying and reporting security incidents.

Policy:

It is the policy of Essent to protect the confidentiality and integrity of all electronic Protected Health Information (ePHI). As such, it is Essent’s policy to identify and report any suspected security breaches as defined in Essent policies and procedures. Security incident response and reporting should be done in accordance with the procedures outlined in this policy. The Facility Security Officer (FSO) is responsible for overseeing the proper resolution and documentation of each incident.

PROCEDURE and DEFINITIONS:

The security incident response process can be organized into four (4) phases. Appendix A represents a flow chart that describes all four phases.

1. Incident Identification

The incident identification phase consists of the decentralized processes that occur when a security incident has occurred or occurring. During this phase, an individual (manually) or a tool (automatically) reports that a security incident has occurred or is currently occurring. An incident report is opened by calling, paging or e-mailing the Help Desk at the local facility. Facilities are instructed to make certain that there is appropriate coverage for help desk during off hours.

Incidents are defined in three (3) categories:

- External Breach (Virus, worm)



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Security Incident Reporting & Response	Revision Date:	4/20/05
Policy #:	ISP-012	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

- Internal Breach (Unauthorized usage, failed/expired password, failed backups)
- Physical Breach (Theft, unauthorized access to computer room)

Instances where an individual would report a security incident include:

- An individual manually reviewing log entries notices a failure (i.e. backups)
- An individual notices a service or device becomes unavailable or not responding and the cause of the interruption is thought to be or determined to be denial of service attack or other security related incident.
- During the regular course of an employee's business day, a security breach is noticed.

Instances when a tool could report a security incident include:

- Firewall logs and alert
- Anti-virus alerts
- WAN vendor (AT&T) managed monitoring tools

The person receiving the reported incident (Help Desk or on-call person) becomes the ***Incident Investigator*** and they must record the incident in a log that will be kept in the facility.

2. Investigation

During this phase, the Incident Investigator will gather all known information regarding the incident and will perform a manual correlation of the current incident to the other incidents and events to determine the urgency and the scope of the incident. Some criteria in determining the severity and urgency are:

- Business Criticality
- System availability
- Level of current functionality
- Effect on patient care
- Lack of alternative methods



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Security Incident Reporting & Response	Revision Date:	4/20/05
Policy #:	ISP-012	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

3. Notification/Alerting and Responding

During this phase, the Incident Investigator will determine the scope of the incident, the immediate impact and initiate the response process. Escalation and alerting of the local and/or corporate IS members, is the responsibility of the Incident Investigator. Should the incident meet any of the following criteria, the incident escalation process should be followed:

- Incident has an immediate enterprise wide impact.
- Incident has visibility outside the company
- Incident has patient care impact
- Incident has caused a business critical service interruption

Escalation

In the event that the incident has immediate impact on the enterprise, the Incident Investigator and the Facility IS director (FISD) will escalate the incident to the Corporate IS department's Help Desk or on-call personnel. Certain incidents may require reporting or alerting an outside third party vendor or agency. Examples might include law enforcement agencies for incidents that include theft or HR department for unauthorized access. In the event that the corporate Help Desk or on-call personnel does not respond within 45 minutes, the Incident Investigator will escalate the call up to the Chief Information Officer of the corporation.

4. Reporting and Documenting

Every security incident within all Essent facilities must be documented with a formal report. All parties involved with the incidents are involved in the feedback and documentation process. The report, at minimum, must include the following information:

- Date and time
- Type
- Person reporting the incident
- Incident Investigator's information



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Security Incident Reporting & Response	Revision Date:	4/20/05
Policy #:	ISP-012	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

- Root cause
- Employee(s) involved
- Action(s) taken
- Resolution
- Date completed
- Future preventions
- Business Impact (if any)
- Damage Caused (if any)
- Management signoff

Reports on incidents that impacted the enterprise will be reviewed by a team from the local facility and CISD and the findings will be reported to the CSO. FSO will maintain a written log of all incidents for a period of six (6) years.

References:

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



ESSENT HEALTHCARE, INC.

Section: Information Systems	Effective Date: 4/20/05
Subject: Security Incident Reporting & Response	Revision Date: 4/20/05
Policy #: ISP-012	Review Date: 6/26/08
Responsible Party: Chief Information Officer	Revision #: 1

Appendix A

