Purpose

Adventist Health System (AHS), will apply, as part of its efforts to protect the confidentiality of patient information, promote compliance with its information security policies, state and federal regulations, appropriate sanctions against workforce members and medical staff who fail to comply with AHS information security policies, procedures, standards and requirements.

Definitions

Workforce Members: All employees, contractors, consultants, temporaries, as well as those representing themselves as being connected with AHS.

Medical Staff: All non-employed physicians that have been provided credentials to electronically access AHS information systems resources.

Policy

AHS will appropriately discipline workforce members and medical staff for violations of security policy or procedure to a degree appropriate for the gravity of the violation.

It is beyond the purview of this policy to assign specific sanctions for specific violations. However, AHS Human Resources and management should consider the following guidelines when determining appropriate sanctions for a given incident.

Sanctions include, but are not limited to, re-training, verbal and written warnings, revocations of privileges, termination of contract and/or dismissal from employment. AHS Human Resources, Compliance, and Administration will refer to the information below for additional guidance when determining appropriate sanctions for security violations.

Security Violation Categories

Category 1: actions which violate federal or state law, including but not limited to;

- Improper disclosure of an individual’s protected health information
- Improper disclosure of personal information which violates federal/state privacy or identity theft protection law
- Using AHS information system resources to threaten, harass, or intimidate others
• User AHS information system resources to engaged in illegal activities

• Using AHS information system resources without authorization to electronically scan, probe, attempt unauthorized access or disable either AHS or non-AHS systems

**Category 2:** actions which violate AHS policies and/or standards, but may not otherwise violate federal or state law including but not limited to:

• Improper or excessive use of AHS resources for non-business purposes such as excessive use of email or internet access for personal use

• Unauthorized attempts to bypass AHS Data Security controls such as anti-virus, web filters, firewalls, etc.

• Inappropriate sharing of credentials such as passwords and identification/access cards

• Inappropriate viewing, displaying or storing of materials (images, video, audio, etc.) that is not in keeping with the standards of AHS but does not otherwise violate federal or state law directly or creates a hostile or threatening work environment

**Category 1 Sanction Guidelines**

Workforce members and medical staff who violate federal and/or state law may be subject to criminal investigation, prosecution or civil monetary penalties in addition to internal AHS sanctions.

AHS Corporate Data Security will investigate any security incident or violation in this category. To the extent possible, AHS Corporate Data Security will mitigate any negative effects related to the incident. Any and/or all of the individuals involved may have their privileges revoked pending completion of the investigation. Incidents in this category may require notification to appropriate law enforcement agencies, government regulatory agencies, and affected individuals.

All Category 1 violations will be reported to the Local Compliance and Privacy Officer (LCPO). The LCPO will immediately notify local hospital administration, human resources, risk management and
the AHS Corporate Data Security Office. The LCPO will document the incident via the AHS Corporate Data Security Incident Reporting Form.

If, through investigation, it is determined that an individual has committed a violation in this category, he/she should expect that internal sanction will be substantial and may likely result in complete revocation of privileges and/or termination of employment. AHS will fully cooperate with any criminal investigation or prosecution efforts as required.

After completion of the investigation, the LCPO, Human Resources, Administration, and the Corporate Data Security Officer will determine the appropriate sanction based on the individual’s intent, expected knowledge concerning their actions, the resulting negative effect of the act and directions received from federal or state agencies.

If the incident involves medical staff the LCPO will also engage the appropriate local medical staff committee for review of appropriate disciplinary actions.

**Category 2 Sanction Guidelines**

Workforce members and medical staff who violate AHS Information System Security Policies and/or Standards will be subject to internal AHS sanctions.

AHS Corporate Data Security will investigate any security incident or violation in this category. To the extent possible, AHS Corporate Data Security will mitigate any negative effects related to the incident. Any and/or all of the individuals involved may have their privileges revoked pending completion of the investigation. Incidents in this category may require notification to government regulatory agencies and/or affected individuals.

All Category 2 violations will be reported to the Local Compliance and Privacy Officer (LCPO). The LCPO will immediately notify the AHS Corporate Data Security Office. The LCPO will document the incident via the AHS Corporate Data Security Incident Reporting Form.

If, through investigation, it is determined that an individual has committed a violation in this category, he/she should expect that
internal sanction(s) will be applied consistent with the facts of the incident.

After completion of the investigation, the LCPO, Human Resources, and the Corporate Data Security Officer will determine the appropriate sanction based on the individual’s intent, expected knowledge concerning their actions, the resulting negative effect of the act and direction received from federal or state agencies.

If the incident involves medical staff the LCPO will also engage the appropriate local medical staff committee for review of appropriate disciplinary actions.

References


Approved By

Donald L. Jernigan / President

Approval Date

1/11/11

Origination Date: October 12, 2007

Revision Date: December 2, 2010