Adventist Health System

Information Services – Corporate Data Security — Company-Wide
Information Security Sanction Policy — CW IS SEC 23

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 who fail to comply with AHS information security policies, procedures, standards and requirements.
Scope	This policy applies to all Adventist Health System workforce members, and information assets.
Definitions	**Workforce Member** includes AHS employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for AHS, is under the direct control of AHS, whether or not they are paid by AHS. ***Employee User***: Staff members that are paid by AHS through the payroll system including administrative, business, clinical, and information systems personnel and are provided access to AHS information assets. ***Medical Staff User***: All non-employed physicians that are credentialed by AHS Medical Staff Office and are provided access to AHS information assets. ***Contingent User***: Any individual or organization that has an active contractual relationship with AHS or is defined as a healthcare provider with whom AHS has a contractual professional services relationship and are provided access to AHS information assets. The contingent user group includes, but is not limited to, approved volunteers, students, and authorized physician office staff. ***Third party User***: Any individual who is not an employee, medical staff or contingent user and with whom AHS may or may not have a contractual agreement or obligation, but through the normal course of business operations AHS may deem it appropriate to provide access to AHS information assets. The third party user group includes, but is not limited to, regulatory inspectors, accreditation surveyors, utilization reviewers, contractors and vendor support personnel.

Policy	AHS will appropriately discipline workforce members 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 Medical Staff 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, pursuit of license/registration denial/revocation and/or dismissal from employment. Once a breach is verified management should consider: • the nature and gravity of the breach and its impact on business; • whether or not this is a first or repeat offense; • whether or not the violator was properly trained • relevant legislation; and business contracts • whether or not the workforce member has cooperated with federal, state, or AHS investigators. Failure to cooperate by any member can and in itself be cause for disciplinary action. In making their determination of disciplinary action. AHS Human Resources, Corporate Responsibility, Medical Staff and Administration will refer to the information below for additional guidance when determining appropriate sanctions for security violations. **<u>Security Violation Categories</u>** **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
- Using AHS information system resources to engage 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

Security Sanction Guidelines

Category 1 Sanction Guidelines
Workforce members who violate federal and/or state law may be subject to criminal investigation, prosecution or civil monetary penalties in additional 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 Regional Corporate Responsibility Officer (RCRO).

The RCRO will immediately notify local hospital administration, human resources, risk management and the AHS Corporate Data Security Office. The RCRO will document the incident via the AHS Corporate Data Security Incident Reporting Form.

If, the need for an investigation arises the individual's supervisor will be notified within 24 hours and if through the 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.

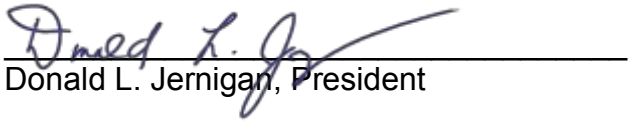
After completion of the investigation, the RCRO, Human Resources, Administration, and the Corporate Data Security Officer will determine the appropriate sanction based on the individual's intent, expected knowledge concerning their actions, the resulting negative effect of the act and directions received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

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

Category 2 Sanction Guidelines

Workforce members 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. **<u>All Category 2 violations will be reported to the Regional Corporate Responsibility Officer (RCRO).</u>** The RCRO will immediately notify the AHS Corporate Data Security Office. The RCRO 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 RCRO, 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 RCRO will also engage the appropriate local medical staff committee for review of appropriate disciplinary actions. The RCRO, Human Resources, and the Corporate Data Security Office will maintain a list employees involved in security incidents with the resulting outcome from the investigation.
References	HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
Approved By	 Donald L. Jernigan, President
Approval Date:	Date Origination Date: October 12, 2007

	Revision Date: December 2, 2010, September 3, 2015, June 7, 2016 Reviewed and affirmed: September 15, 2015