SALT LAKE COUNTY
COUNTYWIDE POLICY
ON
HIPAA SECURITY REQUIREMENTS

Reference –

Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 United States Code § 1320d et seq.; Part C Administrative Simplification.

American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act").

Department of Health and Human Services, 45 Code of Federal Regulations, Parts 160 and 164, subparts A and C of Part ("Security Rule")

Utah's Government Records Access and Management Act (GRAMA), Utah Code Annotated § 63G-2-101 et seq. ("GRAMA")

Salt Lake County Code of Ordinances; Title 2; Chapters 2.81 Security of Personal Identifiers and 2.82 Records Management.

Countywide Policies 1400 Series IT Security Policies; 1500 HIPAA Compliance and Privacy Requirements and 1515 HIPAA Breach Notification Requirements.

Purpose –

The purpose of this policy is to provide requirements applicable to specified County-covered health care components for protecting the security of electronic protected health information (ePHI). This policy shall apply to those covered health care components designated by the Mayor.

1.0 Responsibilities

1.1 Salt Lake County is a "hybrid entity" and has both covered health care components and non- covered health care components within its activities. The County, as a hybrid entity, is responsible for designating which of its activities are covered health care components and for ensuring that those components comply with HIPAA regulations. The County also has certain agencies, divisions, bureaus or other entities that may act as business associates of a covered entity. The County shall ensure compliance with HIPAA security requirements by requiring adherence to the standards set out in the Security Rule and the development and implementation of security procedures by those agencies that have covered health care components.

1.2 Business associates of the County are directly liable for compliance with certain HIPAA Privacy and Security rules requirements as defined by 45 CFR Parts 160, 162 and 164.

1.3 The adoption of the American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act, (HITECH Act), resulted in significant changes to the federal Privacy Rule and Security Rule. The HITECH Act requires notification to individuals if their unsecured PHI is improperly used or

disclosed. In addition, the HITECH Act makes business associates subject to the Security Rules' requirements.

1.4 The guidance provided herein is very general and is not a substitute for the review of all of 45 CFR parts 160, and 164.

2.0 Definitions

The definitions for the terms listed below can be found in 45 CFR 160.103, 45 CFR 162.103, and 45 CFR 164.103.

Access
Administrative Safeguards
Agency
Business Associate
Confidentiality
Covered Entity
Electronic Media
Electronic Protected Health Information (ePHI)
Facility
Individually Identifiable Health Information
Physical Safeguards
Protected Health Information (PHI)
Security or Security Measures
Subcontractor
Technical Safeguards
Workstation

3.0 Designation of HIPAA Security Officers

3.1 Each Agency shall designate an Agency Security Officer to serve as the point of contact for all security related issues for that office, Agency or program. The Agency Privacy Officer may assume this duty or it may be assigned to another individual in the agency. It is the responsibility of the Agency Security Officer to coordinate all security issues with the Agency Privacy Officer.

4.0 Security Procedures

4.1 Agencies must develop written Security Procedures that are appropriate for their divisions and offices in order to protect the privacy of ePHI that is created, received, or maintained during its regular course of business. The procedures shall comply with federal and state laws and be consistent with the HIPAA Security Rule.

4.2 The County and agencies shall modify their Security Procedures as necessary and appropriate to comply with changes in the state and federal law and ongoing business practices. Changes to policies may be made at any time, provided such changes are documented and implemented appropriately.

4.3 Agencies shall maintain written or electronic records of all relevant security documentation for the minimum period required by HIPAA or such longer periods as may be established in accordance with the Salt Lake County retention and disposition requirements as approved by the Government Records Access Management Policy

Administration (GRAMPA) according to County policy. (See 45 CFR 164.316)

5.0 Security Standards and Safeguards

5.1 Implementation specifications for security compliance are identified as either required or addressable standards. Each Agency must comply with all required standards as identified by 45 CFR 164.306, 164.308, 164.310 and 164.312.

5.2 The HIPAA Security Rule identifies three types of security standards that must be evaluated by the covered Agency. These categories include administrative, physical, and technical safeguards.

5.2.1 Administrative safeguards include agency policies, procedures, and guidelines used to manage security of ePHI (45 CFR 164.308). They are arranged into standards that include security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plans, evaluation, and business associate contracts.

5.2.2 Physical safeguards include those relating to facilities, maintenance, and equipment (45 CFR 164.310). They are arranged into standards that include facility access controls, workstation use, workstation security, and device and media controls.

5.2.3 Technical safeguards are those that refer to user security issues (45 CFR 164.312). They are arranged into standards that include access control, audit controls, integrity, authentication of users, and transmission security.

6.0 Business Associates

Agencies acting as Business Associates must comply with the administrative, physical and technical safeguards set out in the Security Rule and have procedures as described in section 3.1 above to comply with the standards (45 CFR §§ 164.308, 164.310, 164.312, and 164.316). Business Associates of Agencies that are Health Care Components should be required by contract to comply with the administrative, physical, and technical safeguards set out in the Security Rule and to have policies and procedures to comply with the standards.

7.0 Training

7.1 Training shall be conducted by those agencies that must comply with HIPAA security requirements and agencies acting as business associates that must comply with certain provisions of the HIPAA security requirements.

7.2 Violation of HIPAA security procedures may result in discipline in accordance with Salt Lake County Policies and Procedures.

APPROVED and PASSED this 30 day of July, 2013.

SALT LAKE COUNTY COUNCIL

_____
Steve DeBry, Chair

ATTEST:

_____
Sherrie Swensen, County Clerk

APPROVED AS TO FORM:

_____
District Attorney's Office Date