SALT LAKE COUNTY
COUNTYWIDE POLICY
ON
HIPAA BREACH NOTIFICATION 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, C, D and E ("Privacy Rule and 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; Chapter 2.82 "Records Management."

Salt Lake County Countywide Policies, HIPAA Compliance and Privacy Requirements 1500 and HIPAA Security Requirements 1510.

Salt Lake County Countywide Policies 1400 Series IT Security Policies.

Purpose –

The purpose of this policy is to provide requirements applicable to specified County covered health care components for reporting breaches of protected health information (PHI). 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. County offices, programs or portions thereof whether or not they are covered health care components, may be "business associates" of a covered entity, necessitating separate agreements between the County and an outside covered entity to cover those functions.

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. For purposes of this policy, the term "Business Associate" shall also include those entities categorized as "Qualified Service Organizations" under 42 CFR Part 2 Subpart B § 2.11. Definitions are found at this link.

1.3 Specific guidelines regarding Agency responsibilities relating to data breach and breach notification are included in the HIPAA Procedures on the County website.

THE GUIDANCE PROVIDED HEREIN IS VERY GENERAL AND IS NOT A SUBSTITUTE FOR THE REVIEW OF ALL OF 45 CFR PARTS 160 AND 164. References to the appropriate CFR sections are provided as assistance.

2.0 Definitions

The definitions for terms listed below can be found in 45 CFR 160.103; and 45 CFR 164.103, 164.304, 164.402, and 164.501.

Access
Breach
Business Associate
Disclosure
Electronic Media
Electronic Protected Health Information (ePHI)
Encryption
HITECH Act
Individually Identifiable Health Information
Protected Health Information (PHI)
Unsecured Protected Health Information

3.0 Unsecured PHI and Data Requirements

3.1 Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified annually by the Secretary of HHS. PHI may reside in data that is defined as data at rest; data in motion; and data disposed. Agencies are responsible to apply appropriate technologies or methodologies to ensure security of the data.

4.0 Breach of PHI and Exceptions

4.1 A breach of PHI is an impermissible use or unauthorized disclosure under the Privacy Rule that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the effected individual.

4.2 There are three impermissible uses or disclosures of PHI that do not constitute a breach. The Agency must investigate and document the circumstances showing that each of the following is not a breach because the Agency has the burden of showing that no breach occurred.

4.2.1 It is not a breach if a workforce member of the Agency, acting under the authority of the Agency or a business associate, unintentionally acquires accesses or uses PHI if the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. For example, a billing employee notices that he is not the intended recipient of an e-mail from a nurse containing PHI. The billing employee notifies the nurse of the misdirected e-mail and then deletes it.

4.2.2 It is not a breach if a workforce member or a business associate authorized to access PHI inadvertently discloses the PHI to another person authorized to access PHI within

the designated health care component of the Agency or a Business Associate, if the information received cannot be further used or disclosed in a manner not permitted by the Privacy Rule. For example, if one person authorized to use or disclose the information inadvertently discloses it to another person who is authorized to use or disclose PHI within the same Agency, the inadvertent disclosure is not a breach so long as the recipient does not use or disclose the information further. However, if the PHI is disclosed to a person at the Agency who is not authorized to use or disclose PHI, such as a person not in the designated health care component, it could constitute a breach.

4.2.3 It is not a breach if the Agency or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure of PHI was made, would not reasonably have been able to retain the information. For example, if a nurse mistakenly hands PHI papers to the wrong patient, but quickly realizes his mistake and recovers the PHI from the patient before that patient reads or retains the information, there has been no breach. Similarly, if PHI is mistakenly sent to the wrong person by mail, but the envelope is returned by the post office unopened and marked as undeliverable, there has not been a breach.

5.0 PHI Breach Investigation Requirements

5.1 All impermissible uses or disclosures of PHI should be investigated to determine whether the PHI was secured and whether there has been a breach. The investigation should be conducted by persons selected by the Data Breach Committee, a subset of the HIPAA Compliance Committee. If the PHI was unsecured, the investigation should determine whether notification is required and who should be notified, and the Agency shall ensure that any required notification is made. The Agency has the burden to show that all notifications were made as required.

6.0 Breach of PHI Notification Requirements to Individuals

6.1 Agencies that are designated health care components must provide notification of the breach of unsecured PHI that is reasonably believed to have been accessed, acquired, used or disclosed. Notification must be to affected individuals, the Secretary of HHS, and in some circumstances, to the media.

6.2 In general, notification to affected individuals includes information about the breach and the types of information (**such as full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information**); steps the individual needs to take; actions taken by the Agency; and contact information. Notification must be provided **without unreasonable delay and in no case later than 60 calendar days** following the discovery of a breach.

6.3 Breach Discovery: A breach of unsecured PHI is considered to be discovered as of the first day on which the breach is known to the Agency, or, if the Agency had exercised reasonable diligence, would have been known to the Agency. In situations where a Business Associate suffers a breach of security and is acting as an agent of the Agency, the date that the Business Associate knew or should have known of the breach may be attributed to the Agency.

6.4 Law Enforcement Delay: If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Agency shall delay the notification, notice, or posting for the time period specified (in writing)by the official. If the delay is stated orally, the Agency must document the statement and delay

notification, notice, or posting no longer than 30 days from the date of the oral statement.

7.0 Breach of PHI Notification by a Business Associate to the Agency:

7.1 Business Associates of an Agency are required by contract to notify the Agency of a breach of PHI or a suspected breach. The contract should require notification to the Agency within 5 business days after the discovery of a breach. The notification should include the identification of each individual affected and any other available information that the Agency is required to include in the notification to individuals.

7.2 The Agency should consider whether insurance requirements for third-party property loss, damages, remediation costs, and government investigations should be included in the Business Associate Contract. It should also consider whether to seek indemnification from the Business Associate for unauthorized use and disclosure and failure to de-identify information properly, if applicable.

7.3 A breach of unsecured PHI is considered to be discovered by the Business Associate as of the first day on which the breach is known to the Business Associate, or if the Business Associate had exercised reasonable diligence, would have been known to the Business Associate.

8.0 Breach of PHI Notification by the Agency as a Business Associate to a Covered Entity

8.1 If the Agency is a Business Associate of a Covered Entity and discovers a breach of PHI in its capacity as a Business Associate, it must notify the Covered Entity for which it is a Business Associate. The notification to the Covered Entity must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach. The notification shall include the identification of each individual affected any other available information that the Covered Entity is required to include in the notification to individuals.

8.2 A breach of unsecured PHI is considered to be discovered by the Agency as a Business Associate as of the first day on which the breach is known to the Agency, or if the Agency had exercised reasonable diligence, would have been known to the Agency.

9.0 Standard Forms

9.1 Salt Lake County shall make available standard forms templates to assist agencies in complying with the HIPAA Privacy Rule breach notification requirements subject to modification by the agencies to meet their specific needs. Changes to forms shall be made when significant policy changes have been made or it is appropriate to comply with changes in the state or federal law or ongoing business practices.

APPROVED and PASSED this 10 day of September, 2013.

SALT LAKE COUNTY COUNCIL

_____
Steve DeBry, Chair

ATTEST:

_____

Sherrie Swensen, County Clerk

APPROVED AS TO FORM:

_____

District Attorney's Office Date