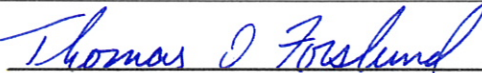
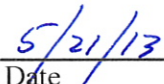


Thomas O. Forslund, Director

Governor Matthew H. Mead

Policy Title:	Integrity	
Policy Number:	S-017	
Effective Date:	July 1, 2013	
Approval:	 _____ Thomas O. Forslund, Director	 _____ Date

Purpose:

This policy establishes Wyoming Department of Health's (WDH) responsibility to guard electronic protected health information (ePHI) from improper alteration or destruction.

Scope:

This policy applies to all WDH workforce.

Definitions:

Data Authentication Controls means technical controls to validate that data has not been altered or destroyed in an unauthorized manner.

Data Transit Controls means controls designed to ensure that data in transit is not improperly modified until it reaches its appropriate destination or is disposed of.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Software Controls means controls to ensure that software used by WDH has the ability to protect against unauthorized alteration or modification, record missing or critical information, and control simultaneous updates.

Workforce Protocols refers to successful implementation of, training on, and workforce compliance with policies addressing administrative, physical, and technical safeguards for data at rest and in transit.

Policy:

1. General

- a. WDH shall maintain a comprehensive internal security control program to protect ePHI from improper alteration or destruction and to keep ePHI consistent with its source. Such program shall consist of a combination of:
 - i. Policies designed to preserve the integrity of ePHI; and
 - ii. Electronic mechanisms to corroborate that ePHI has not been altered or destroyed.
- b. The WDH Compliance Office shall determine and implement appropriate integrity controls based upon several factors, including, but not limited to:
 - i. The results of the risk analysis process as outlined in WDH Policy S-001a; Risk Analysis and Management.
 - ii. The resources required to implement integrity controls and their associated costs.
 - iii. The need to balance confidentiality of ePHI with data integrity and availability.
 - iv. Examination of several implementation considerations, including, but not limited to:
 - A. Data authentication controls (e.g., data recovery features);
 - B. Data transit controls (e.g., encryption);
 - C. Software controls; and
 - D. Workforce protocols.
- c. The WDH Compliance Office shall monitor implemented integrity controls for effectiveness.
- d. WDH data systems that do not have adequate data integrity mechanisms shall not be used to store or transmit ePHI.

2. Encryption

- a. ePHI contained on workstations is required to be either file, folder, or full disk encryption.
- b. Any mobile devices that contain or may contain ePHI that connect to the network shall be encrypted.
- c. Files containing ePHI that are transmitted across the Internet (e.g., via e-mail) shall either be encrypted or delivered via an approved encrypted delivery method (e.g., [gsecure]).
- d. Antiquated systems and applications containing ePHI that are incapable of encryption due to technology limitation, but which have compensating controls, may be granted exception by the WDH Compliance Office. However, such systems and applications shall have a full risk assessment performed to ensure the compensating controls are an acceptable alternative to encryption. Exceptions shall be reviewed periodically and removed once a suitable solution is available.

Contacts:

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

Policies:

AS-010; E-mail, Facsimile, and Printer/Copier/Scanner Machines
AS-013; Acceptable Use of Information Systems
S-001a; Risk Analysis and Management
S-005b; Protection from Malicious Software

References:

45 CFR §§ 164.304 and 312(c) and (e)

Training: