Wyoming
Department
of Health

Commit to your health.
visit www.health.wyo.gov

Thomas O. Forslund, Director

Governor Matthew H. Mead

Policy Title:	Information Systems Activity Review and Audit Controls
Policy Number:	S-001c
Effective Date:	July 1, 2013
Approval:	Thomas O Forslund Thomas O. Forslund, Director 6/17/13 Date

Purpose:

Wyoming Department of Health (WDH) is committed to conducting periodic internal system and records reviews. As such, WDH shall assess potential risks and vulnerabilities to protected health information (PHI) in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with 45 CFR § 164.308.

Scope:

This policy applies to all WDH workforce.

Definition(s):

The Separation of Duties Principle specifies that to prevent any part of a computer system from being under the control of a single person, every duty or transaction requires multiple people to be involved, with tasks being split among them.

Policy:

1. **General**
   a. WDH shall implement a process to ensure access and activity are recorded and reviewed (audited) for all WDH information systems that contain or access PHI.
   b. Such access and activity reviews shall be completed on an annual basis or more frequently as necessary.
   c. To ensure accountability and avoid conflict of interest, more than one person may conduct review functions in accordance with the Separation of Duties Principle. The number of persons assigned to a review shall be determined by the size and complexity of the system environment. Workforce members should not be assigned to monitor or review activity related to their own user accounts.
   d. Reviewers shall have appropriate technical skills (with respect to the operating systems and applications) to access and interpret audit logs correctly.

2. **Monitoring**
   a. Hardware, software, or auditing mechanisms shall be used to track the following:
      i. Date and time of activity;
      ii. Origin of activity;
      iii. Identification of user performing activity; and
      iv. Description of attempted or completed activity.
   b. The following activity shall be monitored:
      i. Account use;
      ii. Start and stop times;
      iii. Failed authentication attempts;

iv. General log-in activity;
v. Password change activity; and
vi. Data modification.

3. **Audit log reviews** shall:
   a. Be conducted daily;
   b. Be conducted manually or by using automated tools;
   c. Examine user login information, including login successes and failures;
   d. Examine whether security incidents were reported and proper follow-up was performed;
   e. Ensure all user access lists are current and all unauthorized user access has been removed; and
   f. Examine whether WDH policies are being followed.

4. **Retention** of system activity review documentation shall be in accordance with WDH Policy S-020; Documentation and Retention.

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:

S-001; Security Management Process
S-020; Documentation and Retention

References:

45 CFR § 164.308
Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham Website.
http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html

Training: