Information System: Amazon AWS Server Instance – GROUSE Research Environment
Information Owner: Dr. Russ Waitman

Description or Purpose:

HIPAA Technical Security Rule Compliance Analysis

§ 164.312 (a)(1) – Access Controls:

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

Implementation Status:
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Description of Compliance: Each user will be assigned with a unique user account, which is associated to a pre-defined project-specific Role (A, B, C) with different level of privileges approved by key stakeholders. A project account manager (Role B Administrator) is assigned and trained with ongoing responsibilities to monitor accounts regularly as well as review accounts at least annually. The account manager is responsible to:

1. Work closely with key stakeholders and Institutional Review Board (IRB) to oversight account provisioning and continuous monitoring.
2. Ensure access to the system is limited to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
3. Ensure access to the system is limited to the types of transactions and functions that authorized users are permitted to execute.
4. Identify distinct account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
5. Enable a centralized and automated account management with at least one “account manager” appointed and properly trained.
6. Establish conditions and policies for group and role membership.

7. Identify authorized users of the information asset and specifying access privileges for each account.

8. Require appropriate approvals for requests to establish accounts.

9. Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions/business functions.

10. Establish, activate, modify, disable, and remove accounts in accordance with defined procedures.

11. Monitors the use of information system accounts (e.g. user accounts).

12. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

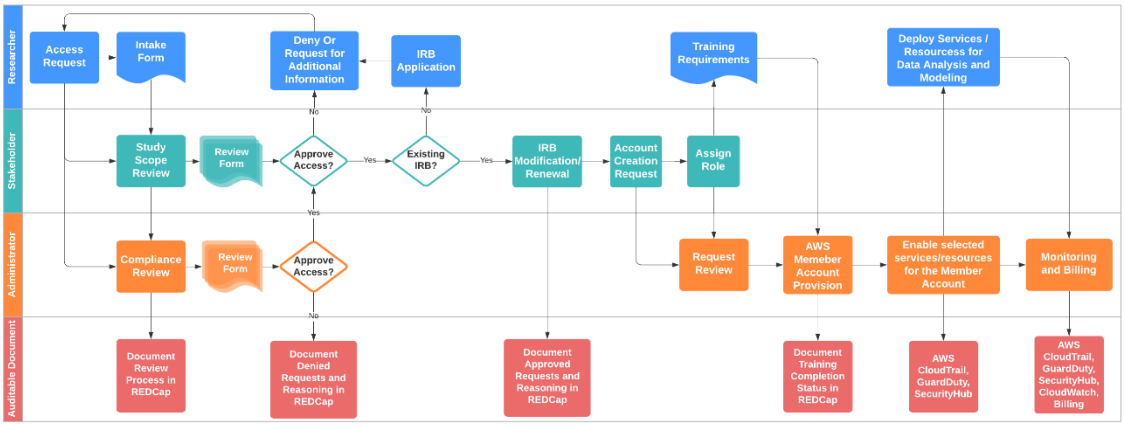
13. Not allow the use of guest/anonymous and temporary accounts.

14. Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.

15. Deactivate/disable emergency, temporary and expired accounts that are no longer required and accounts of terminated or transferred users.

16. Tracks all types of account changes (e.g. creation, enabling, modifying, disabling, deletion) within audit records without interruptions.

GROUSE account governance process is described in the figure below:



Within the AWS environment, we adopt the native federation solution, single-sign-on (SSO), for better central account management, which uses AWS SSO identity store as default identify source. We define Permission Sets (a collection of administrator-defined policies that AWS SSO uses to determine a user's effective permissions) to consistently and programmatically enforce access controls (allow or deny) associated with users' roles and accounts.

§ 164.312 (a)(2)(i) – Unique user identification (required): *Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.*
Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Description of Compliance: Each user will be assigned with a unique user account, which is associated to a pre-defined project-specific Role (A, B, C) with different level of privileges approved by key stakeholders.

§ 164.312 (a)(2)(ii) – Emergency access procedure (required): *Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.*
Implementation Status: ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable
Description of Compliance: The GROUSE Research Environment is intended for research purposes, and is not a “gold-source” solution pertinent to patient care.

§ 164.312 (a)(2)(iii) – Automatic logoff (addressable): *Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*
Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable

Description of Compliance: User sessions automatically terminate **after 30 minutes of inactivity**. Some application accounts as pre-defined (e.g., i2b2) can have idle sessions when users are not running queries and scheduled tasks such as ETL scripts running under system level accounts are not considered user sessions.

§ 164.312 (a)(2)(iv) – Encryption & decryption (addressable):

Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

Implementation Status:
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Description of Compliance: Data is encrypted in transit and at rest within the AWS GROUSE Research Environment with 256-bit AES encryption.

§ 164.312 (b) – Audit Controls:

Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Implementation Status:
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Description of Compliance: The following events are recorded in an audit log within the GROUSE Research Environment:

a. Server alerts and error messages;

b. User log-on and log-off (successful or unsuccessful);

c. All system administration activities;

d. Modification of privileges and access;

e. Start up and shut down;

f. Application modifications;

g. Application alerts and error messages;

h. Configuration changes;

i. Account creation, modification, or deletion;

j. File creation and deletion;

k. Read access to sensitive information;

l. Modification to sensitive information;

m. Printing sensitive information;

n. Anomalous (e.g., non-attributable) activity;

o. Data as required for monitoring privacy controls;

p. Concurrent log on from different work stations;

q. Override of access control mechanisms;

r. Process creation;

s. Attempts to create, read, write, modify, or delete files containing PHI.

§ 164.312 (c)(2) – Implementation specification: Mechanism to authenticate ePHI (addressable):

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Implementation Status:
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Description of Compliance: Data is encrypted in transit and at rest within the AWS GROUSE Research Environment with 256-bit AES encryption. Security audit logging records any activity to the access and alteration of any data within the environment.

§ 164.312 (d) – Person or entity authentication:

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Description of Compliance: Requests for access are subject to a rigorous review process that begins with a request recorded within the REDCap information system and scrutinized from there. Stringent authentication processes are maintained, as well as the use of two-factor authentication.

§ 164.312 (e)(1) – Transmission security: *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*
Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Description of Compliance: Data is encrypted in transit and at rest within the AWS GROUSE Research Environment with 256-bit AES encryption.

§ 164.312 (e)(2)(i) – Integrity controls (addressable): *Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.*
Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Description of Compliance: Data is encrypted in transit and at rest within the AWS GROUSE Research Environment with 256-bit AES encryption. Security audit logging records any activity to the access and alteration of any data within the environment.

§ 164.312 (e)(2)(ii) – Encryption (addressable): *Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.*
Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Description of Compliance: Data is encrypted in transit and at rest within the AWS GROUSE Research Environment with 256-bit AES encryption. Security audit logging records any activity to the access and alteration of any data within the environment.

§ 164.316 (b)(2)(i) – Time limit (required): *Retain the documentation required by* 45 CFR *§ 164.316(b)(1) for 6 years from the date of its creation or the date when it last was in effect, whichever is later.*
Implementation Status: ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Description of Compliance: Documentation regarding the creation and maintenance of the GROUSE Research Environment will be maintained for a minimum of 6 years, per the UM System Records Management Policy.