AudSoft, Inc.
HIPAA Security Policy

Administrative Safeguards
Security Management Policy

Statement of Policy

AudSoft, Inc. is a *Business Associate* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, AudSoft, Inc. is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect AudSoft, Inc.'s commitment to complying with such Regulations. AudSoft, Inc. will comply with the *Covered Entity's* documented HIPAA policies and procedures unless specifically stated in the below policy.

Purpose of Policy

The purpose of the policy is to develop a risk management process for the selection and implementation of security safeguards to reduce the risks to electronic Protected Health Information (ePHI) to reasonable and manageable levels.

Policy

1 Security Management Policy

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(1)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures to prevent, detect, contain and correct security violations."

AudSoft, Inc. will protect the confidentiality, integrity, and availability of ePHI by maintaining appropriate safeguards for the networks and systems that handle ePHI. AudSoft, Inc. will implement policies and procedures to prevent, detect, contain, and correct security violations.

AudSoft, Inc. will comply with the covered entity's policies and procedures where possible and will ensure appropriate policies and procedures for protecting ePHI in addition to the covered entity's policies and procedures.

1.1 Risk Analysis

SAFEGUARD: Administrative
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity."

1. AudSoft, Inc. acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI in the same regard as a covered entity.

2. AudSoft, Inc. acknowledges the potential vulnerabilities associated with storing ePHI, transmitting ePHI locally and transmitting ePHI outside of AudSoft, Inc..

3. To appropriately assess such potential vulnerabilities, AudSoft, Inc. shall perform a Risk Assessment which:

    i. Identify and document all ePHI repositories

    ii. Identify and document potential threats and vulnerabilities to each repository

    iii. Assess current security measures

    iv. Determine the likeliness of threat occurrence

    v. Determine the potential impact of threat occurrence

    vi. Determine the level of risk

    vii. Determine additional security measures needed to lower level of risk

    viii. Document the findings of the Risk Assessment

Procedure

1. **Document all ePHI repositories**

    i. Identify and document where ePHI is stored, received, maintained or transmitted.

        1. ePHI may be indentified through surveys, questionnaires, interviews, review of documentation, automated scans, or other data gathering methods.

    ii. The output of this process should be documentation of all repositories/systems that contain ePHI in an organization.

2. **Identify and document potential threats and vulnerabilities to each repository**

i. Identify and document all reasonably anticipated threats to ePHI. Examples of Threats include:

1. Data entry error
2. Theft of a laptop
3. Power outage

ii. Identify and document all vulnerabilities to each ePHI repository.

iii. The output of this process should be documentation of all reasonably anticipated threats and vulnerabilities to each repository/system that contains ePHI within an organization.

3. Assess current security measures

i. Review the current security measures (safeguards / controls) that are currently in place that are used to mitigate identified risks. Examples of current safeguards include:

1. User awareness training
2. Backup procedures
3. Disaster Recovery procedures
4. Employee termination procedures

ii. The output of this process should be documentation of current security measures to protect any repositories/systems that contain within an organization.

4. Determine the likeliness of threat occurrence

i. For each threat and vulnerability to ePHI that has been identified in step 2 of the Risk Assessment procedure, calculate the likelihood of the threat occurring.

ii. The likeliness or probability of a threat occurring is usually measured in (low, medium or high) or expressed as a number of times a threat is likely to occur in a given year.

iii. Existing security measures as identified in step 3 of the Risk Assessment procedure may lower the likeliness of a threat.

iv. Existing vulnerabilities as identified in step 2 of the Risk Assessment procedure may raise the likeliness of a threat.

v. Examples of a likeliness of a threat includes:

1. If there has been issues with power outages in the past then the threat of a power outage may be assessed as ***High***. Additionally, if a backup generator has been previously installed (current security measure) then the likeliness of a threat of a power outage may be reduced to ***Medium*** or ***Low***.

2. If there have been no issues with flooding in the past 5 years then the threat from flooding may be assessed as ***Low***.

vi. The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI of an organization.

5. Determine the potential impact of threat occurrence

i. For each threat and vulnerability to ePHI, calculate the associated impact of the threat.

ii. Examples of threat impact include:

i. A fire in the computer room that contains all ePHI repositories / systems would have a ***High*** impact. The fire may affect the availability of ePHI repositories / systems.

iii. The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of ePHI within an organization.

6. Determine the level of risk

i. For each threat and vulnerability to ePHI, calculate the level of risk of the associated threat.

ii. The level of risk is calculated by using the likeliness of a threat, as calculated in step 4 of the Risk Assessment procedure and the resulting impact of a threat, as calculated in step 5 of the Risk Assessment procedure.

iii. An example of calculating the level of risk for a threat include:

1. If the threat of a flood has been calculated with a likeliness of **High** and the impact of a flood has been calculated as **High** then the associated level of risk would then be **High**.

2. If the threat of a power outage has been calculated as **Low** and the impact of a power outage has been calculated as **Medium** then the associate risk level would be **Low**.

iv. The output of this process should be documentation of the level of risk associated with each threat and impact to the confidentiality, availability and integrity of ePHI within an organization.

7. Determine additional security measures needed to lower the level of risk

i. Based on the determination of the level of risk as defined in step 6 of the Risk Assessment procedure, additional security measures (safeguards / controls) may be needed to lower the risk.

ii. Examples of additional security measures needed include:

1. If the threat of a power outage has been calculated as **High** and the impact of a power outage has been calculated as **Medium** then the associate risk level would be **High**. An additional security measure that may be implemented would be the installation of a backup generator to lower the likeliness of a power outage impacting any systems containing ePHI.

iii. The output of this process should be documentation of any additional security measures that are needed to lower the level of risk associated with each threat and impact to the confidentiality, availability and integrity of ePHI within an organization.

8. Document the findings of the Risk Assessment

i. The final step in the Risk Assessment process is to document and publish all of the findings in each of the steps of the Risk Assessment procedure.

1.2 Risk Management

SAFEGUARD: Administrative
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (a) [Risk analysis]."

1. AudSoft, Inc. shall implement security measures and safeguards for each ePHI repository sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The level, complexity and cost of such security measures and safeguards must be commensurate with the risk classification of each such ePHI repository.

2. AudSoft, Inc. will reassess the potential risks and vulnerabilities of an ePHI repository as part of a periodic review; it must update the security measures and safeguards for such

ePHI repository to reflect any changes in the risks and vulnerabilities assessment. At a minimum the risk management process will include the following:

i. Assessment and prioritization, on the basis of risks, of each ePHI repository.

ii. Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage, mitigate, or accept identified risks.

iii. Security training and awareness on implemented security measures to workforce members.

iv. Periodic evaluation and revision, as necessary, of the security measures.

Procedure

1. The Risk Management process will be based on the following steps

   i. Risk Analysis – A Risk Analysis will be performed based on Risk Analysis policy (1.1).

   ii. Risk Prioritization - Using information from the risk analysis, risks will be ranked on a scale (from high to low) based on the potential impact to information systems containing ePHI and the probability of occurrence.

   iii. Cost-benefit analysis – An analysis shall identify and define the costs and benefits of implementing or not implementing the identified security methods.

   iv. Safeguard selection – Safeguards shall be selected that are the most appropriate security methods to mitigate or manage identified risks to critical information systems and ePHI. Such selections will be based on the nature of specific risks and the feasibility, effectiveness, and cost of specific safeguards.

   v. Assignment of responsibility – Appropriate workforce members will be identified and assigned responsibility for implementing and managing selected safeguards.

   vi. Security method evaluation - Selected security safeguards will be regularly evaluated and revised as necessary.

   vii. The results of each of the above steps will be formally documented.

1.3 Sanctions for Noncompliance

SAFEGUARD: Administrative
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

1. AudSoft, Inc. acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) it is required to protect ePHI in the same regard as a covered entity.

2. To ensure that all workforce members fully comply with Security Policies, AudSoft, Inc. will appropriately discipline and sanction employees and other workforce members for any violation of the HIPAA Security Policies and Procedures

Procedure

1. Security Violations that Prompt Consideration of Disciplinary Action.

    i. Human Resources or a department / person with similar responsibilities may discipline a workforce member, who violates the HIPAA Security Rule

    ii. Human Resources or a department / person with similar responsibilities may also discipline managers or supervisors, if their lack of diligence or lack of supervision contributes to a subordinate’s Security Violation.

2. Investigation of Security Violation

    i. A workforce member who becomes aware of a Security Violation shall promptly communicate the report to the HIPAA Security Officer and his or her supervisor or Human Resources or a department / person with similar responsibilities.

    ii. After receiving a reported Security Violation, the HIPAA Security Officer or someone designated by him or her shall determine the facts and circumstances surrounding the violation, and report the findings to Human Resources or a department / person with similar responsibilities.

3. Imposition of Discipline

    i. Human Resources or a department / person with similar responsibilities shall impose sanctions for a Security Violation in accordance with Human Resources policies.

4. Reporting of Security Violations

    i. The failure to report a known Security Violation could lead to discipline because each workforce member has an obligation to report any Security Violation of which the workforce member becomes aware to the HIPAA Security Officer and to his or her supervisor or the Human Resources Department or a department / person with similar responsibilities.

1.4 Information System Activity Review

SAFEGUARD: Administrative
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(D)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports."

1. Internal audit procedures shall be implemented or follow a covered entity's procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. To ensure that system activity for all systems that contain ePHI is appropriately monitored and reviewed, a covered entity's procedures should be followed or the following procedures outlined below should be implemented.

    i. An internal audit procedure should be established and implemented to regularly review records of system activity. The internal audit procedure may utilize audit logs, activity reports, or other mechanisms to document and manage system activity.

        1. Audit logs, activity reports, or other mechanisms to document and manage system activity should be reviewed at intervals commensurate with the associated risk of the information system or the ePHI repositories contained on each information system. The interval of the system activity review should not exceed, but may be less than, 90 days.

    ii. An Audit Control and Review Plan should be created and approved by the HIPAA Security Officer. This plan should include:

        1. Systems and Applications to be logged

        2. Information to be logged for each system

        3. Procedures to review all audit logs and activity reports

        4. Security incidents such as activity exceptions and unauthorized access attempts should be detected, logged and reported immediately to the appropriate system management and HIPAA Security Officer in accordance with the HIPAA Security Policy #6 – Security Incident Procedures

3. A Risk Analysis as defined in Section 1.1 of the AudSoft, Inc. HIPAA Security Policy #1 - Security Management Policy should be performed annually but not more than every two years.

Effective Date: 10/22/2018
Last Revision Date: 01/03/2023