108 SECURITY RULE COMPLIANCE

EFFECTIVE DATE: April 29, 2020
REFERENCES: 42 CFR 438.100(d) and 42 CFR 438.208(b)(4); 45 CFR Parts 160, 162, and 164; Section F3, Contractor Chart of Deliverables

This policy applies to the Division Developmental Disabilities (The Division).

Definitions

A. Breach - An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised. As stated in Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act issued in August 2009.

B. Health Insurance, Portability, and Accountability Act (HIPAA) - The Health Insurance Portability and Accountability Act; also known as the Kennedy-Kassebaum Act, signed August 21, 1996 as amended and as reflected in the implementing regulations at 45 CFR Parts 160, 162, and 164.

C. HIPAA Privacy Rule - The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individual health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of individual health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.

D. HIPAA Security Rule - Established national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

E. Health Information Technology for Economic and Clinical Health Act (HITECH) -

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

F. Protected Health Information – Individually identifiable health information as described in 45 CFR 160.103(5) about an individual that is transmitted or maintained in any medium where the information is:

- Created or received by a health care provider, health plan, employer, or health care clearinghouse.
- Relates to the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or payment for the provision of health care to an individual.

Protected health information excludes information:

- In education records covered by the Family Educational Rights and Privacy Act as amended, 20 U.S.C. 1232g
- In records described at 20 USC 1232g(a)(4)(B)(IV)
- In employment records held by a covered entity in its role as an employer
- Regarding a person who has been deceased for more than 50 years.

G. Information Technology (IT) Risk Analysis - The assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information held by a covered entity, and the likelihood of occurrence.

H. Information Technology (IT) Risk Management - The actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its electronic protected health information and meeting the general security standards.

Data Security Audit

The Division must develop policies and procedures to ensure the privacy of protected health information, the security of electronic protected health information, and breach notification to members [42 CFR 438.100(d) and 42 CFR 438.208(b)(4)].

The Division must have a security audit performed by an independent third-party annually. If the Division performs in multiple AHCCCS lines of business, one comprehensive audit may be performed covering all systems for all lines of business or separate audits may be performed.

The audit must include, at a minimum, a review of the following:

1. Compliance with all security requirements as outlined in ACOM Policy 108, Attachment A, AHCCCS Security Rule Compliance Summary Checklist.
2. The Division policies and procedures to verify that appropriate security requirements have been adequately incorporated into the Division's business practices, and the production processing systems. The Division's policies and procedures must include the requirements for the Breach Notification Rule.

Audits performed in the second and subsequent years of the contract will focus primarily on remediation of prior findings and system and policy changes identified since the prior audit.

AHCCCS Security Compliance Report

The Division must submit the AHCCCS Security Rule Compliance Report to AHCCCS annually as described in Section F3, Contractor Chart of Deliverables, by uploading the report to a secure AHCCCS Share Point site. The timeframe audited may be calendar year, fiscal year, or contract year and must be noted in the report. The report must include all findings detailing any issues and discrepancies between the AHCCCS Security Audit Checklist requirements and the Division's policies, practices and systems, and as necessary, a corrective action plan. In addition, the report must include written decisions regarding all addressable specifications.

The Division will verify that the required audit has been completed and the approved corrective action plan is in place and implemented as part of Operational Reviews.

The Division does not intend to release detailed audit reviews; however may, at its discretion, release a summary level of results.

AHCCCS Security Rule Compliance Checklist

A. Instructions

The AHCCCS Security Rule Compliance Checklist, located in the AHCCCS Operations Manual, identifies security rule requirements for administrative, physical, and technical safeguards. The Compliance Checklist must be signed and dated by the Chief Executive Officer or his/her designee verifying the information and must be submitted with the annual report.

B. Implementation Specifications

1. Required Specifications

If an implementation specification is identified as "required" (indicated with an "R" on the checklist), the specification must be implemented.

Addressable Specification: The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards. Addressable implementation specifications are indicated with an "A" on the checklist.

In meeting standards that contain addressable implementation specifications, a covered entity must do one of the following for each addressable specification:

a. Implement the addressable implementation specifications.

b. Implement one or more alternative security measures to accomplish the same purpose.

c. Not implement either an addressable implementation specification or an alternative.

The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. For example, a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.

The decisions that a covered entity makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

2. IT Risk Analysis

The required implementation specification at 45 CFR 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, *"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."*

IT Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic PHI held by a covered entity and the likelihood of occurrence. The risk analysis may include taking inventory of all systems and applications that are used to access and house data and classifying them by level of risk. A thorough and accurate risk analysis would consider all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage.

3. IT Risk Management

The required implementation specification at 45 CFR 164.308(a)(1)(ii)(B), for IT Risk Management, requires a covered entity to *"implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR. 164.306(a) [(the General Requirements of the Security Rule)]."* IT Risk management is the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its electronic PHI and to meet the general security standards.

4. Compliance Status

If the covered entity complies with the requirement, insert a "C" in the column. If the requirement is not met, insert "NC" for non-compliant.

5. Compliance Documentation

List policies, procedures, and processes used to determine compliance with the Implementation Specification.