NetFoundry Alignment to HIPAA

Summary

HIPAA, or the Health Information Portability and Accountability Act is a US law governing the handling of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) There are several areas where NetFoundry can assist a provider in meeting HIPAA standards. Below, you will find excerpts of the various bills that make up HIPAA overall, and an explanation of how NetFoundry can be of assistance in meeting these requirements.

You may find or hear references to HITRUST, which is a cybersecurity framework (CSF) created by a healthcare industry alliance to provide specific technical controls to meet these goals. The license agreement of HITRUST CSF does not allow us to use the text of the framework, so we cannot provide distinct methods and procedures to meet the controls.

HIPAA also had a requirement for regulated entities to ensure compliance with the HIPAA law for their contractors, processors, and other business associates dealing with PHI or ePHI. NetFoundry does not meet the criteria of a Business Associate, and therefore, does not sign Business Associates Agreements (BAAs). The definition of Business Associate is below, from the text of the law, and there is also an excerpt from the Omnibus Rule. The Omnibus Rule was published to clarify a number of items from the initial passage of the law that had caused confusion within the industry. As highlighted, it does explicitly provide the "conduit exception". This is why NetFoundry is not a BA, not covered bu HIPAA directly. While ePHI may pass across our nodes, it does so in a strongly encrypted form. The encryption of each data plane session is ephemeral, dynamic, and done between customer owned nodes, making it complete inaccessible to NetFoundry.

Technical Controls

Excerpted from https://www.law.cornell.edu/cfr/text/45/part-164/subpart-C

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)

(1) ***Standard: Access control.*** 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).

NetFoundry Networks offers the security of certificate based authentication of the device used to access the network, adding a layer of security on top of the application or service credentials required to access the ePHI. This type of layered security model is a goal of modern security architectures to provide for the failure of any one control and still providing the required protection to the actual data assets being protected.

(2) *Implementation specifications:*

(i) *Unique user identification (Required).* Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required).* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

The programmability and software basis along with the agility of cloud based services allows multiple possible scenarios to be planned to extend the secure networking necessary, regardless of physical or Internet location. As this networking can be spun up in virtualized environments, public or private, this can significantly reduce the costs of capital procurement and ongoing maintenance of networking connections and hardware, as well as the difficulties of network design inherent in replicating services in multiple locations.

(iii) *Automatic logoff (Addressable).* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

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

For ePHI in motion, NetFoundry maintains high strength encryption across the path, with only customer owned systems having the necessary keys, and these keys being dynamic and ephemeral.

(b) *Standard: 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.

NetFoundry provides logs of the overall traffic usage, network configuration changes, endpoint online/offline status, and other events and metrics via the NetFoundry APIs. These can be extracted programmatically and placed into a SIEM, centralized logging

facility, or other systems to retain for audit, as well as to provide alerts and alarms to administrators or operators, as necessary.

(c)

(1) *Standard: Integrity.* Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).* Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

NetFoundry Networks offers the security of certificate based authentication of the device used to access the network, adding a layer of security on top of the application or service credentials required to access the ePHI. This type of layered security model is a goal of modern security architectures to provide for the failure of any one control and still providing the required protection to the actual data assets being protected.

(e)

(1) *Standard: 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.

For ePHI in motion, NetFoundry maintains high strength encryption across the path, with only customer owned systems having the necessary keys, and these keys being dynamic and ephemeral.

(2) *Implementation specifications:*

(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.

(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

For ePHI in motion, NetFoundry maintains high strength encryption across the path, with only customer owned systems having the necessary keys, and these keys being dynamic and ephemeral.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

Business Continuity Planning, Disaster Recovery, and other Administrative Controls

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)

(i) ***Standard: Security management process.*** Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) ***Implementation specifications:***

(A) ***Risk analysis (Required).*** 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 or business associate.

(B) ***Risk management (Required).*** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) ***Sanction policy (Required).*** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) ***Information system activity review (Required).*** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

NetFoundry provides logs of the overall traffic usage, network configuration changes, endpoint online/offline status, and other events and metrics via the NetFoundry APIs. These can be extracted programmatically and placed into a SIEM, centralized logging facility, or other systems to retain for audit, as well as to provide alerts and alarms to administrators or operators, as necessary.

(2) ***Standard: Assigned security responsibility.*** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3)

(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

The fine granularity of endpoint to service control of NetFoundry Networks, along with the ease of administration of endpoint groups and other features, allows for the creation of complex rights assignments in terms of access to the services. The programmatic nature of the APIs also allows for the automation, depending on job title or role, or other attributes as appropriate. The ease of assignment can also be very useful in temporarily assigning access for maintenance, audit, or other functions where there is no business need for the users to have consistent access.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision (Addressable).* Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) *Workforce clearance procedure (Addressable).* Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

In (A) through (C), NetFoundry can provide implementation assistance to all of these procedures. By allowing or disallowing access to the network service, NetFoundry can add a layer of protection for the critical ePHI assets. Particularly in (C), the immediate nature of NetFoundry can remove all access to the service through the removal of the endpoint from an endpoint group, or by script to remove it from all assets. This can be fully automated, or manual, as appropriate for the customer.

(4)

(i) *Standard: Information access management.* Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications:*

(A) *Isolating health care clearinghouse functions (Required).* If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization (Addressable).* Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

In (A) though (C), NetFoundry can provide implementation assistance to all of these procedures. By allowing or disallowing the access to the network service, NetFoundry can add a layer of protection for the critical ePHI assets. Particularly in (C), the immediate nature of NetFoundry can remove all access to the service through the removal of the endpoint from an endpoint group, or by script to remove it from all assets. This can be fully automated, or manual, as appropriate for the customer.

(5)

(i) *Standard: Security awareness and training.* Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications.* Implement:

(A) *Security reminders (Addressable).* Periodic security updates.

(B) *Protection from malicious software (Addressable).* Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring (Addressable).* Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management (Addressable).* Procedures for creating, changing, and safeguarding passwords.

(6)

(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

(ii) ***Implementation specification: Response and reporting (Required).*** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7)

(i) ***Standard: Contingency plan.*** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) ***Implementation specifications:***

(A) ***Data backup plan (Required).*** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) ***Disaster recovery plan (Required).*** Establish (and implement as needed) procedures to restore any loss of data.

(C) ***Emergency mode operation plan (Required).*** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

The programmability and software basis along with the agility of cloud based services allows multiple possible scenarios to be planned to extend the secure networking necessary, regardless of physical or Internet location. As this networking can be spun up in virtualized environments, public or private, this can significantly reduce the costs of capital procurement and ongoing maintenance of networking connections and hardware, as well as the difficulties of network design inherent in replicating services in multiple locations.

(D) ***Testing and revision procedures (Addressable).*** Implement procedures for periodic testing and revision of contingency plans.

(E) ***Applications and data criticality analysis (Addressable).*** Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) ***Standard: Evaluation.*** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)

(1) ***Business associate contracts and other arrangements.*** A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) ***Implementation specifications: Written contract or other arrangement (Required).*** Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

From <https://www.law.cornell.edu/cfr/text/45/164.308>

Business Associate Definition

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) ***Business associate*** includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) ***Business associate*** does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

From <https://www.law.cornell.edu/cfr/text/45/160.103>

Omnibus Rule 2013 Excerpt

"Regarding what it means to have “access on a routine basis’’ to protected health information with respect to determining which types of data transmission services are business associates versus mere conduits, such a determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to protected health information to perform the service for the covered entity. **The conduit exception is a narrow one and is intended to exclude only those entities**

providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to protected health information when it reviews whether the data transmitted over its network is arriving at its intended destination. Such occasional, random access to protected health information would not qualify the company as a business associate. In contrast, an entity that requires access to protected health information in order to perform a service for a covered entity, such as a Health Information Organization that manages the exchange of protected health information through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate. We intend to issue further guidance in this area as electronic health information exchange continues to evolve. We note that the conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission. In contrast, an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information. We recognize that in both situations, the entity providing the service to the covered entity has the opportunity to access the protected health information. However, the difference between the two situations is the transient versus persistent nature of that opportunity. For example, a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of "business associate'' to generally provide that a business associate includes a person who "creates, receives, maintains, or transmits'' (emphasis added) protected health information on behalf of a covered entity.