U.S. Health Insurance Portability and Accountability Act (HIPAA)

Covered Entity Compliance with HIPAA and Forcepoint Products

Forcepoint

Forcepoint Products Enable Subscriber Compliance with HIPAA

Overview

Forcepoint recognizes that its Subscribers are subject to various laws and regulations at the global, national, and local levels. One such national law that may apply to certain Forcepoint Subscribers in the United States healthcare industry is the U.S. Health Insurance Portability and Accountability Act (HIPAA). Mindful that such Subscribers are responsible for their own compliance with HIPAA requirements, including requirements to incorporate the minimum necessary standard to limit the use and disclosure of protected health information (PHI) and to maintain appropriate administrative, technical, and physical safeguards that protect against unauthorized uses and disclosures of PHI, Forcepoint has invested heavily to engineer successfully the principle of privacy by design and state of the art security features into its Product portfolio.

Succinctly stated: Forcepoint and Forcepoint Products do not require access to PHI. This includes both locally deployed, on-premises Software Products, such as Forcepoint DLP Suite (IP Protection), as well as Cloud Services, such as Forcepoint Web Security Cloud Services. Despite not requiring access to PHI and only processing certain limited types of personal data, Forcepoint Products can assist Subscribers in their compliance with their own legal and regulatory obligations under HIPAA. This guide is designed to provide insight into how Forcepoint Products and Forcepoint Published Materials, including Forcepoint's comprehensive Product End-User Agreements included with the Forcepoint Products, Data Processing and Protection Measures, and regularly audited and certified robust security policies and practices, support Subscribers in their achievement, maintenance, and demonstration of compliance with their own obligations under HIPAA.

Forcepoint Published Materials

More information on Forcepoint's commitment to data privacy and security, including Product Management of Personal Data materials, can be found in the Forcepoint Trust Hub available at: https://www.forcepoint.com/legal/forcepoint-trust-hub. In addition to other guides and materials that Forcepoint has available through the Forcepoint Customer Hub, Forcepoint has published on its public facing website:

- Forcepoint Product End-User Agreements ("FP EULA"): https://www.forcepoint.com/terms-and-conditions
- Forcepoint Data Processing and Protection Measures ("FP DPPM"): https://www.forcepoint.com/forcepoint-data-processing-agreement
- Forcepoint Data Processing Requirements ("FP DPR"): https://www.forcepoint.com/legal/data-privacy-requirements
- Forcepoint Privacy Policy: https://www.forcepoint.com/company/privacy-policy

Background on HIPAA

Ultimately designed to improve the United States health care system, HIPAA established minimum requirements for what were defined to qualify as a "covered entity," namely health plans, health care clearinghouses, and certain health care providers. HIPAA also included Administrative Simplification provisions requiring the U.S. Department Health and Human Services (HHS) to enact rules that standardize aspects of the health care system, including electronic health transactions and code sets, unique health identifiers, and security. As required under the Administrative Simplification provisions, HHS has repeatedly published and strengthened such rules since HIPAA was signed into law in 1996. This has included the HIPAA Privacy Rule in 2000, the HIPAA Security Rule in 2003, the HIPAA Enforcement Rule in 2006, the HITECH Act Enforcement Rule in 2009, and the Omnibus Rule in 2013.

The Omnibus Rule made several important modifications to the HIPAA Rules. It also provided much needed clarity on what is expected from covered entities in relation to their technology vendors and service providers, including the specialized subset of vendor known as a "business associate."

Business Associates

Prior to the Omnibus Rule, the HIPAA Rules defined "business associate" generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of PHI.

Among other modifications and clarifications, HHS used the Omnibus Rule to respond to public comments and requests for clarity and guidance on business associates and which technology vendors may qualify as a business associate. Notably, through the Omnibus Rule:

- expanded the definition of business associate to include "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 routine access to such protected health information,"
- explained what it means to have "access on a routine basis" to PHI, and
- clarified the conduit exception/exclusion from qualifying as a business associate.

"Access on a routine basis"

In the Omnibus Rule, HHS made clear that determining whether a service provider has access to PHI on a routine basis "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 to the covered entity." Thus, determining business associate status is to be fact intensive and based on whether and to what degree the service provider requires access to PHI to perform its service. Those that require regular, recurring, and routine access to PHI to perform the purchased service would most likely qualify as a business associate whereas those with only occasional, infrequent, random, temporary, or transient access to PHI incidental to the purchased service would not.

As specified in the Omnibus Rule: "data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates." HHS elaborated further: "In contrast, entities that manage the exchange of protected health information through a network, including providing record locator services and performing various oversight and governance functions for the electronic health information exchange, have more than 'random' access to protected health information and thus, would fall within the definition of 'business associate.'"

The Conduit Exception

HHS also created an exclusion from the definition of business associate, known as the "conduit exception." In the Omnibus Rule, HHS restated its definition of a conduit as a service provider that "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." Notably, HHS clarified 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."

For additional clarity, HHS provided contrasting illustrative examples: "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, HHS offers the example of a vendor hired to provide the service 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." As the latter vendor requires regular, routine access to PHI to perform its service of managing the exchange of PHI through the network, it would likely not qualify for the conduit exception and instead fall within the definition of business associate.

Application to Forcepoint Products

As noted above, Forcepoint and Forcepoint Products do not require access to PHI. This includes both locally deployed, on-premises Software Products, such as Forcepoint DLP Suite (IP Protection), as well as Cloud Services, such as Forcepoint Web Security Cloud Services. Using these two Products as examples, Forcepoint has provided information below on how Forcepoint Products and Published Materials, including the FP EULA, FP DPPM, and regularly audited and certified robust security policies and practices, can be used to support Subscribers in their achievement, maintenance, and demonstration of compliance with their own obligations under HIPAA.

<u>Example 1: Forcepoint DLP Suite (IP Protection)</u>

- Nature of Product: Designed to prevent data loss through data policy management and enforcement
- Available deployment: local, on-premises
- Applicable FP EULA: Forcepoint Subscription Agreement

- Applicable Management of Personal Data PDF: Data Loss Prevention

Forcepoint DLP Suite (IP Protection) is locally deployed, on-premises within the Subscriber's network, and does not leverage the Forcepoint Cloud Services infrastructure. As a result, in provisioning Forcepoint DLP Suite (IP Protection), Forcepoint does not require and would not receive any access to personal data or PHI, let alone require routine access to PHI to qualify as a business associate. More information on the fundamental operations of Forcepoint DLP Suite (IP Protection) can be found in the applicable Forcepoint Product Documentation and Management of Personal Data PDF. Even so, any inadvertent disclosures would remain subject to the protections of the applicable FP EULA, including the mutual protections for Confidential Information (see Section 7.1) and the FP DPPM (see Section 13) that incorporates Forcepoint's ISO 27001 certified technical and security measures.

Example 2: Forcepoint Web Security Cloud Services

- Nature of Product: Designed to safeguard web browsing and provide visibility and control over web data and traffic
- Available deployments: Cloud Services; hybrid
- Applicable FP EULA: Forcepoint Subscription Agreement
- Applicable Management of Personal Data PDF: Web Security – Cloud

Unlike Forcepoint DLP Suite (IP Protection), Forcepoint Web Security Cloud Services does leverage the Forcepoint Cloud Services infrastructure. As a result, while Forcepoint Web Security Cloud Services does not require any access to PHI, there are certain limited types of personal data, some optional and others mandatory, that Forcepoint Web Security Cloud Services may process. Details on such limited types of personal data and the temporary, configurable retention periods associated with such data can be found in the applicable Forcepoint Product Documentation and Management of Personal Data PDF. In light of the nature of the Product and the limited types of personal data necessary to operate, it is not anticipated that Forcepoint Web Security Cloud Services will process PHI. However, in the event that PHI is processed by Forcepoint Web Security Cloud Services (e.g., User trips Subscriber configured policy resulting in temporary logging of associated event metadata), such processing would be incidental to the nature of the Product, would infrequently and occasionally occur based on Subscriber's configured policies, and is designed to provide Subscriber with the temporary means to verify that configured policies are being applied to User behaviors and Users are arriving at their authorized and intended destinations. Thus, in provisioning Forcepoint Web Security Cloud Services, Forcepoint may process certain limited types of personal data but does not require any access to PHI, let alone require routine access to PHI to qualify as a business associate. Further, any access to PHI should be understood as incidental to the nature of Forcepoint Web Security Cloud Services and random, infrequent, and occasional, all as described through the conduit exception. Even so, any incidental or inadvertent disclosures would remain subject to the protections of the applicable Forcepoint EULA, including the mutual protections for Confidential Information (see Section 7.1) and the FP DPPM (see Section 13) that incorporates Forcepoint's ISO 27001 certified technical and security measures.

Note that Forcepoint does make local, on-premises deployments available for Forcepoint Web Security that do not leverage the Forcepoint Cloud Services infrastructure. To clarify, in provisioning Forcepoint Web Security in such a local, on-premises deployment, Forcepoint would not receive any access to personal data or PHI.

More Information

For more information on Forcepoint Products, including Forcepoint Product Documentation, please visit the Forcepoint Customer Hub. More information on Forcepoint's commitment to data privacy and security, including Product Management of Personal Data materials, can be found in the Forcepoint Trust Hub available at: https://www.forcepoint.com/legal/forcepoint-trust-hub.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[Forcepoint U.S. HIPAA] 21 Apr. 25