The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Frequently Asked Questions (FAQs)

At Salesforce, Trust is our #1 value and the protection of our customers’ data is paramount. We know that many organizations in the healthcare and life sciences industries have questions about their obligations under HIPAA and the HITECH Act. To help you develop a better understanding of how HIPAA and the HITECH Act apply to your organization’s potential use of Salesforce’s online services that are covered by our Business Associate Addendum (our “BAA”), we have outlined the most common questions asked.

Overview

This document provides answers to frequently asked questions about Salesforce’s online services that: (1) are covered by our BAA (which are called “HIPAA Covered Services”); and (2) can be used by organizations that need to comply with HIPAA. This document does not provide legal advice and the information we present may not take into account future changes in laws and regulations. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

What services does Salesforce offer?

Salesforce is the leading provider of enterprise cloud computing technologies. ‘Cloud computing’ is a broad term but generally denotes a range of IT services provided in various formats through social, mobile and open technologies.

Salesforce enables companies to place their customers at the heart of their business and engage with them in new and powerful ways. Salesforce services include customer relationship management (CRM), collaboration, and social media monitoring for businesses of all sizes. Salesforce also provides platforms to build and run business applications without having to invest in new software, hardware, or related infrastructure. More information on the types of products and services that Salesforce offers can be found on the [Salesforce website](https://www.salesforce.com).

How does Salesforce deliver its services?
Salesforce generally delivers its services via the Internet. Customers log into Salesforce’s services through a website using unique usernames and passwords. Salesforce’s services allow for various additional authentication methods that may be activated by customers, as appropriate to their needs, such as two-factor authentication and IP range restrictions. We also serve our customers through what is known in the industry as cloud-based services architecture, which is designed for security, efficiency, availability, scalability, and rapid innovation.

**What is HIPAA? Who is subject to HIPAA?**

HIPAA, as amended by the HITECH Act, is a broad healthcare law that regulates matters ranging from allowing workers to transfer their health insurance coverage to standardizing healthcare information for electronic medical billing. However, HIPAA is best known for requiring the US Department of Health and Human Services (HHS) to issue rules to protect the privacy and security of certain individually identifiable health information. This information is called “protected health information.”

HHS has issued three main rules under its HIPAA authority. First, the HIPAA Privacy Rule governs the use and disclosure of protected health information primarily by entities regulated under HIPAA. These entities are called “covered entities.” Second, the HIPAA Security Rule specifies safeguards for protecting the confidentiality of electronic protected health information. Third, the HIPAA Breach Notification Rule requires notification following the occurrence of a breach of unsecured protected health information. These rules apply to covered entities, which include health plans, health care clearinghouses, and most healthcare providers. Parts of the HIPAA Privacy and Breach Notification Rules, and most of the HIPAA Security Rule, also apply to service providers of covered entities that store or have access to protected health information. These service providers are called “business associates.”

**Is Salesforce subject to HIPAA?**

Yes, we are subject to HIPAA as a business associate of our customers that are HIPAA-regulated covered entities or business associates and that choose to: (1) enter into a BAA with us; and (2) submit protected health information to the HIPAA Covered Services. Data submitted to our services by customers is called “Customer Data.” Additionally, as further described below, through our BAA we enter into contractual arrangements with some of our customers that include HIPAA-related provisions.

**Do we comply with HIPAA?**

Yes, with respect to the HIPAA Covered Services. In provisioning and operating the HIPAA Covered Services, we comply with the required provisions of HIPAA and the HITECH Act that apply to business associates.

**How do we comply with the HIPAA Privacy Rule?**

We comply with the provisions of the HIPAA Privacy Rule that apply to business associates by not using or disclosing Customer Data that includes protected health information subject to HIPAA, other than: (1) to provide the HIPAA Covered Services and prevent or address service or
technical problems; (2) in connection with customer support matters; or (3) as required by law. However, HIPAA does not subject us to all of a covered entity’s obligations under the HIPAA Privacy Rule. Instead, as a business associate, our obligations under the HIPAA Privacy Rule are still largely determined by the terms of our agreements with our covered entity and business associate customers. In particular, in our BAA, we contractually commit to our customers that we will comply with the foregoing restrictions on the use and disclosure of Customer Data that includes protected health information submitted by them to the HIPAA Covered Services.

**How do we comply with the HIPAA Security Rule?**

We comply with the provisions of the HIPAA Security Rule that apply to business associates by protecting Customer Data, including protected health information, through the use of robust administrative, technical, and physical safeguards.

These administrative safeguards include, but are not limited to:

- Comprehensive information security and privacy policies designed to meet the requirements of ISO 27001 and to reflect our contractual commitments to safeguard Customer Data and satisfy applicable regulatory requirements.
- Designated professionals and departments: (1) led by our Security organization, which is responsible for Salesforce’s security program; and (2) augmented by our Legal Department, which is responsible for Salesforce’s privacy program.
- Limiting access to Customer Data, including protected health information, to personnel who require such access to perform our contractual obligations.
- Providing training on information security and confidentiality: (1) during new hire orientation seminars that new employees must attend following their hiring, and (2) annually for our personnel who could potentially access Customer Data, after which they must pass an associated quiz.

These technical safeguards include, but are not limited to:

- Encrypting Customer Data by default, including protected health information, during transmission.
- Logical network security safeguards, including network and system access restrictions.
- Authentication requirements to ensure that only authorized personnel may access systems containing Customer Data, including protected health information.

These physical safeguards include, but are not limited to:

- Facility access controls for our offices and data centers.
- Workstation policies that require personnel to store confidential information in secure locations, unattended workspaces to be secured, screens of unattended computers to be locked, and portable computer disk drives to be fully encrypted.
- For data centers, additional security standards for physical and environmental security, including physical authentication of personnel before Salesforce infrastructure in those data centers may be accessed.
How do we comply with the breach notification provisions of the HITECH Act?

As a business associate, we comply with the breach notification provisions of the HITECH Act by complying with commitments in our BAA to notify affected customers of any breaches of Customer Data that includes protected health information within the legally mandated period of time.

How do we address encryption under HIPAA?

Under the HIPAA Security Rule, the technical standards for access control and transmission security that deal with encryption include implementation specifications that are “addressable” rather than “required.” This means that HIPAA does not impose specific legal requirements for encrypting protected health information stored at rest or while in transmission. However, HHS has provided guidance on compliance with the HIPAA Security Rule regarding these addressable implementation specifications.

With respect to “in-transit” encryption, the HIPAA Covered Services enable Transport Layer Security (TLS), by default, to provide privacy and data integrity between two communicating applications. TLS is the most widely deployed security protocol used today, and is used for web browsers and other applications that require data to be securely exchanged over a network. TLS ensures that a connection to a remote endpoint is the intended endpoint through encryption and endpoint identity verification. With respect to “at rest” encryption, some HIPAA Covered Services also offer customers the ability to encrypt stored data. For more information on enabling encryption in certain HIPAA Covered Services, customers should refer to the service configuration documentation for their particular HIPAA Covered Services or contact their Salesforce account executive.

If a customer encrypts Customer Data that includes protected health information, do individuals have to be notified under HIPAA if a breach of that data occurs?

HIPAA does not impose specific legal requirements for encrypting protected health information that is stored at rest or while such information is in transmission. However, HHS has provided guidance on encryption standards that, if met, would exempt HIPAA-regulated entities from having to provide notice under the HIPAA Breach Notification Rule if a breach of protected health information occurs. We encourage our customers to seek legal counsel to help determine whether the encryption options available through their implementation of the HIPAA Covered Services can help address these compliance requirements. Customers should also contact their Salesforce account executive if they are interested in discussing the encryption options available through their particular HIPAA Covered Services in more detail.

Do we enter into BAAs with our customers?

Yes. For customers that: (1) are subject to HIPAA as covered entities or business associates; and (2) submit protected health information to the HIPAA Covered Services as Customer Data, we have developed our standardized BAA that satisfies the HIPAA requirements and is tied to the particular services we offer as well as to our master subscription agreement. Among other things, our BAA:
● Sets forth restrictions on the use and disclosure by us of Customer Data that includes protected health information.
● Requires us to sign BAAs with downstream “subcontractors” that are also business associates.
● Includes a commitment by us to comply with the HIPAA Security Rule with respect to safeguarding electronic protected health information.
● Requires notification of breaches and unauthorized uses or disclosures of protected health information.

Can customers comply with HIPAA through use of the HIPAA Covered Services?

We offer our customers a broad array of security features that they can implement in connection with their use of the HIPAA Covered Services. Our product and service features provide our customers with flexibility when complying with stringent security requirements such as those mandated by HIPAA.

Importantly, our customers should be aware that while we comply with HIPAA in provisioning and operating the HIPAA Covered Services as a business associate, it is the sole responsibility of our customers to ensure their compliance with applicable laws concerning their particular use of the HIPAA Covered Services. In particular, when using the HIPAA Covered Services, our customers must use and disclose protected health information only as permitted by HIPAA and ensure that their security settings are appropriately configured.