Salesforce and the HIPAA Security Rule
SECURING ePHI IN THE CLOUD
NOTE:

The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act, are collectively referred to herein as “HIPAA.”

Laws and regulations and how they are interpreted and enforced by courts and governmental authorities sometimes vary, including by size of customer, industry, territory, or jurisdiction and may change over time. This white paper is designed to be a broad overview and is not legal advice, and we urge you to consult with your own counsel to familiarize yourself with the requirements that govern your specific situation. Salesforce complies with the provisions of the HIPAA Security Rule that are required and applicable to it in its capacity as a business associate in providing and operating the Salesforce Services. However, it is the sole responsibility of Salesforce’s HIPAA-regulated Customers to ensure compliance with HIPAA and other applicable laws and regulations in their particular use of the Salesforce Covered Services.

Patients place their trust in the healthcare industry and expect their providers of healthcare and coverage to be good stewards of their health information, including addressing standards set forth by HIPAA to protect the privacy and security of protected health information where applicable. Salesforce recognizes the value and importance of HIPAA to the industry and patients, and takes our compliance with it seriously.

In this white paper, we will outline some of the HIPAA Security Rule’s standards for protecting electronic protected health information (ePHI), and introduce how some features of Salesforce’s Services may help customers keep ePHI secure in the cloud.

This white paper covers ePHI that is submitted by customers that: (1) are HIPAA covered entities or business associates; and (2) have entered into a Business Associate Addendum (“BAA”) with Salesforce (referred to herein as “HIPAA-regulated Customers” or “HIPAA-regulated Entities”) to Salesforce’s online services branded as Health Cloud, Lightning Platform (including Force.com, but excluding Lightning Platform Developer Edition), Sales Cloud, Service Cloud, Community Cloud, Site.com, Database.com, Chatter, Einstein Analytics, and IoT Explorer (the “Salesforce Covered Services”).
Standards for Protecting Electronic Protected Health Information Under the HIPAA Security Rule

In this white paper, we will focus on ePHI (as defined under HIPAA) to the extent that it is submitted by Salesforce’s HIPAA-regulated Customers to the Salesforce Covered Services.

ePHI (subject to certain exclusions) means information transmitted by or maintained in electronic media that:

- Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual
- Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual

The HIPAA Security Rule is designed to protect the confidentiality, integrity, and availability of ePHI, and provides a framework of standards and implementation specifications that require covered entities and business associates to establish policies, procedures, and technology practices. In particular, the HIPAA Security Rule details a number of requirements for administrative, physical, and technical safeguards, along with organizational and documentation requirements.

How Features and Functionality of the Salesforce Covered Services Help Customers Keep ePHI Secure in the Cloud

At Salesforce, trust is our number one value. Many of our customers operate in regulated industries of financial services, government, military, and, of course, healthcare. Earning the trust of our customers in the healthcare and life sciences industries requires that we address the safeguards and requirements outlined by the HIPAA Security Rule.
With respect to providing and operating the Salesforce Covered Services, Salesforce complies with the provisions of the HIPAA Security Rule that are required and applicable to it in its capacity as a business associate. In addition, Salesforce also provides customers with customer-controlled security features in the Salesforce Covered Services, which may help HIPAA-regulated Customers address stringent security requirements.

**CORE SECURITY SAFEGUARDS AND FEATURES**
Salesforce contributes to keeping ePHI secure in the Salesforce Covered Services by implementing security safeguards that apply to all customers by default such as:

- Continually monitoring the services for security violations
- Encrypting all data in transit
- Storing user passwords in the SHA-256 one-way hash format
- Enabling audit logging that allows system administrators to track certain change activity in the Salesforce Covered Services
- Providing customer administrators with configurable tools to maintain strict password security policies which govern access
- Providing customer administrators with configurable tools to define user profiles and permission sets governing data visibility
- Providing customer administrators with configurable tools to define a company-wide sharing model, a role hierarchy, and security rules governing data access
- Providing customer administrators with configurable tools for field level history monitoring and retention

Each customer instance of its Salesforce Covered Services application
(e.g., Lightning Platform (including Force.com), Sales Cloud, Service Cloud, Health Cloud, etc.) is deployed in one of our data centers or securely served from our public cloud infrastructure. The Salesforce Covered Services infrastructure is continually monitored by dedicated operations teams for anomalies, penetration attempts, denial of service attacks, and so on. End-to-end Transport Layer Security (TLS) encrypts transactions between the customer and the Salesforce Covered Services by default. Customers may also implement safeguards if they integrate their implementation of the Salesforce Covered Services with external systems. For example, Salesforce enables the option to leverage mutual authentication for external connections.

Additionally, customer administrators have the ability to easily configure strict password policies. For example, they can dictate that passwords must be a minimum length, with a measure of complexity, and must be rotated periodically. Further, Salesforce managed passwords are hashed with a 256-bit one-way function. If, however, a customer prefers to implement single sign-on (SSO), the customer may rely on a trusted identity provider and configure Federated Single Sign-On using SAML to leverage its own authentication mechanism.

It is important to limit users’ access to data such that they are granted access only to those data records they will need to perform their job function. Administrators can leverage the Profile and Permission Set security constructs to control access to aspects of the user experience like data objects, fields, and application functions like Manage Cases, Create and Customize Reports, or View Encrypted Data. Data record-level access can be managed via a combination of security constructs like Organization-Wide Sharing Settings and Sharing Rules. Leveraging the User Role Hierarchy grants managers the data-level visibility they need to manage their team.

**ENHANCED SECURITY FEATURES — SALESFORCE SHIELD**
Salesforce offers a premium set of features built natively on the Lightning Platform (including Force.com) that customers with complex security, governance, and compliance needs can choose to leverage. These services — Field Audit Trail, Event Monitoring, and Platform Encryption — are available via the Salesforce Shield product offering. For more information about our Salesforce Shield product offering, please refer to the Salesforce Shield for Healthcare white paper.
FIELD AUDIT TRAIL
Field Audit Trail can enable a customer to review the historical state and value of their data. This customer-controlled feature expands what is currently available to a customer via the Field History Retention feature, and has the ability to give a customer up to ten years of audit trail data for up to sixty fields per object.

The field audit trail functionality could be helpful, for example, to a customer engaged in forensic analysis of data (including responding to a data audit or engaging in a data breach investigation).

EVENT MONITORING
Event Monitoring gives customers visibility into what data users are accessing, from what IP address, and what actions are being taken in regards to that data. Customers utilizing this feature can access a standard CSV (comma-separated-value) file via API (application program interface) and can pull the data into any number of visualization tools (including, for example, Einstein Analytics and other third party tools). This feature could enable a customer to track when a page or list view is printed, a record is edited or created, ownership of a record is changed, a list is refreshed, or even when a user exports data. Event Monitoring may be helpful to a customer with regard to responding to data audits. Together with Event Monitoring, Transaction Security — a framework that intercepts a subset of real-time Salesforce events (e.g., logins, data exports, report access) — can be leveraged to apply appropriate actions like requiring a second factor of authentication, blocking the action entirely and/or notifying an administrator based on security policies you create.

PLATFORM ENCRYPTION
Platform Encryption enables a customer using this feature to encrypt data (that is submitted to the Salesforce Covered Services) at rest while maintaining important application functionality—(i.e., search, validation, workflow, etc.). Given that data is encrypted at the metadata layer in the database, key Salesforce application functionality can be made “encryption aware” and work despite the data being encrypted. Platform Encryption is built natively into the platform. With Platform Encryption, customers may be able to render sensitive data unreadable by unauthorized persons.

Conclusion
The trust and success of our customers are the highest priorities for Salesforce. In provisioning and operating the Salesforce Covered Services, Salesforce complies with the provisions of the HIPAA Security Rule that are required and applicable to it in its capacity as a business associate (to the extent that its customers are HIPAA-regulated Entities and choose to submit ePHI to the Salesforce Covered Services following their signing of a BAA with Salesforce). As discussed in this white paper, Salesforce also offers customer-controlled security features that may be implemented by customers in their respective uses of the Salesforce Covered Services. These features can serve as a set of tools to help its customers address certain security requirements, such as portions of the HIPAA Security Rule.