Confidential: Subject to Non-Disclosure Agreement
August 2015

Privacy and Data Protection
Questions and Answers for Salesforce Customers:

HIPAA AND HITECH ACT

The information provided in this document is for your use as you evaluate whether to purchase services branded as Force.com, Sales Cloud, Service Cloud, Communities, Site.com, Database.com, and Chatter from Salesforce (the "Salesforce Services"). We have tried to answer many broadly-applicable questions that many customers and prospective customers have asked us. Laws and regulations and how they are interpreted and enforced by courts and governmental authorities sometimes vary by size of customer, industry, territory, or jurisdiction within a country and may change over time. This document is a broad overview and not legal advice, and we urge you to consult with your own counsel to familiarize yourself with the requirements that govern your specific situation.

What services does Salesforce offer?

Salesforce provides an Internet-based business application (also known as "software-as-a-service" or "enterprise cloud computing") that allows its customers to input, store, and access data about their customers and prospective customers. The Salesforce Services provide comprehensive customer relationship management ("CRM") functionality that include sales force automation, customer support and help desk, and marketing automation features in addition to an on-demand technology platform that enables Salesforce's customers and partners to build and sell entirely new on-demand applications without having to invest in new software, hardware, or related infrastructure.

How does Salesforce deliver its services?

Salesforce delivers the Salesforce Services over the Internet through commercially available Web connections and browser software. Customers log into the Salesforce Services from Salesforce's Web site using a unique username and password. The Salesforce Services allow for additional authentication methods that may be activated by customers, and we encourage customers to implement two-factor authentication or IP range restrictions.

Salesforce serves its customers through secure hardware and software, using what is known in the industry as "multi-tenant" application architecture. A multi-tenant application is one that can be accessed and used by many users simultaneously, with logical separation of data in hardware and software. The logical separation of data allows each Salesforce customer to view only its "instance" of the Salesforce Services and associated data. Salesforce's multi-tenant architecture is similar to that used to provide online banking and brokerage services to consumers (which can also be accessed and used by thousands of users simultaneously through the logical – not physical – separation of data).

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a broad healthcare law that authorizes the U.S. Department of Health and Human Services ("HHS") to promulgate rules to address the privacy and security of individually identifiable health information (known in HIPAA as "protected health information"). HHS has issued three rules in particular under its HIPAA authority: (i) the "Standards for Privacy of Individually Identifiable

Health Information" (commonly known as the "Privacy Rule") governs the use and disclosure of protected health information primarily by covered entities; (ii) the "Health Insurance Reform: Security Standards" (commonly known as the "Security Rule") sets forth safeguards required to protect the confidentiality of electronic protected health information; and (iii) the rule for Breach Notification for Unsecured Protected Health Information (commonly known as the "Breach Notification Rule") requires notification following a breach of unsecured protected health information.

In February 2009, HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") provisions of the American Recovery and Reinvestment Act of 2009 (also known as "ARRA") to strengthen and expand the scope of the HIPAA Privacy and Security Rules, enhance HIPAA's civil and criminal penalties, permit U.S. state attorneys general to enforce HIPAA, and require HIPAA covered entities to notify individuals in the case of breaches of individually identifiable health information. Additionally, the HITECH Act makes some sections of the Privacy Rule and most of the Security Rule directly applicable to service providers of covered entities that have access to or store protected health information ("business associates").

What is the Final Rule?

In January 2013, HHS promulgated the Final Rule, 78 Fed. Reg. 5566, under authority granted to it by the HITECH Act. The Final Rule amended HIPAA and, in particular, the Privacy, Security, and Breach Notification Rules. Generally speaking, however, the Final Rule essentially implements a previously proposed rule from July 2010 without significant amendments, although there are a few exceptions such as the requirements around breach notification (see below).

Who is subject to HIPAA?

HIPAA applies directly to "covered entities," which HIPAA defines as health plans, health care clearinghouses, and health care providers who transmit any health information in connection with certain types of transactions. Under the HITECH Act, certain provisions of HIPAA also apply to "business associates" or service providers of covered entities that have access to or store protected health information.

Is Salesforce subject to HIPAA?

Yes, with respect to those of its customers in the health care industry that are HIPAA covered entities or business associates and choose to submit protected health information to the Salesforce Services ("Customer Data"). Additionally, as further described below, Salesforce enters into contractual agreements with some of its customers that include HIPAA-related provisions.

Does Salesforce comply with HIPAA?

Yes, with respect to the Salesforce Services. In provisioning and operating those services, Salesforce complies with the provisions of HIPAA and the HITECH Act that are required and applicable to business associates.

How does Salesforce comply with the Privacy Rule?

Salesforce complies with provisions of the Privacy Rule applicable to business associates by not

using or disclosing Customer Data, including protected health information subject to HIPAA, other than to (i) provide the Salesforce Services and prevent or address service or technical problems; (ii) in connection with customer support matters; or (iii) as required by law. The Final Rule does not subject Salesforce to all of a covered entity's obligations under the Privacy Rule. Rather, business associates' obligations under the Privacy Rule are still largely determined by the terms of its agreements with the covered entity. Salesforce contractually commits to the foregoing restrictions on the use and disclosure of Customer Data to all of its customers for the Salesforce Services.

How does Salesforce comply with the Security Rule?

Salesforce complies with provisions of the Security Rule applicable to business associates by protecting all Customer Data, including protected health information, using robust administrative, technical, and physical safeguards.

Salesforce's administrative safeguards include:

- comprehensive information security and privacy policies designed to meet the requirements of ISO 27001 and to reflect Salesforce's contractual commitments to safeguard Customer Data and regulatory requirements;
- designated professionals and departments, led by the Chief Trust Officer, who is responsible for Salesforce's security program, and augmented by the Assistant General Counsel, Global Privacy, who is responsible for Salesforce's privacy program;
- limiting access to Customer Data, including protected health information, to personnel who require such access to perform Salesforce's contractual obligations; and
- providing classroom training on information security and confidentiality during monthly new hire orientation seminars all employees must attend upon hire and an annual information security and privacy awareness training that requires personnel to pass an associated quiz.

Salesforce's technical safeguards include:

- encrypting all Customer Data, including protected health information, during transmission;
- logical network security, including stateful firewalls and intrusion detection systems;
- robust authentication requirements to ensure that only authorized personnel may access systems containing Customer Data, including protected health information; and
- strong multi-tenant application security to ensure that only authorized users may login to the Salesforce Services and access data they have permission to access.

Salesforce's physical safeguards include:

- facility access controls for all Salesforce 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 all portable computers disk drives fully encrypted;
- and data center security standards that are on par with the leading civilian data centers in the world, such as five levels of biometric scanning before Salesforce's cages may be accessed.

Is there an encryption requirement under HIPAA?

The technical standards for access control and transmission security in the Security Rule dealing with encryption set forth implementation specifications that are what are known as "addressable" as opposed to "required". This means that HIPAA does not impose specific legal requirements for encrypting protected health information stored at rest or in transmission. HHS has provided guidance on compliance with the Security Rule with respect to addressable implementation specifications. In addition, if you are interested in finding out more about the Salesforce Services' encryption offerings, including Classic Encrypted Custom Fields and Platform Encryption, please speak with an account executive.

How does Salesforce comply with the breach notification provisions of the HITECH Act?

Salesforce complies with the breach notification provisions of the HITECH Act by agreeing in its business associate addendums to notify affected customers of unauthorized use or disclosure of Customer Data constituting protected health information within the statutorily mandated period of time.

If a customer uses the Classic Encrypted Custom Fields feature or the Platform Encryption product to encrypt Customer Data constituting protected health information, does it have to notify individuals of a breach of that data under HIPAA?

Note that HIPAA does not impose specific legal requirements for encrypting protected health information stored at rest or in transmission. However, the Department of Health and Human Services has provided some guidance on encryption standards that, if met, would exempt HIPAA-regulated organizations from having to notify of breaches of such information under the HIPAA Breach Notification Rule. We encourage you to seek legal counsel to help determine whether the Classic Encrypted Custom Fields feature or the Platform Encryption product, each of which is customer-controlled, can help address these compliance requirements given your organization's particular implementation of the Salesforce Services. Please speak with an account executive if you are interested in discussing the Classic Encrypted Custom Fields feature or the Platform Encryption product in more detail.

Does Salesforce enter into HIPAA business associate addendums with its customers?

Yes. For customers that are subject to HIPAA and submit protected health information to the Salesforce Services as Customer Data, Salesforce has a HIPAA business associate addendum that complies with HIPAA, including the new requirements under the HITECH Act and the Final Rule.

Can Salesforce's customers comply with HIPAA in using the Salesforce Services?

Yes. Salesforce offers its customers a broad spectrum of customer-controlled security features that its customers may implement in their respective uses of the Salesforce Services, for example, user permissions and access settings to specify what users can do within an organization, encryption of certain Customer Data at rest via Classic Encrypted Custom Fields and Platform Encryption, and logging and auditing features to monitor the security and user activity of your instance of the Salesforce Services (e.g., Field Audit Trail, Event Monitoring). Salesforce believes that these features provide its customers the flexibility to comply with stringent security requirements, such as HIPAA. Additional information about Salesforce's customer-controlled security features, including the Security Implementation Guide, is available to customers after logging into the Salesforce Services in the "Help & Training" portal.

Please note that while Salesforce complies with HIPAA in provisioning and operating the Salesforce Services, it is the sole responsibility of Salesforce's customers to ensure compliance with applicable laws in their particular use of the Salesforce Services.