FinancialForce and the HIPAA Security Rule

Introduction

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 the privacy and security standards in the U.S. Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations (collectively "HIPAA"). FinancialForce.com, inc. ("FinancialForce") 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 describe how some features of the FinancialForce online services may help customers keep ePHI secure in the cloud. The scope of this white paper is limited to ePHI that is submitted by customers that are HIPAA covered entities or business associates to FinancialForce's online Financial Management, Professional Services Automation (PSA), and Human Capital Management (HCM) applications ("FinancialForce Applications").

This white paper is intended to be a general overview of FinancialForce online service features and controls relevant to the HIPAA Security Rule, and does not contain legal advice or any contractual warranty or representation. If you are considering using FinancialForce Applications for ePHI, you should consult with a qualified expert to assess whether and how FinancialForce Applications can apply to your HIPAA compliance requirements in light of your data, environment and business processes, and to determine the most appropriate configuration of the FinancialForce Applications. FinancialForce and its platform provider, Salesforce, adhere to the provisions of the HIPAA Security Rule applicable to them in their capacity as business associates in providing the FinancialForce online services, but our customers ares solely responsible for their compliance with HIPAA in using the FinancialForce Applications.

About FinancialForce

FinancialForce provides Financial Management, Professional Services Automation (PSA), and Human Capital Management (HCM) applications. FinancialForce Applications are built and run on the Force.com platform, a cloud computing platform provided by Salesforce.com, inc. and its subsidiaries (collectively "Salesforce"). FinancialForce is headquartered in San Francisco, California, and has major offices in the United States, the United Kingdom, Spain, Canada and Australia. Founded in 2009, FinancialForce is backed by Salesforce, Technology Crossover Ventures, Unit4 and Advent International.

Standards for Protecting ePHI 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 FinancialForce's HIPAA-regulated Customers to the FinancialForce Applications. 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; and
- 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.

FinancialForce Security Overview

FinancialForce Applications are designed based on core information security principles:

- *Confidentiality* - Prevent the disclosure of information to unauthorized individuals or systems.
- *Integrity* - Maintain and assure the accuracy and consistency of data over its entire lifecycle.
- *Availability* - Ensure the information is available when needed.

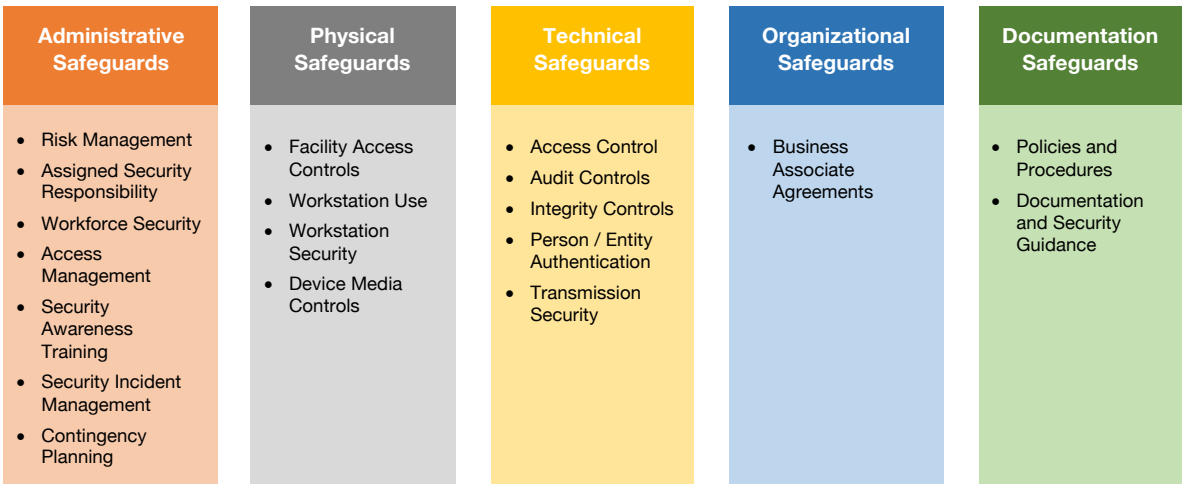
We view our commitment to these principles as fundamental to maintaining the trust of our customers. This commitment is embodied in our security and privacy program, which is designed to provide a range of safeguards for our customers' data across the FinancialForce Applications.

Information Security Program

FinancialForce has a dedicated Security and Trust function that coordinates security policy, program and verification efforts, to help ensure that appropriate protections are in place for customer and company information assets. Our Information Security Program includes policies and controls to identify, evaluate and report on security risks; comply with security and privacy regulations and commitments; address threats and vulnerabilities; and manage and respond to security incidents. Our Information Security Policy and Standards framework, based on ISO 27001/27002, describes standards, best-practice guidelines and approaches required to protect data entered into FinancialForce Applications by our customers ("Customer Data") as well as corporate information assets. For more details in our security practices please review our Security Whitepaper and visit our Trust site.

How FinancialForce Services Help Customers Keep ePHI Secure in the Cloud

FinancialForce complies with all requirements under the HIPAA Security Rule that apply to FinancialForce in its capacity as a business associate. In addition, FinancialForce Applications provide customer-controlled security features that can help our customers address their individual security and compliance requirements under HIPAA.



Administrative Safeguards

Risk Management

FinancialForce's process for identifying, assessing and managing risks is a critical component of our internal control system. FinancialForce has a Security Risk Committee, comprised of a cross-functional group of business representatives, dedicated to identifying, evaluating and addressing information security risk across FinancialForce and its products and services. The Security Risk Committee meets quarterly to evaluate existing and emerging risks, monitor progress against remediation plans, and re-adjust as appropriate. The Security Risk Committee reports up to our Risk Management Committee, comprised of senior executives and function heads. The Risk Management Committee meets quarterly to identify, evaluate and address the full range of risks to the business, and monitor the operation of the company's internal controls.

Customers are responsible for risk assessment in their own operations, including their use of FinancialForce Applications and services, and the data they upload into the FinancialForce Applications.

Sanction Policy

FinancialForce has a Code of Conduct adopted by the Board Directors, as well as information security policies adopted by management, which provide for sanctions for violations. FinancialForce employees who violate the Code of Conduct, an information security policy, or any law may be subject to disciplinary action by FinancialForce including, without limitation, warnings, reprimands, temporary suspensions, probation or termination of employment. Suspected criminal behavior may be referred to a law enforcement agency.

Information System Activity Review

FinancialForce Applications are hosted on Salesforce's Force.com platform. All systems used in the provision of the FinancialForce Applications - including firewalls, routers, network switches and operating systems - log information to their respective system log facility or, in the case of network systems, to a centralized syslog server. Salesforce provides several types of audit logs for monitoring logins and changes to a customer's Salesforce instance ("Org"), including, for example, user login history and object history tracking. These audit features can be configured, and the logs can be viewed, by the Salesforce administrator assigned by the customer to administer the FinancialForce Applications.

Assigned Security & Compliance Responsibility

FinancialForce's Senior Vice President and General Counsel acts as the company's Compliance Officer. As part of this role, the General Counsel is responsible for communication, training, and monitoring of, and overall compliance with, the Code of Conduct. The General Counsel, with the support and cooperation of the FinancialForce directors, officers, and managers, seeks to foster an atmosphere where employees and service providers are comfortable in communicating and reporting concerns and possible Code of Conduct violations. FinancialForce also has a Senior Director of Trust and Security, responsible for the company's enterprise Information Security Program. The Security department coordinates security policy, program and verification efforts, to help ensure that customer and company information assets are adequately protected.

Workforce Clearance Procedure

Individuals offered a position at FinancialForce undergo background checks prior to commencing employment. FinancialForce's standard background check includes substantiation of educational credentials, previous employment, credit history, and criminal record as well as employment reference checks. Prospective employees must complete an employment application and sign a consent to the release of information for the background check. Prior to starting, a new FinancialForce employee or contractor is required to sign an offer letter, employment contract or independent contractor agreement, including a confidentiality agreement binding the employee to maintain the confidentiality of corporate and customer information. FinancialForce's background checks may vary by country in accordance with local laws.

Access Authorization

Customers control access to their Salesforce Orgs where their FinancialForce Applications and Customer Data are hosted, and can implement a variety of controls made available as part of the Force.com platform to address their compliance policies and requirements. Access to FinancialForce

Applications requires authentication via one of the supported mechanisms described in the Salesforce Security Implementation Guide, as determined and controlled by the customer. The Force.com platform, provided as part of the FinancialForce Applications, includes a variety of configurable security controls that enable customers to tailor the security of the applications to a range of business and compliance requirements.

Security Awareness and Training

Upon acceptance of employment, FinancialForce employees are required to review and sign the company's Employee Handbook, which includes information security policies. The Employee Handbook outlines how FinancialForce conducts business and describes the company's shared values, responsibilities and expected behavior. The Employee Handbook, along with other company policies, are published internally and available to all FinancialForce personnel. After joining the company, employees are required to undergo annual security awareness training. The training covers key security threats and risks, and employee obligations regarding protection of Customer Data and company information and systems. Personnel whose responsibilities include access to Customer Data or personal data (e.g., for support purposes) are informed of the confidential nature of this data and trained on appropriate controls. FinancialForce also provides regular newsletters to all personnel about information security and privacy topics.

Protection from Malicious Software

The Force.com platform infrastructure includes several controls against malware, including hardened UNIX / Linux operating systems on all production servers, centralized logging and alerting, intrusion detection, network access control, antivirus / anti-malware software, host-based firewalls, and data loss prevention tools. All laptops of FinancialForce personnel providing support to customers are encrypted and have anti-virus / anti-malware software that is updated centrally and cannot be disabled. FinancialForce Applications do not scan Customer Data or files uploaded by customers; however, such files are not executed in the FinancialForce Applications or Force.com platform, thereby minmizing the risk of any malware in such files damaging or compromising the FinancialForce Applications or Force.com platform. We recommend that all customers install and run current anti-malware / antivirus software on all devices accessing the service.

Login Monitoring

As part of the FinancialForce Applications, the Force.com platform provides audit and logging capabilities to monitor successful and failed login attempts. Customers can monitor their Orgs for various types of events, including:

- *User Login History* - All successful and failed login attempts are recorded and saved for 180 days.
- *Setup Audit Trail* - Every configuration (Setup) change is logged and archived for 180 days. The Setup Audit Trail shows any change and who made the change. This audit log is especially helpful for organizations with multiple administrators.
- *Object History Tracking* - You can select certain standard and custom fields to track the change history.

User access logs record date, time, User ID, URL executed, operation performed (created, updated, deleted) and source IP address. Logging is kept for a minimum of 90 days in a secure area to avoid tampering.

Password Management

FinancialForce Applications enable customers to configure and manage access and authorization as described under Access Authorization above. User passwords are stored using a salted hash encryption format. Passwords are not logged under any circumstances. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

Security Incident Procedures

Salesforce monitors the Force.com platform, including the FinancialForce Applications, for unauthorized intrusions using network-based intrusion detection mechanisms. Both FinancialForce and Salesforce maintain security incident management policies and procedures. FinancialForce promptly notifies impacted customers of any actual or reasonably suspected unauthorized access to or disclosure of Customer Data.

Data Backup

All Customer Data submitted to the FinancialForce Applications resides on a primary database server with multiple active clusters, and is stored on carrier-class disk storage using redundant devices and multiple data paths, to maximize availability, reliability and performance. Customer Data, up to the last committed transaction, is automatically replicated on a near real-time basis to a secondary site, and is further backed up on a regular basis and stored on backup media for an additional 90 days in production environments. The Force.com platform enables customers to back up their Customer Data off-platfom through multiple mechanisms, including backup APIs and regular data exports, if required.

Disaster Recovery

As part of the FinancialForce Applications, the Force.com platform performs real-time replication to disk within each data center, and near real-time data replication between the production data center and a remote disaster recovery data center. Data are transmitted across encrypted links. Salesforce conducts regular disaster recovery tests to verify the projected recovery times and the integrity of customer data.

Physical Safeguards

Facility Access Control

Production data centers used to provide the FinancialForce Applications have robust access control systems that permit only authorized personnel to enter secure areas. Salesforce data centers, where FinancialForce Applications are hosted, are ISO/IEC 27001:2005 certified. Salesforce employs 24-hour manned security, including foot patrols, perimeter inspections, and video surveillance of the facility perimeters and interiors. Biometric scanning is used for secure area access. Access to secure sub-areas is allocated on a role-specific basis. Only authorized data center personnel have access to data halls. Centralized security management systems are deployed at all data centers to control the electronic access control systems and CCTV networks.

Disposal

After contract termination, Customer Data submitted to the FinancialForce Applications is retained in inactive status within the services for 180 days and a transition period of up to 30 days, after which it is securely overwritten or deleted. Customer Data submitted to the FinancialForce Applications (including Customer Data retained in inactive status) will be stored on backup media for an additional 90 days after it is securely overwritten or deleted. This process is subject to applicable legal requirements.

Technical Safeguards

Access Controls

As indicated above, access to FinancialForce Applications requires authentication via one of the supported mechanisms described in the Salesforce Security Implementation Guide, as determined by the customer. The Force.com platform includes a variety of configurable security controls that enable customers to tailor the security of the applications to various business and compliance requirements. FinancialForce Applications provide each user with a unique username and password that must be entered each time a user logs in. To protect established sessions, FinancialForce Applications terminate idle sessions after a configurable period of time. Customers can configure access and

authorization controls for a range of policies and standards.

Audit Controls

Customers can enable audit logs and object history tracking, and monitor these controls to detect alteration or destruction of data. To help record and examine activity, FinancialForce Applications provide auditing capabilities that capture information about usage of the system, which can be critical in diagnosing potential or real security issues. Such capabilities include:

- Record Modification Fields (core)
- Login History (core)
- Field History Tracking (core)
- Field Audit Trail (add-on)
- Setup Audit Trail (core)
- Event Monitoring (add-on)

Integrity Controls

To help protect Customer Data from improper alteration or destruction, administrators can control a user's visibility of and access to a variety of data elements and application functions by setting permissions in his or her profile and permission sets. A profile is a collection of settings and permissions that determine what a user can do. Permission sets provide a more granular level of permission control; while a user can only be assigned one profile, he or she may be assigned multiple permission sets.

Encryption

FinancialForce Applications use industry-accepted encryption products to protect Customer Data and communications during transmissions between the customer's network and Salesforce's network, including minimum 128-bit TLS Certificates and minimum 2048-bit RSA public keys. Additionally, Customer Data is encrypted during transmission between data centers for replication purposes.

Policies and Procedures

FinancialForce security and privacy and policies apply to all of our information handling practices.

Contractual Privacy Protection for Customers

FinancialForce contracts include confidentiality provisions that prohibit us from disclosing customer

confidential information, including Customer Data, except under certain narrowly defined circumstances, such as when required by law. FinancialForce agrees not to access customer's accounts, including Customer Data, except to maintain the FinancialForce Applications, prevent or respond to technical or service problems, at a customer's request in connection with a customer support issue, or where required by law.

Code of Conduct, Confidentiality Agreements, and Information Security Policies

Every FinancialForce employee is required to comply with FinancialForce's Code of Conduct, sign a confidentiality agreement, and follow FinancialForce's information security policies. Consequences for violating any of these policies or obligations may include discipline, up to and including termination of employment

Contacts

If you have questions or complaints regarding FinancialForce's privacy practices, please contact us at privacy@financialforce.com. For security related questions please email us at security@financialforce.com

Additional Resources and Links

- FinancialForce Security Whitepaper
  http://www.financialforce.com/trust#whitepaper

- FinancialForce Security and Trust Website
  http://trust.financialforce.com/

- FinancialForce Privacy and Data Protection
  http://www.financialforce.com/company/cloud-erp/legal/data-processing-addendum/

- FinancialForce Privacy Statement
  http://www.financialforce.com/company/cloud-erp/legal/privacy-statement/

- Salesforce Security and Trust Resources
  https://trust.salesforce.com/

- Salesforce Administrator Security Best Practices
  http://content.trust.salesforce.com/trust/en/learn/bestpractices/

- Salesforce Security Implementation Guide
  https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/