Certinia and the HIPAA Security Rule

Effective Date:

April 19, 2024

Information Security Department

Certinia

Table of Contents

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"). Certinia.com, inc. ("Certinia") 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 Certinia 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 Certinia's online applications ("Certinia Applications").

This white paper is intended to be a general overview of Certinia 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 Certinia Applications for ePHI, you should consult with a qualified expert to assess whether and how Certinia 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 Certinia Applications. Certinia 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 Certinia online services, but our customers are solely responsible for their compliance with HIPAA in using the Certinia Applications.

About Certinia Applications

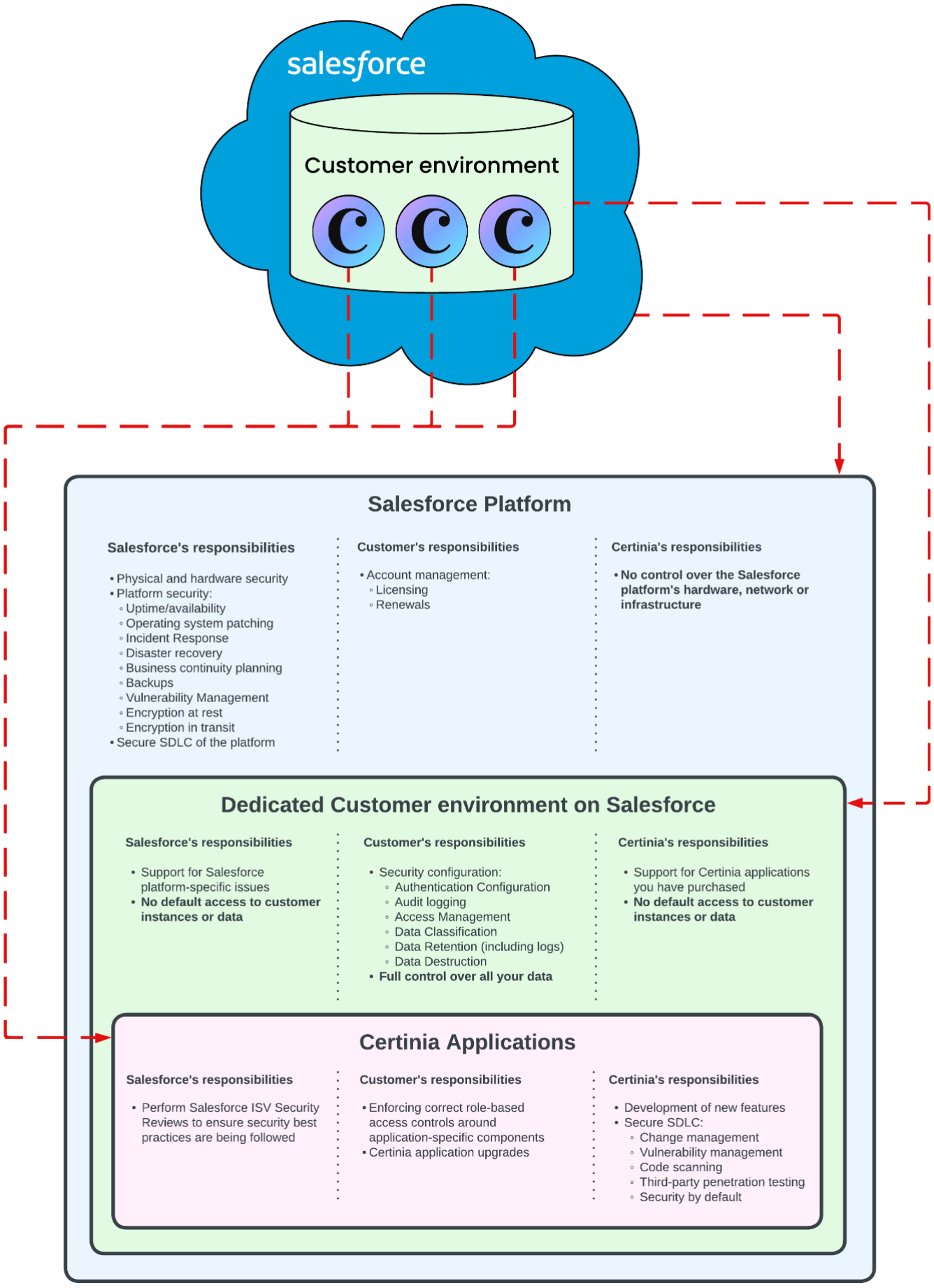
Certinia provides various applications as an Independent Software Vendor (ISV). The Certinia applications are 100% native Salesforce applications, and as such, all Customer Data processed by Certinia applications reside on the Salesforce cloud platform which is owned, operated, and managed by Salesforce. Certinia only provides applications but no infrastructure. Salesforce provides the required platform infrastructure. Salesforce provides the data center and all customer data is stored at Salesforce. As such, all of the network, infrastructure, and platform security controls are inherited and implemented at Salesforce.

Certinia applications are built on the Salesforce platform and are listed on AppExchange (Salesforce cloud applications marketplace). As such, we use the Salesforce Platform as the underlying technology,

which includes tools for development, reporting, workflow authorizations, dashboards, social media (Chatter) and integration. All AppExchange applications go through a qualitative and quantitative review process to ensure applications meet a set of security standards and best practices. By leveraging an industry-leading cloud platform for business applications, Certinia applications and our customers' data benefit from a variety of security features and controls in such areas as user management, access control, disaster recovery, backups, physical and network security. As a result, Certinia applications satisfy our customers' most stringent data security requirements, and comply with major security, privacy and data protection laws and standards globally.

Considering that Salesforce provides the cloud infrastructure required for Certinia applications, a shared security responsibilities model is in place that recognizes the security responsibilities of Certinia, Salesforce, and Customers.

The following graphic on the next page illustrates the shared security responsibilities model at an overview:


salesforce
Customer environment
Salesforce Platform
Salesforce's responsibilities
• Physical and hardware security
• Platform security:
◦ Uptime/availability
◦ Operating system patching
◦ Incident Response
◦ Disaster recovery
◦ Business continuity planning
◦ Backups
◦ Vulnerability Management
◦ Encryption at rest
◦ Encryption in transit
• Secure SDLC of the platform
Customer's responsibilities
• Account management:
◦ Licensing
◦ Renewals
Certinia's responsibilities
• No control over the Salesforce platform's hardware, network or infrastructure
Dedicated Customer environment on Salesforce
Salesforce's responsibilities
• Support for Salesforce platform-specific issues
• No default access to customer instances or data
Customer's responsibilities
• Security configuration:
◦ Authentication Configuration
◦ Audit logging
◦ Access Management
◦ Data Classification
◦ Data Retention (including logs)
◦ Data Destruction
• Full control over all your data
Certinia's responsibilities
• Support for Certinia applications you have purchased
• No default access to customer instances or data
Certinia Applications
Salesforce's responsibilities
• Perform Salesforce ISV Security Reviews to ensure security best practices are being followed
Customer's responsibilities
• Enforcing correct role-based access controls around application-specific components
• Certinia application upgrades
Certinia's responsibilities
• Development of new features
• Secure SDLC:
◦ Change management
◦ Vulnerability management
◦ Code scanning
◦ Third-party penetration testing
◦ Security by default

HIPAA Security Rule: Standards for Protecting ePHI

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

Certinia Security Overview

Certinia 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 Certinia Applications.

Information Security Program

Certinia 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 Certinia Applications by our customers ("Customer Data") as well as corporate information assets. For more details in our security practices please review our Trust site.

How Certinia Services Help Customers Keep ePHI Secure in their Salesforce Environments

Certinia complies with all requirements under the HIPAA Security Rule that apply to Certinia in its capacity as a business associate. In addition, Certinia Applications provide customer-controlled security features that can help our customers address their individual security and compliance requirements under HIPAA. The HIPAA Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of e-PHI. Below is an overview of the three domains.

Administrative Safeguards	Physical Safeguards	Technical Safeguards
• Security Management Process (Risk Management) • Assigned Security Responsibility • Workforce Security • Information Access Management • Security Awareness Training • Security Incident Procedures • Contingency Plan • Evaluation • Business Associate Contracts and Other Arrangements	• Facility Access Controls • Workstation Use • Workstation Security • Device Media Controls	• Access Control • Audit Controls • Integrity • Person / Entity Authentication • Transmission Security

In the following sections, we'll explain how Certinia complies with the applicable requirements as a business associate as well as how the shared security responsibilities model applies, noting how the Salesforce platform is leveraged and what responsibilities Customers should be cognizant of in order to achieve compliance.

Administrative Safeguards

Security Management Process

Risk Management and Analysis

Certinia's process for identifying, assessing and managing risks is a critical component of our internal control system. This includes management of risks relevant to the development, maintenance, and

delivery of our products and services. Certinia's Chief Legal Officer oversees enterprise risk management as well as the operations of the security team. Certinia's risk management program is further outlined in our SOC 1, SOC 2 and SOC 3 reports.

Certinia does not store Customer Data on our internal systems, as all such data resides on the Customer's Salesforce environment. As such, Customers are responsible for risk assessment in their own operations, including their use of Certinia Applications and services, and the data they upload into the Certinia Applications.

Sanction Policy

Certinia 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. Certinia employees who violate the Code of Conduct, an information security policy, or any law may be subject to disciplinary action by Certinia 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

Certinia Applications are hosted on the Salesforce platform. 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 Certinia Applications.

Assigned Security Responsibility

Certinia has defined roles and responsibilities for risk management, security, and compliance. Certinia's Chief Legal Officer oversees Certinia's enterprise risk management program as well as the operations of the security team. The Head of Information Security is responsible for overseeing the day to day operations of the security team as well as technical and product security. The Security Compliance Analyst is responsible for managing the overall security compliance program, GRC operations, and oversight of third-party security audits and assessments.

Workforce Security

Individuals offered a position at Certinia undergo background checks prior to commencing employment subject to local laws and regulations. Certinia'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 Certinia 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. Certinia's background checks may vary by country in accordance with local laws.

Information Access Management

Customers control access to their Salesforce Orgs where their Certinia Applications and Customer Data are hosted, and can implement a variety of controls made available as part of the Salesforce platform to address their compliance policies and requirements. Access to Certinia Applications requires authentication via one of the supported mechanisms described in the Salesforce Security Guide, as determined and controlled by the customer. The Salesforce platform 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. For their Salesforce instance (and by extension the Certinia Applications), Customers can configure role based access, segregation of duties, and measures to align to the principle of least privilege. Additionally by default, Certinia does not have access to the Customer's Salesforce instance and by extension their implementation of Certinia applications and relevant Customer Data.

Security Awareness and Training

Upon acceptance of employment, Certinia employees are required to review and sign the Acceptable Use Policy (AUP), which includes information security policies. The AUP outlines how Certinia conducts business and describes the company's shared values, responsibilities and expected behavior. The AUP, along with other company policies, are published internally and available to all Certinia 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.

Security Incident Procedures

Salesforce hosts all Customer Data on their platform infrastructure. As such, Salesforce monitors the Salesforce platform, inclusive of the Customer's implementation of Certinia Applications and relevant Customer Data, for unauthorized intrusions using network-based intrusion detection mechanisms. Both Certinia and Salesforce maintain security incident management policies and procedures. Certinia

promptly notifies impacted customers of any actual or reasonably suspected unauthorized access to or disclosure of Customer Data. Additionally, Salesforce maintains their own guidance for Customers regarding incident response notification, which is available through their Compliance site (requires Salesforce authentication).

Contingency Plan

Data Backup

All Customer Data submitted to the Certinia Applications reside on the Customer's Salesforce instance which 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 Salesforce platform enables customers to back up their Customer Data off-platform through multiple mechanisms, including backup APIs and regular data exports, if required.

Disaster Recovery and Business Continuity

As 100% native Salesforce applications, the Certinia Applications require the Salesforce platform infrastructure which hosts all Customer Data. As such, Salesforce ensures the relevant disaster recovery and business continuity controls are implemented for their platform. The Salesforce 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.

Evaluation

As stated previously, given the nature of Certinia's applications, a shared security responsibilities model is applicable in which Certinia, Salesforce, and Customers are responsible for implementing security controls and processes to achieve full compliance. Salesforce owns and operates the platform infrastructure which hosts the Certinia Applications and relevant Customer Data. As such, Salesforce has various third-party audits, assessments, and certifications that speak directly of the security controls they implement for their platform and organization. Similarly, Certinia has annual third-party audits conducted focused specifically on the security controls relevant for the Certinia Applications and the scope of Customer Data. Our SOC 1 Type II, SOC 2 Type II, and SOC 3 audit reports in addition to our annual application penetration test report are available securely via our Full Whistic Profile. As such,

Customers are responsible for the security controls that they implement over their own Salesforce instance and are responsible for evaluating the effectiveness of their own controls as necessary to meet the HIPAA Security Rule requirements.

Business Associate Contracts and Other Arrangements

Certinia complies with the requirements of the HIPAA Security Rule that apply to Certinia in its capacity as a business associate. In addition, Certinia applications provide configurable security features that can help our customers address their security and compliance requirements under HIPAA.

Certinia customers that are subject to HIPAA and wish to use our applications for electronic Protected Health Information (ePHI) must first sign a Certinia business associate addendum.

Physical Safeguards

Facility Access Control

Salesforce production data centers have robust access control systems that permit only authorized personnel to enter secure areas. Salesforce data centers, where Certinia Applications are hosted, are ISO/IEC 27001:2013 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.

Workstation Use and Security

As noted previously, Certinia does not store Customer Data on our internal systems. Salesforce provides the required platform infrastructure which hosts all Customer Data. By default, Certinia does not have access to the Customer's Salesforce instance (and by extension their Certinia application implementation and relevant Customer Data). Certinia requires all personnel to acknowledge our Acceptable Use Policy (AUP) upon hire and at least annually. The AUP outlines requirements for secure handling of workstations and other physical security best practices. Note that Customers should ensure that relevant workstation security controls are implemented for their company workstations accessing their Salesforce instance and Customer Data.

Device Media Controls

Additionally, Certinia restricts all USB ports on all company workstations, and the use of removable storage media is restricted. As all Customer Data resides on the Customer's Salesforce instance, Customer should ensure that relevant device media controls are implemented for their company workstations accessing their Salesforce instance.

Technical Safeguards

Access Controls

As indicated above, access to Certinia Applications requires authentication via one of the supported mechanisms described in the Salesforce Security Guide, as determined by the customer. The Salesforce platform includes a variety of configurable security controls that enable customers to tailor the security of the applications to various business and compliance requirements. Salesforce requires each user to have a unique username and password. Salesforce is compatible with a variety of SSO and MFA solutions. To protect established sessions, Customer can set their Salesforce instance configurations to terminate idle sessions after a determined 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, Certinia 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 (Salesforce native)
- Login History (Salesforce native)
- Field History Tracking (Salesforce native)
- Field Audit Trail (Salesforce native)
- Setup Audit Trail (Salesforce native)
- Event Monitoring (Salesforce native)
- Permission Logging (Certinia)

Integrity Controls

To help protect Customer Data from improper alteration or destruction, administrators for the Customer's Salesforce instance 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, and may be grouped into "permission set groups" for added versatility; while a user can only be assigned one profile, he or she may be assigned multiple permission sets or permission set groups. Certinia products deliver a set of functionality-centric permission sets which abide by the principle of least privilege.

Person / Entity Authentication

As stated previously, Customer is responsible for implementing their own access controls over their Salesforce instance (and by extension their implementation of the Certinia Applications and relevant Customer Data). As such, Customer is responsible for implementing processes and controls to ensure the appropriate verification of the identity of any user seeking access to Customer Data. Salesforce requires the use of a unique user ID and password for each user, and is also compatible with various authentication solutions such as MFA, SSO, mTLS, etc.

Transmission Security

Certinia Applications, through leveraging the Salesforce platform, 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.

Contacts

Issues and inquiries regarding Certinia's privacy practices can be directed to: privacy@certinia.com.

Issues and inquiries regarding Certinia's organization and product security can be directed to: security@certinia.com.

Additional Resources and Links

Certinia Security and Trust Website
https://certinia.com/trust/

Certinia Privacy and Data Protection
https://certinia.com/privacy/

Certinia Privacy Statement
https://certinia.com/privacy/privacy-statement/

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

Salesforce Security and Privacy Compliance Documents
https://compliance.salesforce.com/

Salesforce Security Best Practices
https://security.salesforce.com/security-best-practices/

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