servicenow

ServiceNow security & HIPAA

ServiceNow's response to the HIPAA security and privacy requirements

servicenow

Table of contents

servicenow

Introduction

This white paper is intended to help ServiceNow customers understand the security controls available within the Now Platform® to address the security and privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related laws and regulations. Our approach to security is to safeguard all customer data with the same rigorous measures regardless of its type or sensitivity.

The information put forward in this document is not meant to serve as an exhaustive attestation of ServiceNow's compliance with the HIPAA security requirements; covered entities should contact ServiceNow directly for further HIPAA related queries.

HIPAA and ServiceNow

Recognizing the security and privacy challenges facing covered entities, ServiceNow has developed the Now Platform to include options and features that enable its healthcare customers to comply with privacy and security requirements stipulated by law. These requirements include:

- Ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI) the organization creates, receives, maintains, or transmits as customer data
- Protecting against any reasonably anticipated threats and hazards to the security or integrity of ePHI
- Protecting against reasonably anticipated uses or disclosures of such information not permitted by the Privacy Rule[1].

ServiceNow security

Certification and attestation

ServiceNow has made significant investments in technology, processes, and expertise to ensure that our cloud services meet the most stringent global standards for performance, scalability, security, privacy, and compliance. The most effective way of demonstrating this to our customers is through the process of independent certification and accreditation.

A complete list of all ServiceNow certifications and attestations is available in the Qualifying ServiceNow as a Vendor eBook..

Encryption

ServiceNow offers several encryption options designed to enable the customer, as the covered entity, to retain control over all data processed and stored in the customer's instance(s). These security features allow regulated customers to implement preventative data protection controls that limit access to their data and protect sensitive data at rest.

For more information about encryption offerings, please review the Data Encryption eBook.

Policies and procedures

It is ServiceNow policy to treat all data that the customer has entered into their instance as "Customer Confidential". This means that it is treated with the highest sensitivity and in accordance with the appropriate controls as described in this document.

[1] Per NIST 800-66

You can access a number of ServiceNow standard operating procedures and policies by accessing the CORE (Compliance Operations Readiness Evidence) platform available via ServiceNow Community. ServiceNow CORE enables ServiceNow customers to have self-serve access to documentation they need to help support internal audit and assessment requirements, prepare for onsite audits, and address regulatory requirements.

Controls

To further enhance the customer's security program, the Now Platform is developed with specific security measures and controls that facilitate data protection. In the context of HIPAA, a number of these controls are discussed later in this document in greater detail.

For a more comprehensive understanding of the technical controls available, visit the ServiceNow Trust and Compliance Center.

ServiceNow as a business associate and business associate agreements (BAA)

Under HIPAA, a business associate is generally defined as an entity that creates, receives, maintains or transmits protected health information on behalf of a covered entity.

Covered entities are required to enter into a written contract or written arrangement with their business associates, often referred to as a business associate agreement or addendum (BAA). ServiceNow will enter into a BAA if the covered entity customer chooses to store ePHI in their instance. The standard ServiceNow BAA attests to the following:

- ServiceNow has implemented appropriate safeguards to protect the customer data, including ePHI contained therein.
- ServiceNow will comply with provisions applicable to business associates, including the Security Rule (Subpart C of 45 CFR Part 164). In summary, the Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.
- ServiceNow will comply with applicable requirements of the Privacy Rule (Subpart D of 45 CFR Part 164). In summary, the Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients control over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- ServiceNow will comply with applicable requirements of the Breach notification (Subpart E of 45 CFR Part 164). In summary, the Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. The ServiceNow BAA sets forth notification requirements that ServiceNow follows in the event of any data breach or suspected data breach so that the customer can comply with HIPAA's breach notification requirements.
- ServiceNow will have written agreements with any subcontractors who may have access to or will otherwise use or disclose customer data (which may contain ePHI) to ensure compliance with HIPAA.

While ServiceNow enters into a BAA with customers that may process ePHI within the subscription service, it is important to understand that ServiceNow is not a typical business associate. ServiceNow will not enter into a BAA that requires ServiceNow to carry out the customer's obligations under HIPAA as the covered entity. Consistent with the model described above, and

in terms of data privacy there are two defined roles: data controller and data processor, each with their own associated responsibilities.

- The data controller is a person or legal entity who determines why and how the data is used.
- The data processor is a person or legal entity that carries out the processing of that data on behalf of the data controller.

In the case of a customer using ServiceNow, the customer is the data controller, and retains the primary responsibility for ensuring compliance with HIPAA, whereas ServiceNow is the data processor.

ServiceNow satisfies its obligations as a business associate differently than traditional business associates. For example, some BAAs require business associates to provide an individual access to its ePHI within their "Designated Record Set" and within a prescribed period of time. However, customers are able to and are responsible for providing access to individuals who request for access to their ePHI directly by using the Now Platform and accessing the relevant information requested.

Security Rule standards and ServiceNow implementation

The following tables list the various HIPAA Security Rule standards, the implementation specifications, and how ServiceNow addresses implementation. The tables are intended to provide ServiceNow customers with a high-level mapping of how its security controls are designed to help address HIPAA Security, Privacy, and Breach Notification Rule requirements.

While ServiceNow implements and maintains a security program as outlined below, safeguarding hosted ePHI data is a shared responsibility between ServiceNow and its customers. Accordingly, customers have an independent obligation to comply with HIPAA and the HITECH Act and are responsible for complying with their responsibilities as covered entities by implementing appropriate administrative, technical, and physical safeguards to protect ePHI hosted and processed by ServiceNow as customer data.

Note: in the tables below (R) = required and (A) = addressable per HIPAA.

Administrative safeguards

Standards	Sections	Implementation specifications	ServiceNow implementation
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)	ServiceNow has a formal Risk Management program, based on ISO 27001 and 27002, ISO3100 2009, IEC/ISO 31010 2009, NIST SP800-30_r1, and COBIT 5 that includes overall risk management program, risk analysis procedures, and system security reviews. Information Security Policies and an Acceptable Use Policy are in place to ensure sanction policy is applied against workforce members who fail to comply with the security policies and procedures.
Assigned Security Responsibility	164.308(a)(2)	(R)	ServiceNow's chief information security officer (CISO) is responsible for security.

Standards	Sections	Implementation specifications	ServiceNow implementation
			Additionally, key stakeholders oversee the ServiceNow security program.
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)	ServiceNow screens all employees and contractors prior to employment. It performs criminal, employment, reference, and financial background checks in accordance with our internal SOPs and as allowable by law. There is also a mandatory drug screening (where legally permitted) prior to employment. Employee access is determined by the employee's role and function within ServiceNow and technical controls are in place to validate access. Access management and authorization to the instance is the responsibility of the customer. ServiceNow provides access control list (ACL) rules to restrict access to all database and personalization operations. Customers have the capability within their instance to configure and enforce least privileges to the appropriate personnel only. ServiceNow has a termination process that ensures employee and contractor access and entitlements are revoked immediately upon termination of employment.
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)	Although ServiceNow does not perform the health care clearing house function, all ServiceNow customer data is isolated per the ServiceNow logically single-tenant architecture. Access management and authorization to the instance is the responsibility of the customer. ServiceNow provides a plugin called the 'SNC Access Control Plugin'. Customers can use this plugin to control instance level access by ServiceNow support personnel. ServiceNow has implemented processes and procedures to manage user-level access to systems and applications based on the requestor's job functions on a need-to-know basis. The ServiceNow compliance team reviews high-risk user authorizations for critical systems on a quarterly basis.
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A)	ServiceNow requires all employees to participate in an annual security awareness training that covers malware, monitoring, password management, data protection, privacy, and general security threats.

Standards	Sections	Implementation specifications	ServiceNow implementation
		Password Management (A)	Additionally, ServiceNow developers are specifically trained in secure coding practices (e.g. OWASP). Additional, mandatory security training is assigned for personnel in sensitive roles where appropriate. In addition to the mandatory Security Awareness Training, periodic reminders in the form of security posters, phishing tests, clean desk/clear screen checks, security policies, and other security topics are shared with employees.
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)	ServiceNow has a formal, documented security incident response policy, process, and workflow. Its incident response process includes event discovery, triage, escalation, notification (including customer notification) remediation, and post-mortem review. If a customer environment or data is impacted, the customer will be notified via their normal support contacts.
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)	ServiceNow has a comprehensive information system contingency plan (ISCP) that considers the criticality of customer data and infrastructure involved with the subscription service, and includes procedures on activation, notification, recovery and reconstitution. The plan applies to the entire ServiceNow subscription service offering. The ServiceNow AHA architecture[2] provides customers with business continuity in the event of an incident or outage. Additionally, ServiceNow backs up customer data to local disks at both active and passive data center sites nightly. ServiceNow has a target recovery point objective (RPO) of one hour and recovery time objective (RTO) of two hours. The Disaster Recovery and Business Continuity Procedure controls are validated on an annual basis to ensure the continuation of critical business processes during the event of an emergency.
Evaluation	164.308(a)(8)	Evaluation (R)	ServiceNow performs periodic evaluations of security requirements and controls. Additionally, third-party evaluation of security-related controls is performed on an annual

[2] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-sn-advanced-high-availability-architecture.pdf

Standards	Sections	Implementation specifications	ServiceNow implementation
			basis (ISO27001, SSAE18 SOC 1 Type II, and SOC 2). ServiceNow has technical evaluation of its application through its application penetration testing program, which includes major release penetration testing by a third-party vendor contracted by ServiceNow and customer penetration testing. Periodic technical and nontechnical evaluations are performed based upon standards implemented and/or in response to environment or operational changes affecting security. However, given the nature of services provided by ServiceNow to its customers, all customer data (including potential ePHI stored on customer instances) is treated equally as 'Customer Confidential' data.
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)	Customers potentially storing ePHI in their instance can enter into the ServiceNow BAA to ensure compliance with HIPAA, as amended by the Omnibus Rule. Customers have full control over the data in their instance. ServiceNow treats all customer data equally, and any customer data that is stored or processed by a ServiceNow instance is classified internally as 'Customer Confidential' regardless of the data classification determined by the customer. ServiceNow does not outsource its development and support functions to any third parties or grant access to customer data to its vendors. Therefore, ServiceNow does not maintain BAAs with its vendors regarding the services provided to its customers.

Physical safeguards

Standards	Sections	Implementation specifications	ServiceNow implementation
Facility Access Controls	164.310(a)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A)	The ServiceNow ISCP considers the criticality of customer data and infrastructure involved with the subscription service, and includes procedures on activation, notification, recovery and reconstitution. The ServiceNow AHA implements a redundant data center architecture whereby

		Maintenance Records (A)	customer data is replicated between both data centers in near real-time. The ServiceNow Cloud is hosted in data center colocation facilities which inherit physical security and environmental controls from third-party hosting providers. Additionally, ServiceNow controls and grants access to the dedicated cages in which ServiceNow equipment is hosted. Data center access controls are met through a combination of provider-implemented controls and ServiceNow-implemented controls. ServiceNow reviews SSAE18 independent audit reports, or equivalent certifications, that address physical security and environmental controls implemented at third-party hosting providers. ServiceNow stores all customer data in secure data centers that are equipped with 24/7 onsite security of the data center provider, extensive CCTV networks, multiple levels of entry to gain access to the data center halls, visitor control procedures, and biometric access controls. All access- and security-related changes to the physical components of the ServiceNow facility within the data center are authorized, monitored, and logged.
Workstation Use	164.310(b)	Workstation use (R)	ServiceNow workstations may incidentally access customer data during support engagements and similar events. They do not otherwise process, transmit, or maintain customer data; customer data always resides within the secure data center environment. ServiceNow has policies and technical security controls that ensure its workstations are properly used. These controls include the mandatory use of an isolated and secure access facility when events that may require interaction with customer data are necessary. Employees are not able to access, export or otherwise transfer customer data outside of this facility, and all access is logged and monitored.
Workstation Security	164.310(c)	Workstation security (R)	ServiceNow implements technical security controls on all workstations to ensure they are properly secured (e.g. all workstations use full disk encryption and password-based authentication).

Device and Media Controls	164.310(d)(1)	Device and media- controls (R) Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)	ServiceNow has implemented policies and procedures that govern media and device security controls, customer data handling, information security standards, and secure data deletion. ServiceNow follows NIST 800-88 recommendations for the proper disposal of hard drives (no tape media is used) and for proper media reuse. ServiceNow does not use removable media within its cloud operations environment. Movements of hardware are authorized, logged, and monitored using an instance of the ServiceNow CMDB. Customers can export their data from the subscription service at any time. It is their responsibility to protect data once it leaves the subscription service.

Technical safeguards

Standards	Sections	Implementation specifications	ServiceNow implementation
Access Control	164.312(a)(1)	Access control (R) Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)	Access management, including authorization, for the instance is the responsibility of customer. ServiceNow provides ACL rules to restrict access to all database and personalization operations. The Now Platform provides the ability to view and terminate individual user sessions, lock out users from the system, manage passwords, and inactivate users. The default session timeout on each instance can be adjusted to each customer's own requirements. Customers have the ability to configure and enforce least privileges to the appropriate personnel only based on business requirements. ServiceNow grants systems and applications access based on the requestor's job functions, and on a need-to-know basis. Entitlement reviews of high-risk systems are done on a quarterly basis. ServiceNow offers customers the complementary ability to encrypt specific fields (column-level encryption) in the system

			using AES 256-bit encryption and private encryption keys. Optional full disk encryption is provided via self-encrypting hard drives with AES256 bit encryption. This encryption can only be used with dedicated hardware. ServiceNow provides optional Edge encryption using a customer side proxy which will allow encryption of string data before it leave the customer environment. Optional Database Encryption enables all data to be protected with transparent AES-256 encryption, whether the database is online or offline. This capability is available for all supported releases. For Edge and column-level encryption, server-side processing is not possible on certain data; however, some searching and reporting is possible.[3] In addition to all of this, all data backups are encrypted using AES 256 Access control is a shared responsibility between ServiceNow and its customers, as customers have control over the implementation and use of most of the access control features within the service.
Audit Controls	164.312(b)	Audit Controls (R)	System activities are logged both from an infrastructure perspective as well as from within the application. ServiceNow monitors all infrastructure logs. The Now Platform writes detailed log and activity information that is stored in tables within a customer's instance. Customers control and manage the application logging from within their instance. ServiceNow has implemented log management procedures that describe the process of leveraging logs created by devices and applications throughout the ServiceNow global infrastructure. These procedures are intended to facilitate security controls, support regulatory requirements, and maintain an accurate event audit trail. ServiceNow has established procedures for the security operations team to perform daily, weekly, and other periodic reviews of information system and operational activities and reporting of high-risk issues to security leadership.

[3] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-data-encryption-with-servicenow.pdf

Integrity	164.312(c)(1)	Integrity (R) Mechanism to Authenticate Electronic Protected Health Information (A)	ServiceNow does not do content monitoring or DLP. The nature of the Now Platform makes the determination of alteration or loss of data impossible. As an alternative measure, customers can encrypt specific, sensitive information in a ServiceNow instance at the field level. ServiceNow also monitors critical configurations on devices and servers in the customer-facing infrastructure for changes. ServiceNow has implemented file integrity monitoring for the application. Critical system files have appropriate permissions set and only the appropriate roles have access to the underlying operating system.
Person or Entity Authentication	164.312(d)	Person or entity authentication (R)	Access management for the instance is the responsibility of the customer. ServiceNow supports local authentication, LDAP-based authentication (including Active Directory), and SAML-based and SSO solutions for customer instances. ServiceNow access to the production environment is controlled through an IPSec VPN tunnel using two-factor authentication.
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)	Customer data is always encrypted using TLS when traversing public networks. ServiceNow also supports TLS encryption for email, FTP/S for file transfers, and secure LDAP for Active Directory and/or LDAP queries. In addition, user passwords for built-in authentication are stored at rest as hashed values using one-way hashing algorithms.

Organizational requirements

Standards	Sections	Implementation specifications	ServiceNow implementation
Business associate contracts or other arrangements	163.314(a)	Business associate contracts or other arrangements (R) Business associate contracts (R) Business associate contracts (R) Business associate contracts (R)	ServiceNow has implemented its standard BAA as described above to comply with applicable requirements of this subpart. If ServiceNow uses subcontractors that process PHI or ePHI of customers, then it would enter into business associate agreements or other contractual commitments.

		Other arrangements (R) Business associate contracts with subcontractors (R)	

Policies and procedures documentation

Standards	Sections	Implementation specifications	ServiceNow implementation
Policies and procedures	164.316(a)	Policies and procedures (R)	While ServiceNow is not directly required to comply with regulatory requirements (other than SOX, SEC, and business associate requirements under HIPAA), ServiceNow provides a cloud-based software solution to its enterprise customers whose regulatory requirements in many cases extend scope to include our application and our business processes. Customers can customize the solution to meet their internal and regulatory requirements. ServiceNow documents and reviews changes to the policies and procedures via its managed document program and document control procedures. Thus, ServiceNow has implemented reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart.
Documentation	164.316(b)	Documentation (R) Time limit (R) Availability (R)	While there is no explicit HIPAA policy or procedure implemented to specifically meet compliance with this subpart section of the HIPAA Security Rule, reasonable and appropriate measures have been implemented to maintain a record of any action, activity or assessment, where required by this subpart. These records, actions, activities, or assessments are maintained on an internal ServiceNow-managed platform, in the form of control test definitions and activities. Upon contract expiration or exit, customers have a fixed period of time within which to request their data to be returned, after which all hosted backed-up data is automatically deleted and overwritten.

Notification by a business associate

Standards	Sections	Implementation specifications	ServiceNow implementation
General rule	164.410(a)	Breaches treated as discovered	ServiceNow does not perform the function of a covered entity. ServiceNow reports both incidents and security incidents in accordance with the incident management process and security incident response plan. If a customer environment or data is impacted, the customer will be notified via their designated contacts. As the covered entity, it is the responsibility of the customer to notify media and/or individuals of breach of unsecured PHI/ePHI, with required content as per the requirements on the HHS Website, and within the required timeline. ServiceNow will provide its covered entity customers with other available information that the covered entity customer is required to include in notification to applicable entities (or individuals), to the extent such information is available in the ordinary course of operating the subscription service.
N/A	164.410(b)	Timeliness of notification Content of notification	

Law enforcement delay

Standards	Sections	Implementation specifications	ServiceNow implementation
Law Enforcement Delay	164.412	N/A	ServiceNow does not perform the function of a covered entity. The customer, as a covered entity, is the owner of the data stored within the instance and is responsible for the information stored, along with any regulatory requirements for that information. As a business associate, ServiceNow will provide information to the extent such information is available in the ordinary course of operating the subscription service.

Administrative requirements and burden of proof

Standards	Sections	Implementation specifications	ServiceNow implementation

N/A	164.414(a)	Administrative Requirements	ServiceNow does not perform the function of a covered entity. The customer, as a covered entity, is the owner of the data stored within the instance and is responsible for the information stored, along with any regulatory requirements for that information. As a business associate, ServiceNow will provide information to the extent such information is available in the ordinary course of operating the subscription service.
N/A	164.414(b)	Burden of Proof	

Uses and disclosures: organizational requirements

Standards	Sections	Implementation specifications	ServiceNow implementation
Business Associate Contracts	164.504(e)	Business associate contracts Other arrangements Other requirements for contracts and other arrangements Business associate contracts with subcontractors	ServiceNow does not perform the function of a covered entity or government entity. ServiceNow does not outsource its development and support functions or grant access to customer data to its subcontractors. If ServiceNow uses subcontractors that process PHI or ePHI of customers, then it would enter into business associate agreements or other contractual commitments.

Conclusion

This document has provided detailed responses to each of the standards defined by the HIPAA Security Rule. This is intended to illustrate how the ServiceNow Cloud provides customers with the ability to implement controls that meet or exceed the requirements for HIPAA.

servicenow

Appendix A: Resources

Acronyms Used

HIPAA	Health Information Portability and Accountability Act
ACL	Access control list
AES	Advanced Encryption Standard
AHA	Advanced High Availability
BAA	Business Associate Agreement
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
CMDB	Configuration Management Data Base
COBIT	Control Objectives for Information and Related Technologies
DLP	Data Loss Prevention
DoD	(United States) Department of Defense
ePHI	electronic Protected Health Information
FTP	File Transfer Protocol
GRC	Governance, Risk and Compliance
HHS	Health and Human Services
HITECH	Health Information Technology for Economic and Clinical Health
IEC	International Electrotechnical Commission
IIHI	Individually Identifiable Health Information
IPSec VPN	Internet Protocol Security Virtual Private Network
ISCP	Information System Contingency Plan
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PaaS	Platform as a Service

PHI	Protected Health Information
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SLA	Service level Agreement
SOC	Service Organization Control
SSAE	Statement on Standards for Attestation Engagements
TLS	Transport Layer Security

Further reading

- ServiceNow Assurance Pack (SNAP)
  - Available via your ServiceNow or Partner sales representative or CORE (link below)
  - Provides further detail on the ServiceNow security program, including topics covered in this document
- Delivering Secure, Scalable, and Compliant Cloud Services eBook
- Trust and Compliance Center
- Product Documentation
- CORE (Compliance Operations Readiness Evidence) platform
- Data Encryption eBook

About ServiceNow

ServiceNow is changing the way people work. By defining, structuring, and automating work, we are creating a modern and secure service experience for everyone in the enterprise. Find out more at www.servicenow.com.