

WITHINGS

HIPAA Compliance Guide

v2 - January 2024

- **Notices** [3](#)
- **Purpose and intended audience** [3](#)
- **Definitions** [4](#)
- **WITHINGS vision** [6](#)
- **What is HIPAA?** [6](#)
- **To whom does HIPAA apply?** [7](#)
- **What are the HIPAA requirements?** [8](#)
 - Overview [8](#)
 - Privacy obligations of a business associate [8](#)
 - De-identification of health information [9](#)
 - Security obligations of a business associate [9](#)
 - Breach notifications obligations of a business associate [10](#)
- **HIPAA compliance at WITHINGS** [11](#)
 - Overview [11](#)
 - WITHINGS Information Security Management System and scope [12](#)
 - History [12](#)
 - Purpose [13](#)
 - Scope [14](#)
 - WITHINGS Compliance Program [15](#)
 - WITHINGS Compliance Program mapping to HIPAA requirements [19](#)
 - HIPAA Security rules – Administrative safeguards [19](#)
 - HIPAA Security rules – Physical safeguards [24](#)
 - HIPAA Security rules – Technical safeguards [27](#)
 - HIPAA Security rules – Organizational safeguards [29](#)
 - HIPAA Privacy rules [32](#)
 - HIPAA Breach Notification rules [35](#)

NOTICES

Customers are responsible for making their own independent assessment of the information in this document. This guide is (a) for informational purposes only, (b) does not intend the information or recommendations in this guide to constitute legal advice, (c) does not create any commitments or assurances from WITHINGS and its suppliers or licensors, and (d) represents current WITHINGS offerings and practices, which are subject to change without notice.

PURPOSE AND INTENDED AUDIENCE

The purpose of this guide is to help WITHINGS customers to improve their knowledge of HIPAA standards and help them to comply with these standards. It will also provide all the necessary information to assure customers that WITHINGS meets its obligations and requirements with regards to HIPAA. This guide is intended to apply to security officers, compliance officers, or any other resources who are in charge of HIPAA implementation and compliance at their companies.

DEFINITIONS

Any capitalized terms used but not otherwise defined in this document have the same meaning as in [HIPAA](#).

AFNOR Certification

WITHINGS Certification Body for the ISO 27001:2017, ISO 27701:2019 and HDS certifications of WITHINGS ISMS. Description: AFNOR Certification was the first French certification body to be awarded COFRAC (French Accreditation Committee) accreditation. The scope of this accreditation is regularly extended in order to secure greater confidence in AFNOR Certification certificates, equally spanning inspection, business management system certification, competency certification, product certification and services certification or qualification of firms. [More information on AFNOR](#).

Business Associates

A “business associate” is an entity that accesses, uses, processes or discloses PHI on behalf of a covered entity for a service described in HIPAA regulations. WITHINGS cloud services hosted on WITHINGS Medical(s) Platform(s), such as WITHINGS RPM or WITHINGS API, could make WITHINGS a business associate when WITHINGS provides these services to HIPAA-covered entities, or to a business associate of a HIPAA-covered entity if the covered entities were leveraging the online services to store and transmit PHI.

Business Associate Agreements

The HIPAA Privacy Rule and the HIPAA Security Rule require covered entities to obtain written assurances from their business associates that the business associates will appropriately safeguard the PHI they receive or create on behalf of the covered entity. These assurances typically are provided in a contract between the covered entity and business associate, known as a “business associate agreement,” or “business associate addendum.”

DEFINITIONS

Covered Entities

HIPAA “covered entities” are:

- healthcare providers that engage in certain electronic transactions, including any healthcare provider that makes claims against a patient’s health insurance;
- health plans, including health insurers and group health plans; or
- healthcare clearinghouses, which are entities that translate electronic health transactions formats.

Software vendors are not identified as covered entities, but they may be business associates to covered entities, depending on the services offered and how they are used.

Protected Health Information (PHI)

PHI is a subset of health information, in any media, including demographic information collected from an individual, that is:

- created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse;
- relates to an individual’s health, provision of healthcare to the individual, or payment for the provision of healthcare; and
- identifies an individual or could reasonably be used with other available information to identify an individual; and
- is not specifically excluded from the definition of PHI (generally, education, and employment records are excluded from HIPAA coverage).

PHI includes many common identifiers, such as name, address, and Social Security Number, and can be in any form or media, whether electronic, paper, or oral. When used in an electronic form, PHI is also defined as “electronic protected health information” (ePHI).

WITHINGS VISION

It is now well-known by healthcare industry professionals that the rate of chronic disease is increasing and will reach the majority of the population. Remote patient monitoring, defined as the use of wireless technology to collect and track medical information from an individual outside of a healthcare provider's office or facility, is slated to become the future of modern medicine.

By providing medical-grade hardware products with clinical validation, and healthcare industry-compliant applications and services, WITHINGS is actually the world leader in connected health, with more than ten (10) years of expertise, and will be the best and most valuable partner for any covered entity.

WITHINGS wants to be a trusted partner for any of its customers by committing to protect the data of its customers. Customers' trust is essential, especially in the healthcare industry, where healthcare providers need to deliver high-quality patient care with innovations, proactively engaging their patients and controlling their costs. WITHINGS compliance program includes the word-reference standards in terms of privacy and security of PHI, allowing WITHINGS customers to manage their health and track progress in this increasingly challenging industry and ensure their compliance.

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a U.S. federal law that mandates national standards to protect the privacy and security of health information, and the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") is a 2009 law that increases the obligations and penalties under HIPAA. These laws place the onus of compliance with security and privacy regulations in healthcare on the shoulders of what have been termed covered entities and by extension, their business associates or suppliers that come into contact with electronic Protected Health Information (ePHI).

TO WHOM DOES HIPAA APPLY?

Healthcare providers

Healthcare providers who conduct certain financial and administrative transactions electronically for which HHS has adopted a standard. Such providers include:

- Doctors;
- Clinics;
- Psychologists;
- Dentists;
- Nursing homes;
- Pharmacies.

Health plans

Individual and group plans that provide or pay the cost of medical care. Such plans include:

- Medicare, Medicaid, and Medicare supplement insurers;
- Health, dental, vision, and prescription drug insurers;
- Health maintenance organizations (HMOs);
- Employer-sponsored group health plans;
- Multiemployer health plans;
- Government and church-sponsored health plans.

Healthcare clearinghouses

Entities that process non-standard health information they receive from another entity into a standard format, or the converse. Such entities might include:

- Billing services;
- Repricing companies;
- Community health management information systems.

[To learn more, refer to HHS' covered entities guidance.](#)

If a covered entity engages a vendor, or supplier, called a business associate to help it carry out its healthcare activities and functions, the Business Associate needs to adhere to and comply with the HIPAA standard as well. This agreement is contractually defined in a written Business Associate Agreement (BAA). Therefore, the two parties are then bound by a shared responsibility agreement to protect the privacy and security of protected health information.

WHAT ARE THE HIPAA REQUIREMENTS?

Overview

WITHINGS wants to share its knowledge about HIPAA regulations to help its customers in their strategies and increase their knowledge of information security and privacy. It is also very important that everyone clearly understands roles and responsibilities. WITHINGS has provided a brief overview of this matter in this section.

HIPAA's principal components concern the standards set by the Privacy, Security, and Breach Notification Rules, which govern the protection of PHI. HHS' Office for Civil Rights is authorized to enforce these rules. Covered entities and their business associates must comply with the following HIPAA rules by implementing adequate safeguards.

Privacy obligations of a business associate

Privacy rules are very similar to the EU GDPR rules, as they both relate to granting individuals greater control over their PHI. They aim to safeguard the privacy of individuals and their PHI, while allowing appropriate uses and disclosures of the data without patients' approval to improve the healthcare system and overall public health by using the de-identification process. The ISO/IEC 27018 standard covers the majority of the HIPAA Privacy Rules.

[More information on Privacy Rules.](#)

Business associate agreements must include certain requirements of the HIPAA rules. Specifically, business associates must:

- abide by the limitations on the use and disclosure of PHI set forth in the agreement;
- not use or further disclose PHI other than as permitted or required by the agreement or as required by law;
- use appropriate safeguards to prevent a use or disclosure of PHI other than as provided for by the agreement;
- comply with certain requirements with respect to individuals' right to access, amend, and receive an accounting of disclosures of PHI;
- return or destroy PHI upon termination of the agreement.

De-identification of health information

As mentioned, the Privacy Rules allow the use of health information from individuals without patients' prior approval, as long as the information is de-identified. De-identification is the process of removing identifiers from protected health information to mitigate the privacy risks to individuals. Covered entities or their business associates are allowed to use de-identified health information without adhering to HIPAA requirements, such as when anonymized patient data is used for medical research purposes. For more information on de-identification of health information, please refer to this [link](#).

Security obligations of a business associate

Basically, the goal of the Security Rules is to ensure the protection of the Privacy Rule with appropriate and proportionate technical and non-technical measures or controls. As for the Privacy Rules, the Security Rules only apply to protected health information in electronic form (ePHI). [More information on Security Rules.](#)

The HIPAA Security Rule requires that a covered entity or business associate implements different types of safeguards—mechanisms, processes, or procedures used to mitigate security vulnerabilities and reduce security risks—to protect electronic PHI. These safeguards include:

- administrative safeguards (e.g., security management process, security awareness training);
- physical safeguards (e.g., facility access controls, device and media controls);
- technical safeguards (e.g., access control, transmission security);
- organizational safeguards (e.g., contracts)

These security measures must be documented and kept current, and the business associate must retain such documentation for at least six years.

The best way to comply with the Security Rules is to implement an Information Security Management System (ISMS) that is compliant with the ISO/IEC 27001 standard.

Breach notifications obligations of a business associate

The HIPAA Breach Notification Rule requires business associates notify covered entities following the discovery of a breach of unsecured PHI. This notification must be made without unreasonable delay and no later than 60 days after discovery of the breach. The business associate agreement may require a shorter time frame. The rule also requires that business associates have reasonable measures in place to detect breaches of unsecured PHI.

[More information on Breach Notification Rules.](#)

The business associate must also notify the affected individuals, the HHS Secretary, and, in certain cases, the media.

An unsecured PHI is defined as a PHI that has been disclosed to unauthorized persons, or a PHI where there was a breach of availability, integrity or traceability. For example, it could be indecipherable information.

HIPAA COMPLIANCE AT WITHINGS

Overview

While the U.S. Department of Health and Human Services (HHS) does not recognize a formal certification process for HIPAA compliance, WITHINGS has launched its Compliance Program to ensure the compliance of its Information Security Management System (ISMS) with regards to international standards. Therefore, WITHINGS regularly undergoes several independent audits to assess the security, privacy, operational, and compliance controls implemented at WITHINGS. This means that an independent certification body has examined the controls present in ISMS based on global standards that encompass requirements outlined in HIPAA.

It is essential to understand that HIPAA compliance is a shared responsibility between WITHINGS and its customers, and WITHINGS works continuously to ensure the highest level of controls. As part of the ISMS, WITHINGS has appointed specific task forces to work on compliance with standards and regulations around the world. They are also in charge of facilitating and supporting independent audits and assessments by third parties in order to earn a sufficient level of trust.

History

WITHINGS was registered in June 2008. WITHINGS is headquartered (HQ) in Issy-les-Moulineaux (France), with offices in Boston (Massachusetts, USA) and Hong Kong, and distributes products worldwide.

WITHINGS designs, develops, manufactures and sells connected health devices for home monitoring. WITHINGS has implemented a Quality Management System (QMS) and passed the international standards certification ISO 13485:2016 for Connected Medical Electronic Devices.

WITHINGS also designs, develops and sells a wide range of B2C and B2B services, including web applications (mainly SaaS), Apple iOS & Android applications, Apple iOS & Android Software Development Kit (SDK).

More recently, developing health services for B2C customers such as product reimbursement by healthcare systems, and B2B services for care providers and medical professions, such as patient remote monitoring platforms, is one of the key parts of the WITHINGS strategy. It appears pretty obvious that WITHINGS would need strong technical and organizational safeguards and processes in place to be compliant with industry standards.

WITHINGS has therefore implemented different cloud platforms hosted on different physical infrastructures in order to separate historical consumer activities from new activities that would require more advanced certification:

- WITHINGS Consumer Cloud;
- WITHINGS Certified Cloud(s), also called WITHINGS Medical Cloud(s).

In order to meet international regulations for those activities and customers expectations, WITHINGS has decided to implement:

- An Information Security Management System (ISMS) that is compliant with ISO 27001:2017;
- A Privacy Information Management System (PIMS) that is compliant with ISO 27701:2019.

Purpose

WITHINGS is committed to protecting the security and privacy of its business information in the face of incidents and unwanted events and has implemented both an Information Security Management System (ISMS) and a Privacy Information Management System which are respectively compliant with ISO/IEC 27001:2017 and ISO 27701:2019, the international standards for information security and privacy (see below the full Withings Compliance Program).

The purposes of the ISMS/PIMS are to:

1. Understand the organization's needs and the necessity for establishing information security/privacy management policy and objectives;
2. Implement and operate controls and measures for managing the organization's overall capability to manage information security/privacy incidents;
3. Monitor and review the performance and effectiveness of the ISMS;
4. Continually improve the organization's information security and privacy based on objective measurement.

Scope

The scope of the ISO 27001:2017, ISO 27701:2019 and HDS certifications of WITHINGS Information Security and Privacy Management System (ISMS & PIMS) includes all systems, people and processes that are involved in the design, development, operations, validation and support of applications and services that are hosted on the WITHINGS Medical Cloud(s), and processing or disclosing Protected Health Information (PHI). Locations include the WITHINGS headquarters in Issy-les-Moulineaux, France.

As a non-exhaustive list, the following products and services are within the scope of the ISMS/PIMS, when they are hosted in Medical Cloud(s), along with the data contained or collected by those offerings:

- WITHINGS RPM;
- WITHINGS API;
- Data Collection Service, using WITHINGS IoT and/or WITHINGS Mobile Application and/or WITHINGS SDK;
- All other future products and services that are hosted on the certified cloud.



The departmental scope for this ISMS/PIMS comprises:



- Product Management team (HQ);
- Software Development team (HQ);
- Cloud Engineering team (HQ);
- Software Quality Assurance team (HQ);
- Customer Support Team (HQ);
- Research & Development team (HQ);
- Data Science team (HQ);
- Legal team (HQ);
- Human Resources team (HQ).


WITHINGS Compliance Program

In addition to documenting our approach to security and privacy design, WITHINGS undergoes several independent third-party audits on a regular basis to provide customers with external verification. WITHINGS also performs self-assessment when there is no formal certification recognized by the regulatory body, such as HIPAA or GDPR.

To avoid any confusion, external certifications by certification bodies and self-assessments are explicitly mentioned below.

Standard	Compliance		Description
<p>ISO/IEC 27001:2017</p> 	<p>AFNOR Certification - N° 2020 / 86561.1</p>	<p>Security</p>	<p>The ISO/IEC 27001:2017 is a security world-class standard that outlines and provides the requirements for an information security management system (ISMS). WITHINGS has passed the certification with the independent certification body, AFNOR.</p> <p>Certificate available on our website.</p>
<p>HDS v1.1 2018</p> 	<p>AFNOR Certification - N° 2020 / 86563.5</p>	<p>All</p>	<p>Introduced by the French governmental agency for health, ASIP Santé (Agence Française de la Santé Numérique), HDS provides a framework to strengthen the security and protection of PHI. For more information.</p> <p>HDS certification provides the necessary assurance of information security for companies who wish to host the healthcare data of French citizens in the cloud and validates that WITHINGS ensures data confidentiality, integrity, and availability to its customers and partners.</p> <p>HDS framework is based on several ISO standards that guarantee global equivalences:</p> <ul style="list-style-type: none"> • ISO/IEC 27001:2017: the full standard requirements are included in HDS • ISO/IEC 27018:2014: the full standard requirements are included in HDS • ISO/IEC 20000-1:2011: the part 1 of the standard is included in HDS • Additional controls <p>WITHINGS has passed the certification with the independent certification body, AFNOR.</p> <p>Certificate available on our website.</p>

Standard	Compliance		Description
<p>ISO/IEC 27701:2019</p> 	<p>AFNOR Certification - N° 2023/104367.1</p>	<p>Privacy</p>	<p>The ISO/IEC 27701:2019 is a privacy world-class standard that outlines and provides the requirements for a Privacy Information Management System (PIMS). WITHINGS has passed the certification with the independent certification body, AFNOR.</p> <p>Certificate available on our website.</p>
<p>HIPAA</p> 	<p>Self assessment</p>	<p>All</p>	<p>The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law that mandates national standards to protect the privacy and security of protected health information (PHI).</p> <p>As a business associate, WITHINGS has assessed its HIPAA compliance on all Security Rules, Privacy Rules and Breach Notification Rules based on the cross-correlation with its ISO 270001, ISO 27701 and HDS certifications.</p> <p>There is no formal certification recognized by the regulatory body.</p>

Standard	Compliance	Description
<p>GDPR</p> 	<p>Self assessment Privacy</p>	<p>The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.</p> <p>WITHINGS complies with GDPR regulation in all its activities by:</p> <ul style="list-style-type: none"> • Receiving the informed consent of the data subject to process the information. The consent is specific to the exposed purpose of treatment and is an unambiguous affirmation given by the data subject; • Maintaining transparent information, communication and modalities for the exercise of the rights of the data subject (access, rectification, erasure, limitation, transfer, etc.); • Maintaining a Privacy Policy, a Data Protection Addendum, a Processing Register, and several Privacy Impact Assessment; • Appointing a Data Protection Officer (DPO). <p>GDPR compliance is enforced by the ISO 27001, ISO 27701 and HDS certifications. HDS certification also ensures ISO/IEC 27018 and ISO/IEC 20000-1 control implementations.</p> <p>There is no formal certification recognized by the regulatory body.</p>

WITHINGS Compliance Program mapping to HIPAA requirements

The cross-reference matrix below presents how WITHINGS Compliance Program is covering the HIPAA rules and requirements. It shows that the WITHINGS ISMS, which is certified ISO 27001:2017, ISO 27701:2019 and HDS v1.1:2018, is the best tool to manage information security in compliance with HIPAA/HITECH and HHS guidelines. As a reminder, HDS is the regulatory framework to process electronic Protected Health Information (ePHI) in France.

This matrix is provided for informational purposes only. The content herein is correct as of the time it was written. National and international standards may change due to law modification or WITHINGS internal policies, and measures may change as WITHINGS continually improves its ISMS/PIMS for better customer protection. Customers are responsible for making their own independent assessment of HIPAA. WITHINGS cannot be held responsible for any assessment performed based on the following table.

HIPAA Security rules - Administrative safeguards

HIPAA Rules References		ISO 27001:2017 / ISO 27018:2014 / / ISO 20000-1:2011 References
Security rules	Administrative safeguards	164.308(a)(1)(i) - Security Management Process 5.2 Information Security Policy A.5.1.1 Policies for information security A.5.1.2 Review of the policies for information security

Security rules	Administrative safeguards	164.308(a)(1)(ii)(A) – Risk Analysis	<ul style="list-style-type: none"> 8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment
Security Rules	Administrative safeguards	164.308(a)(1)(ii)(A) – Risk Analysis	<ul style="list-style-type: none"> A.12.7.1 Information systems audit controls A.18.2.3 Technical compliance review
Security Rules	Administrative safeguards	164.308(a)(1)(ii)(B) – Risk Management	<ul style="list-style-type: none"> 6.1 Actions to address risks and opportunities A.9.1.1 Access control policy A.9.2.1 User registration and deregistration A.9.2.2 User access provisioning A.9.2.3 Management of privileged access rights A.9.2.4 Management of secret authentication information of users A.9.2.5 Review of user access rights A.9.2.6 Removal or adjustment of access rights A.12.2.1 Controls against malware A.12.6.1 Management of technical vulnerabilities A.13.1.1 Network controls A.13.1.2 Security of network services

Security rules	Administrative safeguards	164.308(a)(1)(ii)(C) – Sanction Policy	A.7.2.1 Management responsibilities A.7.2.3 Disciplinary process A.13.2.4 Confidentiality or nondisclosure agreements
Security Rules	Administrative safeguards	164.308(a)(1)(ii)(D) – Information System Activity Review	9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review A.18.2.1 Independent review of information security A.18.2.2 Compliance with security policies and standards
Security Rules	Administrative safeguards	164.308(a)(2) – Assigned security responsibility	5.3 Organizational roles, responsibilities and authorities A.6.1.1 Information security roles and responsibilities
Security Rules	Administrative safeguards	164.308(a)(3)(i) – Workforce security	A.6.1.2 Segregation of duties A.7.1.1 Screening A.7.1.2 Terms and conditions of employment A.7.2.1 Management responsibilities A.7.3.1 Termination or change of employment responsibilities

Security rules	Administrative safeguards	164.308(a)(4)(i) - Information access management	A.7.1.2 Terms and conditions of employment A.9.1.1 Access control policy A.13.2.4 Confidentiality or nondisclosure agreements
Security Rules	Administrative safeguards	164.308(a)(5)(i) - Security awareness and training	7.3 Awareness A.7.2.2 Information security awareness, education and training
Security Rules	Administrative safeguards	164.308(a)(6)(i) - Security incident procedures	A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses A.16.1.4 Assessment of and decision on information security events A.16.1.5 Response to information security incidents A.16.1.6 Learning from information security incidents A.16.1.7 Collection of evidence

<p>Security rules</p>	<p>Administrative safeguards</p>	<p>164.308(a)(6)(i) - Security incident procedures</p>	<p>ISO 27018 4.4.3.2 PII disclosure notification ISO 27018 4.4.3.3/4 Recording of PII disclosures ISO 27018 4.4.5.1 Notification of a data breach involving PII ISO 27018 4.4.6.12 Contract measures</p>
<p>Security Rules</p>	<p>Administrative safeguards</p>	<p>164.308(a)(7)(i) - Contingency plan</p>	<p>A.12.1.3 Capacity management A.17.1.1 Planning information security continuity A.17.1.2 Implementing information security continuity A.17.1.3 Verify, review and evaluate information security continuity A.17.2.1 Availability of information processing facilities ISO20000 6.3 Management of service continuity and availability ISO20000 6.5 Capacity management</p>
<p>Security Rules</p>	<p>Administrative safeguards</p>	<p>164.308(a)(8) - Evaluation</p>	<p>9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review 10.1 Nonconformity and corrective action 10.2 Continual improvement</p>

HIPAA Security rules - Physical safeguards

HIPAA Rules References		ISO 27001:2017 / ISO/IEC 27018:2014 / ISO 20000-1:2011 References
Security rules	Physical safeguards	164.310(a)(1) - Facility access controls
		<ul style="list-style-type: none"> A.11.1.1 Physical security perimeter A.11.1.2 Physical entry controls A.11.1.3 Securing offices, rooms and facilities A.11.1.4 Protecting against external and environmental threats A.11.1.5 Working in secure areas A.11.1.6 Delivery and loading areas

Security rules

Physical safeguards

164.310(b) - Workstation use

- A.6.2.1 Mobile device policy
- A.6.2.2 Teleworking
- A.9.2.4 Management of secret authentication information of users
- A.9.2.5 Review of user access rights
- A.9.2.6 Removal or adjustment of access rights
- A.9.3.1 Use of secret authentication information
- A.9.4.1 Information access restriction
- A.9.4.2 Secure log-on procedures
- A.9.4.3 Password management system
- A.10.1.1 Policy on the use of cryptographic controls
- A.10.1.2 Key management
- A.11.2.1 Equipment siting and protection
- A.11.2.4 Equipment maintenance
- A.11.2.5 Removal of assets
- A.11.2.6 Security of equipment and assets off-premises
- A.11.2.7 Secure disposal or reuse of equipment
- A.11.2.8 Unattended user equipment
- A.11.2.9 Clear desk and clear screen policy
- A.12.2.1 Controls against malware
- A.12.5.1 Installation of software on operational systems
- A.12.6.2 Restrictions on software installation
- A.18.1.2 Intellectual property rights

<p>Security rules</p>	<p>Physical safeguards</p>	<p>164.310(d)(1) – Device and media controls</p>	<p>A.8.1.1 Inventory of assets A.8.1.2 Ownership of assets A.8.1.3 Acceptable use of assets A.8.1.4 Return of assets</p>
<p>Security Rules</p>	<p>Physical safeguards</p>	<p>164.310(d)(2)(iv) – Data backup and storage</p>	<p>A.12.3.1 Information backup A.17.1.1 Planning information security continuity A.17.1.2 Implementing information security continuity A.17.1.3 Verify, review and evaluate information security continuity A.17.2.1 Availability of information processing facilities A.18.1.3 Protection of records ISO 27018 4.4.6.3 Control and logging of data restoration ISO20000 6.3 Management of service continuity and availability ISO20000 6.5 Capacity management</p>

HIPAA Security rules - Technical safeguards

HIPAA Rules References			ISO 27001:2017 / ISO/IEC 27018:2014 / ISO 20000-1:2011 References
Security rules	Technical safeguards	164.312(a)(1) - Access control	A.7.1.2 Terms and conditions of employment A.9.1.1 Access control policy A.13.2.4 Confidentiality or nondisclosure agreements
Security rules	Technical safeguards	164.312(a)(2)(iv) - Encryption and decryption	A.10.1.1 Policy on the use of cryptographic controls A.10.1.2 Key management A.18.1.5 Regulation of cryptographic controls ISO 27018 4.4.6.6 Encryption of PII transmitted over public data transmission networks
Security rules	Technical safeguards	164.308(a)(1)(ii)(D) and 164.312(b) - Audit controls	A.7.3.1 Termination or change of employment responsibilities A.9.1.2 Access to networks and network services A.12.4.1 Event logging A.12.4.2 Protection of log information A.12.4.3 Administrator and operator logs A.12.4.4 Clock synchronization

Security rules	Technical safeguards	164.312(e)(2)(ii) - Encryption	A.8.2.1 Classification of information A.8.2.2 Labeling of information A.8.2.3 Handling of assets A.10.1.1 Policy on the use of cryptographic controls A.10.1.2 Key management A.18.1.5 Regulation of cryptographic controls ISO 27018 4.4.6.6 Encryption of PII transmitted over public data transmission networks
----------------	----------------------	--------------------------------	--

HIPAA Rules References		ISO 27001:2017 / ISO/IEC 27018:2014 / ISO 20000-1:2011 References
Security rules	Organizational safeguards	164.314(a)(2)(i) - Business associate contracts A.13.2.4 Confidentiality or nondisclosure agreements A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain A.15.2.1 Monitoring and review of supplier services A.15.2.2 Managing changes to supplier services A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.4 Privacy and protection of personally identifiable information ISO 27018 4.4.4.1 Disclosure of subcontracted PII processing ISO 27018 4.4.6.12 Contract measures ISO 27018 4.4.6.13 Sub-contracted PII processing

<p>Security rules</p>	<p>Organizational safeguards</p>	<p>164.314(a)(2)(iii) – Business associate contracts with subcontractors</p>	<p>A.13.2.4 Confidentiality or nondisclosure agreements A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain A.15.2.1 Monitoring and review of supplier services A.15.2.2 Managing changes to supplier services A.18.1.4 Privacy and protection of personally identifiable information ISO 27018 4.4.4.1 Disclosure of subcontracted PII processing ISO 27018 4.4.6.12 Contract measures ISO 27018 4.4.6.13 Sub-contracted PII processing</p>
-----------------------	----------------------------------	--	--

Security rules	Organizational safeguards	164.314(a)(2)(iii) - Business associate contracts with subcontractors	<p>A.13.2.4 Confidentiality or nondisclosure agreements A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain A.15.2.1 Monitoring and review of supplier services A.15.2.2 Managing changes to supplier services A.18.1.4 Privacy and protection of personally identifiable information ISO 27018 4.4.4.1 Disclosure of sub- contracted PII processing ISO 27018 4.4.6.12 Contract measures ISO 27018 4.4.6.13 Sub-contracted PII processing</p>
Security rules	Organizational safeguards	164.314(a)(2)(i) - Business associate contracts	<p>A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain A.15.2.1 Monitoring and review of supplier services A.15.2.2 Managing changes to supplier services</p>
Security rules	Organizational safeguards	164.316 - Policies and procedures and documentation requirements	<p>5.2 Information Security Policy ISO 27018 4.4.6.12 Contract measures + almost all references</p>

HIPAA Rules References		ISO 27001:2017 / ISO/IEC 27018:2014 / ISO 20000-1:2011 References	
Privacy rules	Uses and disclosures: Organizational requirements	164.504(e)(2) - Implementation Specifications: Business Associate Contracts	ISO 27018 4.4.5.3 PII return, transfer and disposal
Privacy Rules	Uses and disclosures: Organizational requirements	164.504(e)(2) - Implementation Specifications: Business Associate Contracts	<ul style="list-style-type: none"> A.8.3.1 Management of removable media A.8.3.2 Disposal of media A.8.3.3 Physical media transfer A.11.2.4 Equipment maintenance A.11.2.5 Removal of assets A.11.2.6 Security of equipment and assets off-premises A.11.2.7 Secure disposal or reuse of equipment ISO 27018 4.4.5.3 PII return, transfer and disposal ISO 27018 4.4.6.2 Restriction of the creation of hard copy material ISO 27018 4.4.6.4 Protecting data on storage media leaving the premises ISO 27018 4.4.6.5 Use of unencrypted portable storage media and devices ISO 27018 4.4.6.7 Secure disposal of hard copy materials

HIPAA Mapping

Privacy Rules	Uses and disclosures: Organizational requirements	164.504(e)(2) - Implementation Specifications: Business Associate Contracts	ISO 27018 4.4.7.1 Geographical location of PII Additional Requirements 4.5.5. Regionalization
Privacy Rules	Uses and disclosures: Organizational requirements	164.504(e)(2) - Implementation Specifications: Business Associate Contracts	7.3 Awareness A.7.2.2 Information security awareness, education and training A.7.1.2 Terms and conditions of employment A.13.2.4 Confidentiality or nondisclosure agreements
Privacy Rules	Uses and disclosures: Organizational requirements	164.504(e)(4) - Implementation Specifications: Other Requirements for Contracts and Other Arrangements	A.7.1.2 Terms and conditions of employment A.13.2.4 Confidentiality or nondisclosure agreements A.16.1.7 Collection of evidence A.18.1.1 Identification of applicable legislation and contractual requirements ISO 27018 4.4.2.1 Public cloud PII processor's purpose ISO 27018 4.4.2.2 Public cloud PII processor's commercial use
Privacy Rules	Access of individuals to protected health information	164.524 - Access of Individuals to Protected Health Information	ISO 27018 4.4.1.1 Obligation to cooperate regarding PII principals' rights ISO 27018 4.4.5.3 PII return, transfer and disposal

HIPAA Mapping

Privacy Rules	Amendment of protected health information	164.526 - Amendment of Protected Health Information	ISO 27018 4.4.1.1 Obligation to cooperate regarding PII principals' rights ISO 27018 4.4.5.3 PII return, transfer and disposal
Privacy Rules	Accounting of disclosures of protected health information	164.528(a) - Right to an Accounting of Disclosures	A.16.1.7 Collection of evidence A.18.1.1 Identification of applicable legislation and contractual requirements

HIPAA Breach Notification rules

HIPAA Rules References			ISO 27001:2017 / ISO/IEC 27018:2014 / ISO 20000-1:2011 References
Breach Notification Rules	Notification	164.404 - Notification to individuals	ISO 27018 4.4.3.2 PII disclosure notification ISO 27018 4.4.3.3/4 Recording of PII disclosures ISO 27018 4.4.5.1 Notification of a data breach involving PII
Breach Notification Rules	Notification	164.406 Notification to the media	ISO 27018 4.4.3.2 PII disclosure notification ISO 27018 4.4.3.3/4 Recording of PII disclosures ISO 27018 4.4.5.1 Notification of a data breach involving PII
Breach Notification Rules	Notification	164.408 - Notification to the Secretary	ISO 27018 4.4.3.2 PII disclosure notification ISO 27018 4.4.3.3/4 Recording of PII disclosures ISO 27018 4.4.5.1 Notification of a data breach involving PII

HIPAA Mapping

Breach Notification Rules	Notification	164.410 - Notification by a business associate	ISO 27018 4.4.3.2 PII disclosure notification ISO 27018 4.4.3.3/4 Recording of PII disclosures ISO 27018 4.4.5.1 Notification of a data breach involving PII
Breach Notification Rules	Law enforcement	164.412 - Law enforcement delay	10.1 Nonconformity and corrective action
Breach Notification Rules	Administrative requirements and burden of proof	164.414 - Administrative requirements and burden of proof	A.16.1.7 Collection of evidence A.18.1.1 Identification of applicable legislation and contractual requirements