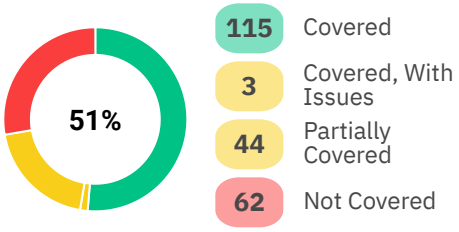
Controls Assessment Printable Report

Standards Coverage



CC1.1	CC1.2	CC1.3	CC1.5
CC2.1	CC2.2	CC2.4	CC2.8
CC2.11	CC2.12	CC2.13	CC2.14
CC2.15	CC3.1	CC4.1	CC5.1
CC5.2	CC7.1	CC7.2	CC7.3
CC7.4	CC7.5	CC7.6	CC7.7
CC7.8	CC7.16	CC7.17	CC7.18
CC7.19	CC7.20	CC8.1	CC8.2
CC8.3	CC8.4	CC8.5	CC8.6
CC8.7	CC8.8	CC8.10	CC8.13
CC8.14	CC8.15	CC8.16	CC8.18
CC8.24	CC8.30	CC8.41	CC8.42
CC9.2	CC9.4	CC10.1	CC11.1
CC13.1	CC13.5	CC13.6	CC14.1
CC14.2	CC14.4	CC14.7	CC14.8
CC14.9	CC14.10	CC14.12	CC14.13
CC14.15	CC14.18	CC16.1	CC17.1
CC17.2	CC17.5	CC17.6	CC17.7
CC17.8	CC17.9	CC17.10	CC17.11
CC17.12	CC18.2	CC18.6	CC18.7
CC18.8	CC18.10	CC18.11	CC18.12
CC18.13	CC18.14	CC18.15	CC18.16

CC18.17	CC18.18	CC18.19	CC19.1
CC19.3	CC19.4	CC19.5	CC19.6
CC19.7	CC19.8	CC19.14	CC19.15
CC19.16	CC19.17	CC19.19	CC19.20
CC19.21	CC19.22	CC20.1	CC20.2
CC20.3	CC20.4	CC20.5	CC20.6
HPR-1	HPR-2	HPR-3	HPR-4
HPR-5	HPR-6	HPR-7	HPR-8
HPR-9	HPR-10	HPR-11	HPR-12
HPR-13	HPR-14	HPR-15	HPR-16
HPR-17	HPR-18	HPR-19	HPR-20
HPR-21	HPR-22	HPR-23	HPR-24
HPR-25	HPR-26	HPR-27	HPR-28
HPR-29	HPR-30	HPR-31	HPR-32
HPR-33	HPR-34	HPR-35	HPR-36
HPR-37	HPR-38	HPR-39	HPR-40
HPR-41	HPR-42	HPR-43	HPR-44
HPR-45	HPR-46	HPR-47	HPR-48
HPR-49	HPR-50	HPR-51	HPR-52
HPR-53	HPR-54	HPR-55	HPR-56
HPR-57	HPR-58	HPR-59	HPR-60
HPR-61	HPR-62	HPR-63	HPR-64
HPR-65	HPR-66	HPR-67	HPR-68
HPR-69	HPR-70	HPR-71	HPR-72
HPR-73	HPR-74	HPR-75	HPR-76
HPR-77	HPR-78	HPR-79	HPR-80
HPR-81	HPR-82	HPR-83	HPR-84
HPR-85	HPR-86	HPR-87	HPR-88
HPR-89	HPR-90	HPR-91	HPR-92

HPR-93	HBNR-1	HBNR-2	HBNR-3
HBNR-4	HBNR-5	HBNR-6	HBNR-7
HBNR-8	HBNR-9	HBNR-10	HBNR-11
HBNR-12	HBNR-13	HBNR-17	HBNR-18
HBNR-19	CSS1	CSS2	CSS3

Inventories

No

Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, i..

Active Standards

NIST CSF

ID.AM-1
ID.AM-2
ID.AM-3
ID.AM-4

Data Locations

Yes, With Issues

Locate and identify all organizational data, including data stored on local devices, mobile devices, servers, mass storage, p..

Active Standards

NIST CSF

ID.AM-3

Data Flow Mapping

Yes, Fully

Create a map of how data flows within and in/out of the organization.

Active Standards

NIST CSF

ID.AM-3

Baseline Configurations

Yes, Fully

Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile devices,..

Active Standards

NIST CSF

DE.AE-1
PR.IP-1

Implement Logging/Audit Controls

Yes, Fully

Ensure that audit/log records are implemented to record and examine activities on local devices, network devices, and cloud s..

Active Standards

NIST CSF

PR.PT-1

Physical Access Policies

Yes, Fully

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tamp..

Active Standards

NIST CSF

PR.IP-5

In-transit Data Protection

Yes, Fully

Ensure data-in-transit is protected.

Active Standards

NIST CSF

PR.DS-2

Monitor, Control, and Protect Communications

No

Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational info..

Active Standards

NIST CSF

PR.PT-4

Implement Subnetworks

Yes, Partially

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal netw..

Active Standards

Business Continuity & Disaster Recovery Plans

No

Write effective Business Continuity and Disaster Recovery plans that meet all regulatory requirements and are in place and ma..

Active Standards

NIST CSF

PR.IP-9

Resource Criticality

No

Establish and communicate the criticality of all resources.

Active Standards

NIST CSF

ID.AM-5

Organizational Priorities

No

Establish and communicate priorities based on the organization's mission, objectives, activities, legal requirements, and reg..

Active Standards

NIST CSF

ID.BE-3

Dependencies

Yes, Fully

Identify and document all dependencies for each critical function. Include technology, people, and facilities.

Active Standards

NIST CSF

ID.BE-4

Resliency Requirements

No

Establish resilience requirements to support the delivery of critical services.

Active Standards

NIST CSF

ID.BE-5

Business Impact Analysis

No

Conduct Business Impact Anlyses (BIA) with all departments to measure the financial, regulatory, and reputational impact of i..

Active Standards

NIST CSF

ID.RA-5

Likelihood Analysis

No

Determine the likelihood of an incident based on historical information and other resources.

Active Standards

NIST CSF

ID.RA-5

Data Backup Plan

Yes, Fully

Write a comprehensive data backup plan that identifies the locations of all business-critical and regulated data, and the det..

Active Standards

NIST CSF

PR.IP-10

Backups

Yes, Partially

Ensure all business-critical and regulated data is backed up regularly to meet the organization's recovery priorities. Includ..

Active Standards

NIST CSF

PR.IP-4

Restoration Testing

Yes, Partially

Ensure that backups are fully tested on a regular schedule to ensure that recoveries can take place as planned.

Active Standards

NIST CSF

PR.IP-4

Recovery Capability Testing

Ensure that restoration testing proves that the RTO and RPO's can be met. If not, adjust the RTO and RPO to what has been pro..

Yes, Partially

Active Standards

NIST CSF

PR.IP-10

Workforce Training

Implement workforce training that covers all required policies and procedures.

Yes, Partially

Active Standards

NIST CSF

PR.AT-1

Vulnerability Scans

Scan for vulnerabilities and encryption status in organizational systems and applications periodically and when new vulnerabi..

Yes, Partially

Active Standards

NIST CSF

DE.CM-8

Vulnerability Plan

Ensure that a written vulnerability management plan is developed and implemented.

Yes, Partially

Active Standards

NIST CSF

PR.IP-12

Identify Threats

Yes, Partially

Identify and document threats, both internal and external.

Active Standards

NIST CSF

ID.RA-3

Threat and Vulnerability Information

Yes, Fully

Receive and respond to threat and vulnerability information from information sharing forums and sources and communicate to st..

Active Standards

NIST CSF

ID.RA-2

Risk Determination

Yes, Partially

Determine risk using threats, vulnerabilities, likelihoods, and impacts.

Active Standards

NIST CSF

ID.RA-5

Risk Responses

Yes, Fully

Risk responses are identified and prioritized.

Active Standards

NIST CSF

ID.RA-6

Risk Management

Yes, Partially

Establish and manage risk management processes as agreed to by organizational stakeholders.

Active Standards

NIST CSF

ID.RM-1

Risk Tolerance

Yes, Partially

Organization risk tolerance is determined and clearly expressed.

Active Standards

NIST CSF

ID.RM-2

Risk Tolerance Alignment

No

Risk management aligns with all legal and regulatory requirements, the organization's role in critical infrastructure, and a ..

Active Standards

NIST CSF

ID.RM-3

Newly-Identified Vulnerabilities

Yes, Partially

Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.

Active Standards

NIST CSF

RS.MI-3

Triage Events

Yes, With Issues

Analyze and triage events to support event resolution and incident declaration.

Active Standards

NIST CSF

DE.AE-2

Event Data Correlation

Yes, Fully

Ensure that event data are aggregated and correlated from multiple sources and sensors.

Active Standards

NIST CSF

DE.AE-3

Event Impact Determination

Yes, Fully

Ensure that the impact of events is determined.

Active Standards

NIST CSF

DE.AE-4
ID.RA-4
RS.AN-2

Incident Alert Thresholds

Yes, Fully

Ensure that incident alert thresholds are established.

Active Standards

NIST CSF

DE.AE-5

Physical Environment Monitoring

Yes, Fully

Active Standards

NIST CSF

DE.CM-2

Personnel Activity Monitoring

Yes, Fully

Ensure that personnel activity is monitored to detect potential cybersecurity events.

Active Standards

NIST CSF

DE.CM-3

Malicious Code Detection

Yes, Fully

Ensure that malicious code is detected.

Active Standards

NIST CSF

DE.CM-4

Mobile Code Detection

Yes, Fully

Ensure that unauthorized mobile code is detected.

Active Standards

NIST CSF

DE.CM-5

Monitor Service Provider Activity

No

Ensure that external service provider activity is monitored to detect potential cybersecurity events.

Active Standards

NIST CSF

DE.CM-6

Monitoring

Yes, Partially

Ensure that monitoring the network for unauthorized personnel, connections, devices, and software is performed.

Active Standards

NIST CSF

DE.CM-1
DE.CM-7

Detection Compliance

Yes, Fully

Ensure that detection activities comply with all applicable requirements.

Active Standards

NIST CSF

DE.DP-2

Test Detection Processes

Yes, Fully

Ensure that detection processes are tested.

Active Standards

NIST CSF

DE.DP-3

Detection Information Communications

Yes, Fully

Ensure that event detection information is communicated to appropriate parties.

Active Standards

NIST CSF

DE.DP-4

Improve Detection Processes

Yes, Fully

Ensure that detection processes are continuously improved.

Active Standards

NIST CSF

DE.DP-5

Incident Response Plan

Yes, Fully

Ensure that an effective Incident Response Plan is in place and managed.

Active Standards

NIST CSF

RS.RP-1

Contain Incidents

Yes, Fully

Ensure that incidents are contained.

Active Standards

NIST CSF

RS.MI-1

Mitigate Incidents

Yes, Fully

Ensure that incidents are mitigated.

Active Standards

NIST CSF

RS.MI-2

Perform Forensics

Yes, Fully

Ensure that forensics are performed.

Active Standards

NIST CSF

RS.AN-3

Categorize Incidents

Yes, Fully

Ensure that incidents are categorized consistent with response plans.

Active Standards

NIST CSF

RS.AN-4

Understand Incident Impact

Yes, Fully

Ensure that the impact of an incident is understood.

Active Standards

NIST CSF

ID.RA-4

Investigate Detection System Notifications

Yes, Fully

Ensure that notifications from detection systems are investigated.

Active Standards

NIST CSF

RS.AN-1

Personnel Incident Responsibilities

Yes, Fully

Ensure that personnel know their roles, limitations, and order of operations when a response is needed.

Active Standards

NIST CSF

RS.CO-1

Incident Reporting Determination

Yes, Fully

Determine that the incident meets the requiremends for reporting.

Active Standards

NIST CSF

RS.CO-2

Incident Documentation & Reporting

Yes, Partially

Ensure that events are documented and reported consistent with established criteria, including all legal and regulatory requi..

Active Standards

NIST CSF

RS.CO-2

Incident Information Sharing

Yes, Partially

Ensure that information is shared consistent with response plans.

Active Standards

NIST CSF

RS.CO-3

Stakeholder Incident Coordination

Yes, Fully

Ensure that coordination with stakeholders occurs consistent with response plans, legal advice, law enforcement requirements,..

Active Standards

NIST CSF

RS.CO-4

Stakeholder Information Sharing

Yes, Fully

Ensure that voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awar..

Active Standards

NIST CSF

RS.CO-5

Response Plan Lessons Learned

Yes, Fully

Active Standards

NIST CSF

RS.IM-1

Update Response Strategies

Yes, Fully

Ensure response strategies are updated.

Active Standards

NIST CSF

RS.IM-2

Organization's Supply Chain Role

Yes, Fully

Identify and communicate the organization's role in the supply chain.

Active Standards

NIST CSF

ID.BE-1

Organization's Critical Infrastructure Role

Yes, Partially

Identify and communicate the organization's role in critical infrastructure.

Active Standards

NIST CSF

ID.BE-2

Workforce Cybersecurity Roles & Responsibilities

Yes, Fully

Establish and document cybersecurity roles and responsibilities within the workforce.

Active Standards

NIST CSF

ID.AM-6

Roles & Responsibilities Coordination

Yes, Fully

Coordinate and align information security roles & responsibilities with internal roles and external partners.

Active Standards

NIST CSF

ID.GV-2

Detection Roles & Responsibilities

Yes, Fully

Ensure that roles and responsibilities for detection are well defined to ensure accountability.

Active Standards

NIST CSF

DE.DP-1

Privileged Users

Yes, Fully

Ensure privileged users understand roles & responsibilities

Active Standards

NIST CSF

PR.AT-2

Third-Parties

Yes, Fully

Ensure third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

Active Standards

NIST CSF

PR.AT-3

Senior Executives

Yes, Fully

Ensure senior executives understand roles & responsibilities.

Active Standards

NIST CSF

PR.AT-4

Physical Security Personnel

Yes, Fully

Ensure physical security personnel understand their roles & responsibilities and are trained to perform them.

Active Standards

NIST CSF

PR.AT-5

Follow Incident Recovery Plan

Yes, Partially

Ensure the recovery plan is executed during or after an event.

Active Standards

NIST CSF

RC.RP-1

Recovery Plan Lessons Learned

Yes, Fully

Ensure recovery plans incorporate lessons learned.

Active Standards

NIST CSF

RC.IM-1

Update Recovery Strategies

Yes, Fully

Ensure recovery strategies are updated.

Active Standards

NIST CSF

RC.IM-2

Manage Public Relations

Yes, Fully

Ensure public relations are managed.

Active Standards

NIST CSF

RC.CO-1

Reputation Repair

Yes, Fully

Ensure that the organization's reputation after an event is repaired.

Active Standards

NIST CSF

RC.CO-2

Communicate Recovery Activities

Yes, With Issues

Ensure that recovery activities are communicated to internal stakeholders and executive and management teams.

Active Standards

NIST CSF

RC.CO-3

Legal and Regulatory Requirements

Yes, Fully

Identify and manage all legal and regulatory requirements.

Active Standards

NIST CSF

ID.GV-3

Written Cybersecurity Policies

Yes, Fully

Write policies addressing all cybersecurity requirements.

Active Standards

NIST CSF

ID.GV-1

Risk Assessment/Risk Analysis

Yes, Fully

Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functi..

Active Standards

NIST CSF

ID.RA-1

Prioritize Risks

Yes, Fully

Prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

Active Standards

NIST CSF

ID.GV-4

Identity Management

Yes, Partially

Manage identities and credentials for authorized devices and users.

Active Standards

NIST CSF

PR.AC-1

Physical Access Management

Yes, Fully

Manage and protect physical access to assets.

Active Standards

NIST CSF

PR.AC-2

Remote Access Management

No

Manage remote access to assets.

Active Standards

NIST CSF

PR.AC-3

Access Permission Management

No

Manage access permissions, incorporating the principles of least privilege and separation of duties.

Active Standards

NIST CSF

PR.AC-4

Network Segregation

No

Protect network integrity, incorporating network segregation where appropriate.

Active Standards

NIST CSF

PR.AC-5

HR Cybersecurity Alignment

No

Ensure that cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

Active Standards

NIST CSF

PR.IP-11

Unique User Identification

Yes, Fully

Assign a unique name and/or number for identifying and tracking user identity.

Active Standards

Identity Authentication

Yes, Fully

Implement procedures to verify that a person or entity seeking access to data is the one claimed.

Active Standards

Identify System Users

Yes, Fully

Identify information system users, processes acting on behalf of users, or devices.

Active Standards

Escort & Monitor Visitors

Yes, Fully

Escort visitors and monitor visitor activity.

Active Standards

Facility Security Plan

No

Implement documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical a..

Active Standards

Physical Access Devices

No

Control and manage physical access devices.

Active Standards

Physical Access Logs

No

Maintain audit logs of physical access.

Active Standards

Protect Data

No

Ensure data-at-rest (stored) is protected.

Active Standards

NIST CSF

PR.DS-1

Manage Assets

No

Ensure assets are formally managed throughout removal, transfers, and disposition.

Active Standards

NIST CSF

PR.DS-3

Ensure Adequate Capacity

No

Ensure there is adequate capacity to ensure availability is maintained.

Active Standards

NIST CSF

PR.DS-4

Protect Against Data Leaks

No

Protections against data leaks are implemented.

Active Standards

NIST CSF

PR.DS-5

Integrity Checking

No

Use integrity checking mechanisms to verify software, firmware, and information integrity.

Active Standards

NIST CSF

PR.DS-6

Separate Development & Testing Environments

No

Separate development and testing environment(s) from the production environment.

Active Standards

NIST CSF

PR.DS-7

Implement Life Cycle

No

Implement a System Development Life Cycle to manage systems.

Active Standards

NIST CSF

PR.IP-2

Change Controls

No

Ensure configuration change control processes are in place.

Active Standards

NIST CSF

PR.IP-3

Data Destruction

No

Ensure data is destroyed according to policy, including deleting data no longer required for business purposes, and beyond an..

Active Standards

NIST CSF

PR.IP-6

Improve Processes

No

Continuously improve data protection processes.

Active Standards

NIST CSF

PR.IP-7

Share Effectiveness Information

No

Share the effectiveness of protection technologies with appropriate parties.

Active Standards

NIST CSF

PR.IP-8

Protect & Restrict Removable Media

No

Ensure that removable media is protected and its use restricted according to policy.

Active Standards

NIST CSF

PR.PT-2

Control & Limit Access

No

Ensure that access to systems and assets is controlled, incorporating the principle of least functionality.

Active Standards

NIST CSF

PR.PT-3

Install Patches & Updates

Ensure that all software and firmware are updated with patches and updates within 7 days of becoming available, unless warnin..

No

Active Standards

Disposal

Implement policies and procedures to address the final disposition of electronic data and/or the hardware or electronic media..

Yes, Fully

Active Standards

Update Protection

Update malicious code protection mechanisms when new releases are available.

Yes, Partially

Active Standards

Incident Management Process

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analys..

No

Active Standards

NIST CSF

PR.IP-9

Scan Files

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, ..

Yes, Partially

Active Standards

Perform & Control Maintenance & Repairs

Yes, Fully

Ensure maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controll..

Active Standards

NIST CSF

PR.MA-1

Manage Remote Maintenance

Yes, Fully

Ensure that remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthor..

Active Standards

NIST CSF

PR.MA-2

Cyber Security Standard 1

Yes, Partially

Active Standards

Avis Supply Contract v1.0

ASC1

Cigna Insurance Policy v2.2

CP1

CISO's Requirements Gold

CS1

Cyber Security Standard 2

Yes, Fully

Active Standards

Avis Supply Contract v1.0

ASC2
Cigna Insurance Policy v2.2

CP2
CISO's Requirements Gold

CS2

Cyber Security Standard 3

Yes, Fully

Active Standards

Avis Supply Contract v1.0

ASC3
Cigna Insurance Policy v2.2

CP3
CP4
CISO's Requirements Gold

CS3

Administrative Requirements

Yes, Fully

Administrative Requirements. A covered entity is required to comply with the administrative requirements of the Breach Notif..

Active Standards

Definitions: Breach - exceptions Unsecured PHI

Yes, Fully

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which ..

Active Standards

Notice to Individuals

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual..

Yes, Fully

Active Standards

Timeliness of Notification

A covered entity shall provide the notification without unreasonable delay and in no case later than 60 calendar days after d..

Yes, Fully

Active Standards

Content of Notification

The notification required by paragraph (a) of this section shall include, to the extent possible: (A) A brief description o..

Yes, Fully

Active Standards

Notification by a Business Associate

(a) Standard. (1) General Rule. A business associate shall, following the discovery of a breach of unsecured protected health..

Yes, Fully

Active Standards

Law Enforcement Delay

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting requir..

Yes, Fully

Active Standards

Burden of Proof

In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall..

Yes, Fully

Active Standards

Training

All workforce members must receive training pertaining to the Breach Notification Rule.

Yes, Partially

Active Standards

Complaints to the Covered Entity

All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rul..

Yes, Fully

Active Standards

Sanctions

All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.

Yes, Fully

Active Standards

Refraining from Retaliatory Acts

All covered entities must have policies and procedures in place to prohibit retaliatory acts.

No

Active Standards

Waiver of rights

All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any righ..

Yes, Fully

Active Standards

Policies and Procedures

All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification R..

Yes, Fully

Active Standards

Documentation

All covered entities must have policies and procedures in place for maintaining documentation.

Yes, Fully

Active Standards

Definitions: Breach - Risk Assessment.

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted which compromises the security or p..

Yes, Partially

Active Standards

Uses and Disclosures

Ensure that the covered entity or business associate does not use or disclose protected health information, except as permitt..

No

Active Standards

HIPAA Privacy Rule

§164.502(a)(1)

Disclosures by whistleblowers

Yes, Fully

It is not considered a violation of the Privacy Rule if a staff member or business associate discloses PHI, as long as they b..

Active Standards

HIPAA Privacy Rule

§164.502(j)(1)

Disclosures by workforce members who are victims of a crime

Yes, Partially

The Privacy Rule is balanced to protect an individual's privacy while allowing important law enforcement functions to continu..

Active Standards

HIPAA Privacy Rule

§164.502(j)(2)

Business associate contracts

No

The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business asso..

Active Standards

HIPAA Privacy Rule

§164.504(e)

Requirements for group health plans

Yes, Fully

A "group health plan" is one type of health plan and is a covered entity (except for self-administered plans with fewer than ..

Active Standards

HIPAA Privacy Rule

§164.504(f)

Permitted uses and disclosures

No

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's au..

Active Standards

HIPAA Privacy Rule

§164.506(a)

Consent for uses and disclosures

Yes, Partially

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosur..

Active Standards

HIPAA Privacy Rule

§164.506(b); (b)(1); and (b)(2)

Authorizations for uses and disclosures is required

Yes, Fully

An "authorization" is required by the Privacy Rule for uses and disclosures of protected health information not otherwise all..

Active Standards

HIPAA Privacy Rule

§164.508(a)(1-3) and §164.508(b)(1-2)

Compound authorizations -- Exceptions

Yes, Partially

Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any ..

Active Standards

HIPAA Privacy Rule

§164.508(b)(3)

Prohibition on conditioning of authorizations

No

A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or el..

Active Standards

HIPAA Privacy Rule

§164.508(b)(4)

Uses and Disclosures for which an Authorization is Required – Documentation and Content

Yes, Fully

Documentation. A covered entity must document and retain any signed authorization under this section. Implementation specifi..

Active Standards

HIPAA Privacy Rule

§164.508(b)(6) and §164.508(c)(1-4)

Covered Entities: Required Disclosures

Yes, Partially

Ensure that the covered entity discloses protected health information as required to an individual and to the Office for Civi..

Active Standards

HIPAA Privacy Rule

§164.502(a)(2)

Use and Disclosure for Facility Directories; Opportunity to Object

No

Standard: Use and disclosure for facility directories. (1) Permitted uses and disclosure. Except when an objection is express..

Active Standards

HIPAA Privacy Rule

§164.510(a)(1) and §164.510(a)(2)

Uses and Disclosures for Facility Directories in Emergency Circumstances

Yes, Fully

Emergency circumstances. (i) If the opportunity to object to uses or disclosures cannot practicably be provided because of th..

Active Standards

HIPAA Privacy Rule

§164.510(a)(3)

Permitted uses and disclosures

Yes, Partially

Standard: Uses and disclosures for involvement in the individual's care and notification purposes (1) Permitted uses and dis..

Active Standards

HIPAA Privacy Rule

§164.510(b)(1)

Uses and disclosures with the individual present

Yes, Partially

Standard: Uses and disclosures for involvement in the individual's care and notification purposes Uses and disclosures with ..

Active Standards

HIPAA Privacy Rule

§164.510(b)(2)

Limited uses and disclosures when the individual is not present

Yes, Fully

Limited uses and disclosures when the individual is not present. If the individual is not present, or the opportunity to agre..

Active Standards

HIPAA Privacy Rule

§164.510(b)(3)

Uses and disclosures for disaster relief purposes

Standard: Uses and disclosures for involvement in the individual's care and notification purposes Uses and disclosures for d..

No

Active Standards

HIPAA Privacy Rule

§164.510(b)(4)

Uses and disclosures when the individual is deceased

Standard: Uses and disclosures for involvement in the individual's care and notification purposes. Uses and disclosures when ..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.510(b)(5)

Uses and disclosures required by law

A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by la..

No

Active Standards

HIPAA Privacy Rule

§164.512(a)

Uses and disclosures for public health activities

Standard: Uses and disclosures for public health activities. (1) Permitted uses and disclosures. A covered entity may use or..

No

Active Standards

HIPAA Privacy Rule

§164.512(b)

Disclosures about victims of abuse, neglect or domestic violence

Standard: Disclosures about victims of abuse, neglect or domestic violence (1) Permitted disclosures. Except for permitted re..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.512(c)

Disclosures to Business Associates

A covered entity may disclose protected health information to a business associate and may allow a business associate to crea..

No

Active Standards

HIPAA Privacy Rule

§164.502(e)

Uses and disclosures for health oversight activities

Standard: Uses and disclosures for health oversight activities (1) Permitted disclosures. A covered entity may disclose prot..

No

Active Standards

HIPAA Privacy Rule

§164.512(d)

Disclosures for judicial and administrative proceedings

Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administra..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.512(e)

Disclosures for law enforcement purposes

Yes, Fully

Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such re..

Active Standards

HIPAA Privacy Rule

§164.512(f)(1)

Disclosures for law enforcement purposes - for identification and location -

Yes, Fully

Permitted disclosures: Limited information for identification and location purposes. Except for disclosures required by law, ..

Active Standards

HIPAA Privacy Rule

§164.512(f)(2)

Disclosures for law enforcement purposes-- PHI of a possible victim of a crime

Yes, Fully

Permitted disclosure: Victims of a crime. Except for disclosures required by law, a covered entity may disclose protected hea..

Active Standards

HIPAA Privacy Rule

§164.512(f)(3)

Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct

No

Permitted disclosure: Decedents. A covered entity may disclose protected health information about an individual who has died ..

Active Standards

HIPAA Privacy Rule

§164.512(f)(4)

Disclosures for law enforcement purposes: crime on premises

No

Permitted disclosure: Crime on premises. A covered entity may disclose to a law enforcement official protected health informa..

Active Standards

HIPAA Privacy Rule

§164.512(f)(5)

Disclosures for law enforcement purposes

Yes, Fully

Permitted disclosure: Reporting crime in emergencies. A covered health care provider providing emergency health care in resp..

Active Standards

HIPAA Privacy Rule

§164.512(f)(6)

Uses and disclosures about decedents

Yes, Fully

Standard: Uses and disclosures about decedents. (1) Coroners and medical examiners. A covered entity may disclose protected ..

Active Standards

HIPAA Privacy Rule

§164.512(g)

Uses and disclosures for cadaveric organ, eye or tissue donation

Yes, Fully

Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose p..

Active Standards

HIPAA Privacy Rule

§164.512(h)

Business Associates: Permitted Uses and Disclosures

Yes, Fully

A business associate may use or disclose protected health information only as permitted or required by its business associat..

Active Standards

HIPAA Privacy Rule

§164.502(a)(3)

Uses and disclosures for research purposes -- Permitted Uses and Disclosures

Yes, Fully

Standard: Uses and disclosures for research purposes (1) Permitted uses and disclosures. A covered entity may use or disclose..

Active Standards

HIPAA Privacy Rule

§164.512(i)(1)

Uses and disclosures for research purposes -- Documentation of Waiver Approval

No

Standard: Uses and disclosures for research purposes (2) Documentation of waiver approval. For a use or disclosure to be perm..

Active Standards

HIPAA Privacy Rule

§164.512(i)(2)

Uses and disclosures for specialized government functions -- Military

No

Standard: Uses and disclosures for specialized government functions. (1) Military and veterans activities (i) Armed Forces ..

Active Standards

HIPAA Privacy Rule

§164.512(k)(1)

Uses and disclosures for specialized government functions -- National Security and intelligence activities

No

National security and intelligence activities. A covered entity may disclose protected health information to authorized feder..

Active Standards

HIPAA Privacy Rule

§164.512(k)(2)

Uses and disclosures for specialized government functions -- Protective Services

Yes, Fully

Protective services for the President and others. A covered entity may disclose protected health information to authorized Fe..

Active Standards

HIPAA Privacy Rule

§164.512(k)(3)

Uses and disclosures for specialized government functions – Correctional institutions

Yes, Fully

Medical suitability determinations.- A covered entity that is a component of the Department of State may use protected health..

Active Standards

HIPAA Privacy Rule

§164.512(k)(5)

Uses and disclosures for specialized government functions – Providing public benefits

Yes, Fully

Covered entities that are government programs providing public benefits. (i) A health plan that is a government program provi..

Active Standards

HIPAA Privacy Rule

§164.512(k)(6)

Disclosures for workers' compensation

Yes, Fully

Standard: Disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by ..

Active Standards

HIPAA Privacy Rule

§164.512(l)

Requirements for De-Identification of PHI & Re-Identification of PHI

No

Implementation specifications: Requirements for de-identification of protected health information. A covered entity may deter..

Active Standards

HIPAA Privacy Rule

§164.502(d)
§164.514(b) & §164.514(c)

Standard: Minimum Necessary & Minimum Necessary Uses of PHI

No

Standard: Minimum necessary (1) Minimum necessary applies. When using or disclosing protected health information or when req..

Active Standards

HIPAA Privacy Rule

§164.502(b)
§164.514(d)(1)-§164.514(d)(2)

Health Plan prohibited uses and disclosures of genetic information for underwriting purposes

Yes, Fully

Health plans may not use or disclose genetic information for underwriting purposes.

Active Standards

HIPAA Privacy Rule

§164.502(a)(5)(i)

Minimum Necessary - Disclosures of PHI

Implementation specification: Minimum necessary disclosures of protected health information. (i) For any type of disclosure ..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.514(d)(3)

Minimum Necessary requests for protected health information

Implementation specifications: Minimum necessary requests for protected health information. (i) A covered entity must limit a..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.514(d)(4)

Minimum Necessary - Other content requirement

Implementation specification: Other content requirement. For all uses, disclosures, or requests to which the requirements in ..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.514(d)(5)

Limited Data Sets and Data Use Agreements

Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements, if the cover..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.514(e)

Uses and Disclosures for Fundraising

Yes, Partially

Fundraising communications. (1) Standard: Uses and disclosures for fundraising. A covered entity may use, or disclose to a b..

Active Standards

HIPAA Privacy Rule

§164.514(f)

Uses and Disclosures for Underwriting and Related Purposes

Yes, Partially

Standard: Uses and disclosures for underwriting and related purposes. If a health plan receives protected health information ..

Active Standards

HIPAA Privacy Rule

§164.514(g)

Verification Requirements

Yes, Fully

Standard: Verification requirements. Prior to any disclosure, a covered entity must: Verify the identity of a person requesti..

Active Standards

HIPAA Privacy Rule

§164.514(h)

Notice of Privacy Practices

No

Right to notice. An individual has a right to adequate notice of the uses and disclosures of protected health information tha..

Active Standards

HIPAA Privacy Rule

§164.520(a)(1) & (b)(1)

Content requirements

Yes, Fully

Required elements. The covered entity must provide a notice that is written in plain language and that contains the elements ..

Active Standards

HIPAA Privacy Rule

§164.520(a)(1) & (b)(1)

Provisions of Notice - Health Plans

Yes, Fully

Implementation specifications: Provision of notice. A covered entity must make the notice required by this section available ..

Active Standards

HIPAA Privacy Rule

§164.520(c)(1)

Deceased individuals

Yes, Fully

PHI related to deceased individuals is protected for 50 years after their death.

Active Standards

HIPAA Privacy Rule

§164.502(f)

Provisions of Notice - Certain Covered Health Care Providers

No

Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment r..

Active Standards

HIPAA Privacy Rule

§164.520(c)(2)

Provision of Notice - Electronic Notice

Specific requirements for electronic notice. (i) A covered entity that maintains a web site that provides information about t..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.520(c)(3)

Joint Notice by Separate Covered Entities

Implementation specifications: Joint notice by separate covered entities. Covered entities that participate in organized heal..

No

Active Standards

HIPAA Privacy Rule

§164.520(d)

Documentation

Implementation specifications: Documentation. A covered entity must document compliance with the notice requirements, by reta..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.520(e)

Right of an Individual to Request Restriction of Uses and Disclosures

Standard: Right of an individual to request restriction of uses and disclosures. (i) A covered entity must permit an individ..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.522(a)(1)

Restricted Uses and Disclosures

No

A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health in..

Active Standards

HIPAA Privacy Rule

§164.502(c)

Terminating a Restriction

Yes, Fully

Implementation specifications: Terminating a restriction. A covered entity may terminate a restriction, if : (i) the individ..

Active Standards

HIPAA Privacy Rule

§164.522(a)(2)

Documentation

Yes, Fully

Implementation specification: Documentation. A covered entity must document a restriction.

Active Standards

HIPAA Privacy Rule

§164.522(a)(3)

Confidential Communications Requirements

Yes, Fully

Standard: Confidential communications requirements. (i) A covered health care provider must permit individuals to request an..

Active Standards

HIPAA Privacy Rule

§164.522(b)(1)

Right to access

Standard: Access to protected health information. (1) Right of access. Except as otherwise provided, an individual has a righ..

No

Active Standards

HIPAA Privacy Rule

§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)

Personal representatives

The personal representative stands in the shoes of the individual and has the ability to act for the individual and exercise ..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.502(g)

Denial of Access

Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected healt..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.524(d) (2)

Unreviewable grounds for denial

Standard: Access to protected health information. (2) Unreviewable grounds for denial. A covered entity may deny an individua..

No

Active Standards

HIPAA Privacy Rule

§164.524(a)(2)

Reviewable grounds for denial

Yes, Partially

Standard: Access to protected health information. (3) Reviewable grounds for denial. A covered entity may deny an individual ..

Active Standards

HIPAA Privacy Rule

§164.524(a)(3)

Review of denial of access

No

Standard: Access to protected health information. (4) Review of a denial of access. If access is denied on a permitted ground..

Active Standards

HIPAA Privacy Rule

§164.524(a)(4) & (d)(4)

Documentation

Yes, Partially

Implementation specification: Documentation. A covered entity must document the following and retain the required documentati..

Active Standards

HIPAA Privacy Rule

§164.524(e)

Right to Amend

Yes, Fully

Standard: Right to amend. (1) Right to amend. An individual has the right to have a covered entity amend protected health inf..

Active Standards

HIPAA Privacy Rule

§164.526(a)(1)

Denying the Amendment

Standard: Right to amend. (2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it det..

No

Active Standards

HIPAA Privacy Rule

§164.526(a)(2)

Accepting the Amendment

Implementation specifications: Accepting the amendment. If the covered entity accepts the requested amendment, in whole or in..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.526(c)

Denying the Amendment

Implementation specifications: Denying the amendment. If the covered entity denies the requested amendment, in whole or in pa..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.526(d)

Right to an Accounting of Disclosures of PHI

Right to an accounting of disclosures of protected health information. (1) An individual has a right to receive an accountin..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.528(a)

Confidential communications

Yes, Fully

Health plans and covered health care providers must permit individuals to request an alternative means or location for receiv..

Active Standards

HIPAA Privacy Rule

§164.502(h)

Content of the Accounting

No

Implementation specifications: Content of the accounting. The covered entity must provide the individual with a written accou..

Active Standards

HIPAA Privacy Rule

§164.528(b)

Provision of the Accounting

Yes, Partially

Implementation specifications: Provision of the accounting. (1) The covered entity must act on the individual's request for a..

Active Standards

HIPAA Privacy Rule

§164.528(c)

Documentation

Yes, Partially

Implementation specification: Documentation. A covered entity must document the following and retain the documentation : (1) ..

Active Standards

HIPAA Privacy Rule

§164.528(d)

Personnel designations

(a)(1) Standard: Personnel designations. (i) A covered entity must designate a privacy official who is responsible for the d..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.530(a)

Training

Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to p..

Yes, Fully

Active Standards

HIPAA Privacy Rule

§164.530(b)

Safeguards

Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to p..

Yes, Partially

Active Standards

HIPAA Privacy Rule

§164.530(c)

Complaints to the Covered Entity

Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints conce..

No

Active Standards

HIPAA Privacy Rule

§164.530(d)(1)

Complaints to the Covered Entity

No

Implementation specification: Documentation of complaints. A covered entity must document all complaints received, and their ..

Active Standards

HIPAA Privacy Rule

§164.530(d)(2)

Sanctions

Yes, Fully

Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to ..

Active Standards

HIPAA Privacy Rule

§164.530(e)(1)

Mitigation

Yes, Fully

Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the cove..

Active Standards

HIPAA Privacy Rule

§164.530(f)

Uses and disclosures consistent with notice

No

Uses and disclosures of protected health information must be consistent with the entity's notice of privacy practices.

Active Standards

HIPAA Privacy Rule

§164.502(i)

Refraining from Intimidating or Retaliatory Acts

Yes, Fully

Standard: Refraining from intimidating or retaliatory acts. A covered entity— (1) May not intimidate, threaten, coerce, di..

Active Standards

HIPAA Privacy Rule

§164.530(g)

Waiver of rights

Yes, Fully

Standard: Waiver of rights. A covered entity may not require individuals to waive their HIPAA rights , as a condition of the ..

Active Standards

HIPAA Privacy Rule

§164.530(h)

Policies and Procedures

Yes, Fully

Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health i..

Active Standards

HIPAA Privacy Rule

§164.530(i)

Documentation

Yes, Fully

Standard: Documentation. A covered entity must: (i) Maintain the policies and procedures in written or electronic form; (ii) ..

Active Standards

HIPAA Privacy Rule

§164.530(j)