



CyberQP HIPAA Control Mappings



QGuard FRAMEWORK: HIPAA

Function	Control	Control Description	Requirement
Privilege Account Discovery & Remediation	§164.308(a)(4)(B)	Access authorization	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
	§164.308(a)(4)(C)	Access establishment and modification	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	§164.312(a)(1)	Access Control	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
	§164.308(a)(4)(B)	Access authorization	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
	§164.308(a)(4)(C)	Access establishment and modification	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
	§164.312(a)(1)	Access Control	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
Technician Passwordless Authentication, Tracking & Auditing	§164.308(a)(5)(ii)(C)	Log-in monitoring	Procedures for monitoring log-in attempts and reporting discrepancies.
	§164.312(a)(2)(iii)	Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Privileged Account Just-in-Time Access	§164.312(a)(2)(iii)	Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
	§164.312(b)	Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

QDesk FRAMEWORK: HIPAA

Function	Control	Control Description	Requirement
Endpoint Privilege Management	§164.312(a)(2)(iii)	Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
	§164.312(b)	Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
Identity Verification	§ 164.312(a)(2)(i)	Unique user identification	Assign a unique name and/or number for identifying and tracking user identity.
	§ 164.312(b)	Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
Self-Service Password Reset (SSPR)	§164.308(a)(5)(ii)(D)	Password management	Procedures for creating, changing, and safeguarding passwords.
	§164.312(d)	Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
Essential Account Management	§164.308(a)(5)(ii)(D)	Password management	Procedures for creating, changing, and safeguarding passwords.
	§164.312(b)	Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
	§164.312(d)	Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

CyberQP redefines Zero Trust Access Management with leading-edge Privileged Access Management (PAM) and End-User Access Management (EUAM) solutions. Our platform enables secure elevated access for both IT Professionals and end-users, along with robust self-serve and identity verification capabilities. Backed by SOC 2 Type 2 certification, we empower IT professionals to reduce or eliminate risks stemming from social engineering attacks, standing privilege, and over-privileged accounts, enforce compliance, and enhance operational efficiency. Our mission is simple: "Empowering Access, Redefining Privilege" for security-focused IT professionals around the globe. Learn more <https://cyberqp.com/product-tours>