

HIPAA & Alloantibody Exchange

A point-by-point review of the HIPAA Simplification legislation.

Last review: 2/17/2024

This document contains the HIPAA Administrative, Physical, and Technical safeguards as they are written. Our controls and evidence in response to these concerns are placed below the original legislation. Link to [HIPAA legislation](#).

HIPAA definitions

- Required - A business associate must implement the implementation specifications.
- Addressable - A business associate must use reasonable and appropriate measures to meet the standard.

Order of hierarchy: (a)(1)(i)(A)

§ 164.308 Administrative safeguards. (page 64)

This section applies to us as a Business Associate.

(a)(1)(i) Standard: Security management process.

Implement policies and procedures to prevent, detect, contain, and correct security violations.

Solution: We have a Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT) designed to prevent, detect, contain, and correct security violations.

(a)(1)(ii)(A) Risk analysis (Required).

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

Solution: The Alloantibody Exchange has conducted such a risk analysis identifying the risks and vulnerability to PHI.

(a)(1)(ii)(B) Risk management (Required).

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Solution: The risk analysis was reviewed to mitigate the risks and vulnerabilities.

(a)(1)(ii)(C) Sanction policy (Required).

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

Solution: We have language in our human resource management documents to apply appropriate sanctions against workforce members who fail to comply with the security policies.

(a)(1)(ii)(D) Information system activity review (Required).

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Solution: We have a procedure to regularly information system activity including sign-in logs, database logs, and security incident reports generated in Azure.

(a)(2) Standard: Assigned security responsibility.

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

Solution: The security official responsible for security is the leader of our Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT)

(a)(3)(i) Standard: Workforce security.

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

Solution: We have a documented policy to determine appropriate access PHI.

(a)(3)(ii)(A) Authorization and/or supervision (Addressable).

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Solution: Control of access to software programs is delegated through Microsoft's Azure Active Directory, which provides authentication and authorization based on user roles.

(a)(3)(ii)(B) Workforce clearance procedure (Addressable).

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Solution: We have a procedure to determine access to PHI codified in a policy.

(a)(3)(ii)(C) Termination procedures (Addressable).

Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

Solution: We have a termination procedure to turn off PHI access.

(a)(4)(i) Standard: Information access management.

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

Solution: We have implemented policies/procedures for authorizing access to PHI consistent with subpart E.

(a)(4)(ii)(A) Isolating health care clearinghouse functions (Required).

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Solution: This does not apply because we are not a healthcare clearinghouse.

(a)(4)(ii)(B) Access authorization (Addressable).

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

Solution: We have a policy for granting access to PHI. We also have a procedure to grant/revoke access to PHI.

(a)(4)(ii)(C) Access establishment and modification (Addressable).

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.

Solution: We have a procedure to review and update user's right to access privileged resources.

(a)(5)(i) Standard: Security awareness and training.

Implement a security awareness and training program for all members of its workforce (including management).

Solution: Security awareness and training programs are implemented for the workforce.

(a)(5)(ii)(A) Security reminders (Addressable).

Periodic security updates.

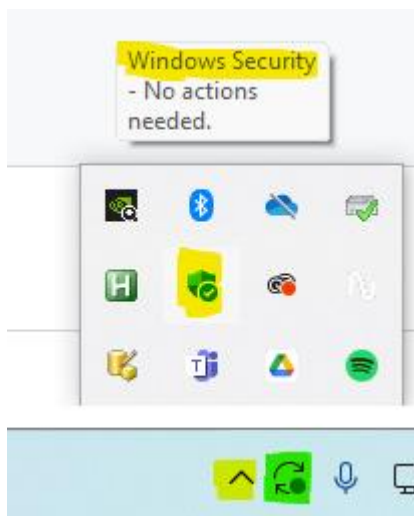
Solution: Microsoft performs security updates to our software, which we purchase as a service.

(a)(5)(ii)(B) Protection from malicious software (Addressable).

Procedures for guarding against, detecting, and reporting malicious software. Solution: These two teams are responsible for guarding against, detecting, and reporting malicious software: Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT).

Solution: Users are responsible for maintaining the updates on the machine they use to access our cloud-serve provide, Azure. They submit proof of this maintenance quarterly in the form of Windows Security review for computers they use to access company resources.

Documentation for Windows machines:



Yellow highlighting above:

Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection
No action needed.



Account protection
No action needed.



Firewall & network protection
No action needed.



Device security
View status and manage hardware security features.



Device performance & health
No action needed.



Family options
Manage how your family uses their devices.



Protection history
View latest protection actions and recommendations.

Green highlighting above:

Windows Update



You're up to date
Last checked: Today, 8:48 AM

[Check for updates](#)

(a)(5)(ii)(C) Log-in monitoring (Addressable).

Procedures for monitoring log-in attempts and reporting discrepancies.

Solution: We monitor log-in attempts and report on discrepancies.

(a)(5)(ii)(D) Password management (Addressable).

Procedures for creating, changing, and safeguarding passwords.

Solution: We use Microsoft's Azure Active Directory for password creation and changing. Employees are responsible for safeguarding passwords.

(a)(6)(i) Standard: Security incident procedures.

Implement policies and procedures to address security incidents.

Solution: These two teams are responsible for addressing security incidents: Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT).

(a)(6)(ii) Response and reporting (Required).

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

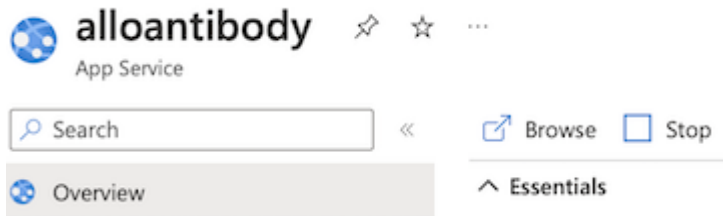
Solution: These two teams are responsible for responding to suspected or known security incidents: Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT).

(a)(7)(i) Standard: Contingency plan.

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Solution: We have a policy to detail how to handle damages to systems that contain PHI. See related HIPAA questions: [1](#), and [2](#)

To disable the web app in the case of a security threat.

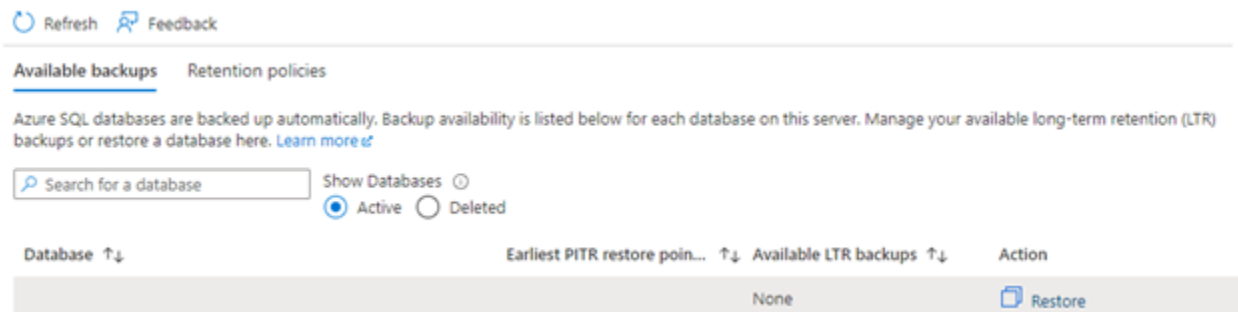


(a)(7)(ii)(A) Data backup plan (Required).

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Solution: We use Microsoft as a cloud service provide for storage of electronic PHI. They store copies of our PHI accessible at any point in time in the last 7 days. They use read-access geo-redundant storage (RA-GRS) to ensure data is preserved even if the data center is unavailable. We can access backup copies as needed to restore our service.

Fore example, Azure database restoration is available in SQL server > Backups > Restore:



(a)(7)(ii)(B) Disaster recovery plan (Required).

Establish (and implement as needed) procedures to restore any loss of data.

Solution: We have a procedure to restore loss of data.

(a)(7)(ii)(C) Emergency mode operation plan (Required).

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Solution: We have a procedure to address emergency situations.

(a)(7)(ii)(D) Testing and revision procedures (Addressable).

Implement procedures for periodic testing and revision of contingency plans.

Solution: We have a procedure to test and review our contingency plan. We will periodically test and revise it once per year or more frequently as needed.

- Review contingency plan yearly

(a)(7)(ii)(E) Applications and data criticality analysis (Addressable).

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Solution: The contingency plan should review specific applications and their relationship to each other in executing the contingency plan.

(a)(8) Standard: Evaluation.

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

Solution: We will conduct and document a technical and nontechnical evaluation yearly to assess our security policies and procedures.

(b)(1) Business associate contracts and other arrangements.

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

Solution: Not applicable.

(b)(2) Business associate contracts and other arrangements.

A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

Solution: Our only business associate is Microsoft. We have reviewed their qualifications.

(b)(3) Written contract or other arrangement (Required).

Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

Solution: Our written contract will contain these requirements.

§ 164.310 Physical safeguards. (page 66)

This section applies to us as a Business Associates.

(a)(1) Standard: Facility access controls.

Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Solution: We employ Microsoft as a cloud services provider. They manage physical access where our data is housed. Employees are not permitted to store patient information outside of the cloud environment.

(a)(2)(i) Contingency operations (Addressable).

Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Solution: We employ Microsoft as a cloud services provider. They manage facility access.

(a)(2)(ii) Facility security plan (Addressable).

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

Solution: We employ Microsoft as a cloud services provider. They provide safeguards to their data facilities.

(a)(2)(iii) Access control and validation procedures (Addressable).

Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Solution: We employ Microsoft as a cloud services provider. They manage facility access. Control of access to software programs is delegated through Microsoft's Azure Active Directory, which provides authentication and authorization based on user roles.

(a)(2)(iv) Maintenance records (Addressable).

Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Solution: We employ Microsoft as a cloud services provider. They manage physical maintenance.

(b) Standard: Workstation use.

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Solution: We have a procedure to specify the proper use and setup of an employee workstation that access PHI.

(c) Standard: Workstation security.

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

[Note](#): The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity's premises or at another location.

Solution: We have a procedure to specify the proper use and setup of an employee workstation that access PHI, including physical safeguards.

(d)(1) Standard: Device and media controls.

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Solution: We employ Microsoft as a cloud services provider. They manage hardware and electronic media.

(d)(2)(i) Disposal (Required).

Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

Solution: We employ Microsoft as a cloud services provider. They manage hardware disposal.

(d)(2)(ii) Media re-use (Required).

Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.

Solution: We employ Microsoft as a cloud services provider. They manage hardware re-use.

(d)(2)(iii) Accountability (Addressable).

Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Solution: We employ Microsoft as a cloud services provider. They manage hardware accountability.

(d)(2)(iv) Data backup and storage (Addressable).

Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Solution: We employ Microsoft as a cloud services provider. They manage hardware movement.

§ 164.312 Technical safeguards. (page 66)

This section applies to us as a Business Associates.

(a)(1) Standard: 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).

Solution: We have a procedure to allow access only to those persons that have granted access. Primarily, we use Azure Active Directory is maintained users and their roles.

(a)(2)(i) Unique user identification (Required).

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

Solution: Azure Active Directory, which we use, provides a unique name ("User principal name") and number ("Object ID") for each user.

(a)(2)(ii) Emergency access procedure (Required).

Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Solution: We have a procedure for how to proceed in the event of a software emergency. [Policy 35] But, it is important to know that in the event the Alloantibody Exchange is not operational, blood banks can and should revert to their pre-existing procedures prior to the Alloantibody Exchange. The Alloantibody Exchange can only operate electronically, and it may not operate in an emergency.

(a)(2)(iii) Automatic logoff (Addressable).

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Solutions: We have implemented an inactivity timer. After 10 minutes of no keystrokes or mouse movement, the logout endpoint is called. It is active in all pages within the website.

References

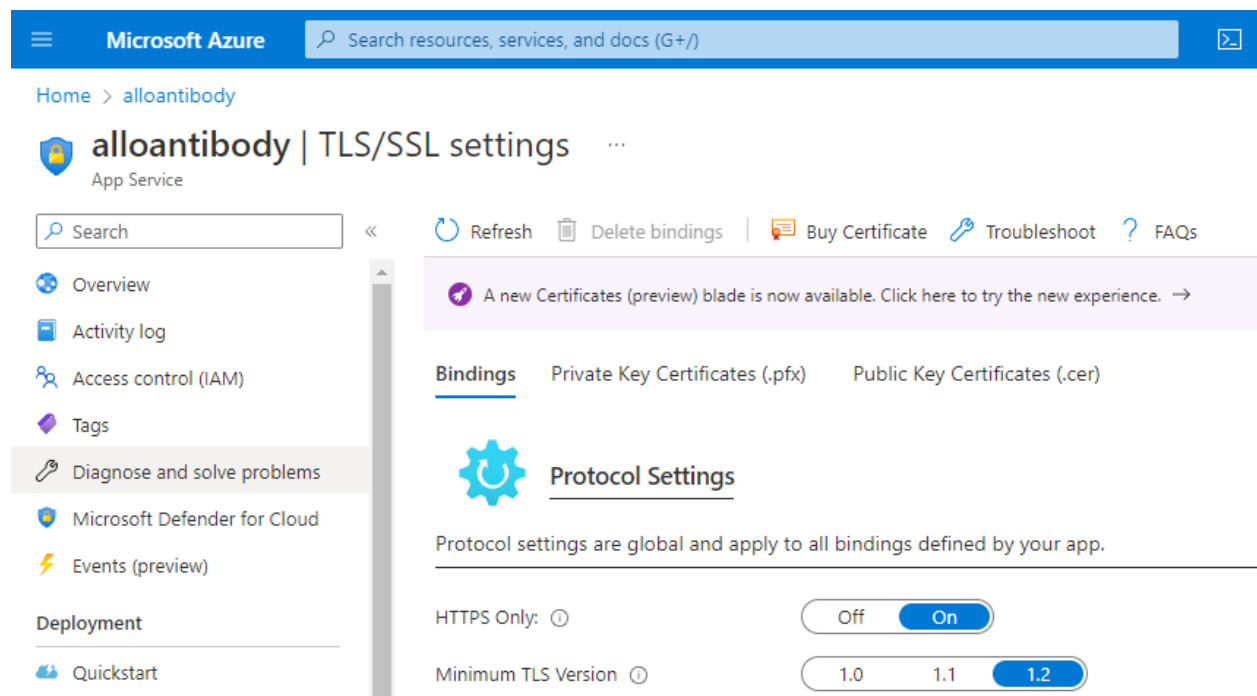
- [How long to set automatic logoff](#)

(a)(2)(iv) Encryption and decryption (Addressable).

Implement a mechanism to encrypt and decrypt electronic protected health information.

Solution: We have implemented an end-to-end encryption solution.

Encryption in transit:



The screenshot displays the Microsoft Azure portal interface for configuring TLS/SSL settings on an App Service named 'alloantibody'. The left-hand navigation pane includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, Events (preview), Deployment, and Quickstart. The main content area shows the 'TLS/SSL settings' page with a search bar and navigation links (Refresh, Delete bindings, Buy Certificate, Troubleshoot, FAQs). A notification banner indicates a new 'Certificates (preview)' blade is available. Below this, there are tabs for 'Bindings', 'Private Key Certificates (.pfx)', and 'Public Key Certificates (.cer)'. The 'Protocol Settings' section is active, featuring a gear icon and a sub-header. A descriptive text states: 'Protocol settings are global and apply to all bindings defined by your app.' Two configuration options are shown: 'HTTPS Only' with a toggle switch set to 'On', and 'Minimum TLS Version' with a dropdown menu set to '1.2'.

Private key certificate(s):

Bindings Private Key Certificates (.pfx) Public Key Certificates (.cer)



Private Key Certificate

Private key certificates (.pfx) can be used for TLS/SSL bindings and can be loaded to the certificate store. To learn more about how to load the certificates for your app to consume click on the learn more link. Uploaded certificates to the Azure Management Portal, they can only be used by your app hosted on App Service after the required permissions are granted. [Learn more](#)

+ Import App Service Certificate + Upload Certificate + Import Key

Private Key Certificates

Status Filter

All Healthy Warning Expired

Health Status	Hostname	Expiration
✓ Healthy	alloantibody.org	
✓ Healthy	www.alloantibody.org	

[Encryption at rest](#). "Data Encryption Key (DEK) – A symmetric AES256 key used to encrypt a partition or block of data, sometimes also referred to as simply a Data Key.":

The screenshot shows the Microsoft Azure portal interface for an SQL database. The page title is "Transparent data encryption". The main content area displays a shield icon with a lock, indicating that transparent data encryption is enabled. Below this, there is a "Data encryption" section with a toggle switch set to "ON". Underneath, the "Encryption status" is shown as "Encrypted" with a green checkmark. The left sidebar contains navigation options such as "Overview", "Activity log", "Tags", "Diagnose and solve problems", "Getting started", "Query editor (preview)", and "Settings". The top navigation bar includes the Microsoft Azure logo and a search bar.

(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.

Solution: We have implemented software and procedural mechanisms to record and examine activity involving PHI.

Example / Sign-in Log:

The screenshot displays the Azure Conditional Access Sign-in logs interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Security > Security | Conditional Access > Conditional Access. The main heading is "Conditional Access | Sign-in logs" with a sub-heading "Azure Active Directory". A left-hand navigation menu lists various options: Overview (Preview), Policies, Insights and reporting, Diagnose and solve problems, and a "Manage" section containing Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication context, and Classic policies. The main content area features a toolbar with "Download", "Export Data Settings", "Troubleshoot", "Refresh", "Columns", and "Got feedback" buttons. A notification banner states: "This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins p". Below the notification, there are filters for "Date: Last 7 days", "Show dates as: Local", and "Add filters". The data table has the following structure:

Date	Request ID	User	Application	Status
			Microsoft App Acces...	Success
			Azure Portal	Success
			Azure Portal	Success
			AlloantibodyExchan...	Success
			AlloantibodyExchan...	Interrupted
			AlloantibodyExchan...	Success
			Azure Portal	Success

Example / Azure SQL Database Auditing ([Ref](#)):

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing

Audit log destination (choose at least one):

(c)(1) Integrity.

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction

Solution: We have procedures in place to avoid PHI alteration or destruction. For example, the website does not allow a user, regardless of their role, to alter or destroy PHI. Also, information received by the Alloantibody Exchange is retained in its original format to cross reference later as needed.

(c)(2) Mechanism to authenticate electronic protected health information (Addressable).

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Solution: We require our users to authenticate through Microsoft Azure Active Directory. We also conduct database audits to identify commands that would alter or destroy PHI.

(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.

Solution: We require our users to authenticate through Microsoft Azure Active Directory. We require two-factor authentication for work on production systems.

(e)(1) Transmission security.

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Solution: We implement multiple technical security measures to guard against unauthorized access to PHI. These include technical security measure that prevent Cross-Site Request Forgery (XSRF/CSRF), SQL injection attacks, Cross-Site Scripting (XSS), open redirect attacks, and Cross-Origin Requests (CORS). We provide end-to-end encryption to PHI. Mitigate data exfiltration, we have limits on the number of patients returned from a search (i.e., 10). And we limit the ability for of the user to conduct vague searches with a wildcard character through front/back-end input validation.

Example of an attempted wildcard search, failing on the front-end.

Patient Search

Enter patient demographics for database matching

First name

Valid first or last name is required.

MI

Last name

Valid first or last name is required.

(e)(2)(i) Integrity controls (Addressable).

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Solution: See related HIPAA questions related to transmission security and audit security above.

(e)(2)(ii) Encryption (Addressable).

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Solution: We provide end-to-end encryption to PHI.