Regulation Checkpoint: HIPAA - BA

Overall Confidence Level: Perfect*

Table 1: Overall summary of the results

Total Control Questions	Questions with Correct Response in the Documentation	Questions with Insufficent Evidence in the Documentation	Compliance Percentage
170	170	0	100

Table 2: Breakdown of the compliance and the gaps

Category	Total Control Questions	Questions with Correct Response in the Documentation	Questions with Insufficent Evidence in the Documentation	Compliance Percentage
Administrative Requirements	35	35	0	100
Amendments and Accountings of Disclosures	5	5	0	100
Business Associate Contracts	25	25	0	100
Complaints and Sanctions	4	4	0	100
Documentation and Record Retention	17	17	0	100
Mitigation and Retaliation Provisions	1	1	0	100
Privacy Practices for Protected Health Information	4	4	0	100
Safeguards for Protected Health Information	76	76	0	100
Use and Disclosure of Protected Health Information	3	3	0	100

More details of compliance checks and gap analysis are in an accompanying spreadsheet (Ulalo HIPAA Certification Job v2 merged_HIPAA - BA.xlsx).
Correct Response: documented evidence is sufficient to conclude that the specific requirements of the regulations sub-article were met. The accompanying spreadsheet includes text snippets from the submitted documents providing the necessary supporting evidence.
Insufficient evidence: documented evidence is insufficient to conclude that the specific requirements of the regulation's sub-article were met, OR documented evidence is sufficient

* Confidence level definitions: 100% (Perfect), 80-99% (High), 60-79% (Medium), 40-59% (Low), <40% (Very low).
** This gap analysis, including the provided overall compliance score, this document and its annexes are not legal advice. Specific legal advice should be taken before acting on any of the topics covered.

to flag violations of the requirements of the regulation's sub-article.

05 / 03 / 2026

Debu Chatterjee

debu@konfer.ai

CEO, President

Konfer Inc.

ULALO

KONFER
Governance by Design

Regulation Checkpoint: HIPAA - BA

Analysis conducted on 2026-04-16 at 23:39 UTC.

Summary of results is in file Ulalo HIPAA Certification Job v2 merged_HIPAA - BA.pdf

Question	Score	Answer	Snippets	Reason	Section	Source	Recommendations
Is the covered entity or business associate currently ensuring the confidentiality, integrity, and availability of all electronic protected health information they create, receive, maintain, or transmit?	Correct	Yes	('This policy and procedure establishes how Ulalo identifies, inventories, classifies, protects, and manages information assets-especially applications and data-throughout their lifecycle.', 'It includes a defined method for Application and Data Criticality Analysis so that security, privacy, resiliency, and compliance controls are applied based on risk and business impact.'), ('Ulalo has adopted this policy to ensure that its Security and Privacy Policies are up to date and effective in ensuring the confidentiality, integrity and availability of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) created, received, maintained and transmitted by Ulalo.')	The cited passages show policies that explicitly require safeguarding the confidentiality, integrity, and availability of all ePHI across its lifecycle, demonstrating that the entity is actively ensuring CIA for every electronic PHI asset.	Safeguards for Protected Health Information	Asset Management Policy and Procedure.pdf::::1 Evaluation-Policy.pdf::::1	
Is the covered entity or business associate currently protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information?	Correct	Yes	('b. Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.'), ('3. Monitor API calls, ensuring they use secure HTTPS connections and that no sensitive data (e.g., PHI) is exposed in transit.', '2. Ensure all backend services handling PHI are secured with proper authentication, authorization, and encryption.'), ('It is the policy of Ulalo to fully comply with the HIPAA Security Rule, including to... (2) protect against reasonably anticipated threats or hazards to the security or integrity of ePHI;')	The cited passages mandate protection against reasonably anticipated threats or hazards and describe concrete safeguards such as secured API traffic, authentication, encryption and ongoing vulnerability management, demonstrating that such protections are in place.	Safeguards for Protected Health Information	Risk-Management-Policy1.pdf::::2 Implementing a Schedule for Regular Vulnerability Scans of Systems Handling PHI.pdf::::4 Security-Privacy-Breach-Policy.pdf::::3	
Is the covered entity or business associate currently protecting against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted or required under subpart "Privacy of Individually Identifiable Health Information" of this part?	Correct	Yes	('Microsoft shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. Microsoft shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA.'), ('When a use or disclosure is not otherwise permitted under these policies, Ulalo will secure a valid authorization prior to making any use or disclosure of PHI.')	The cited passages impose contractual and policy limits that forbid any PHI use or disclosure beyond what the HIPAA Privacy Rule allows and require explicit authorization when an activity is not otherwise permitted, thereby protecting against impermissible uses or disclosures.	Use and Disclosure of Protected Health Information	Microsoft General - HIPAA BAA (May 2025).pdf::::2 Uses-and-Disclosures-of-PHI.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is the covered entity or business associate currently ensuring compliance with the Security subpart by their workforce?	Correct	Yes	('Ulalo must periodically annually evaluate its HIPAA Security or Privacy Procedures to ensure that departments follow such Procedures and that these procedures maintain their technical and non- technical viability and continue to comply with the HIPAA Security or Privacy Policies.'), ('H. SANCTIONS - Ulalo employees who fail to fully comply with Ulalo HIPAA Privacy, Security and Breach Notification Policies and Procedures contained herein will be subject to sanctions as deemed appropriate by management in accordance Ulalo.')	The cited passages mandate regular evaluations, audits, training, and sanctions for workforce members, demonstrating active oversight and enforcement of HIPAA Security Rule requirements across the workforce.	Administrative Requirements	Evaluation-Policy.pdf::::2 Security-Privacy-Breach-Policy.pdf::::6	
Is the covered entity or business associate currently taking into account the size, complexity, and capabilities of the entity when deciding which security measures to use?	Correct	Yes	('c. Assessing the appropriate scope of system reviews based on the size and needs of Ulalo by determining:', 'v. Assessing available organizational resources.'), ('It is the policy of Ulalo to exercise the discretion afforded to it by HHS to select security measures that Ulalo believes are best suited to reasonably and appropriately meet the standards and specifications set forth by the HIPAA Security Rule.')	The cited passages show that Ulalo tailors review scope to its own size, needs, and resources and explicitly chooses security measures suited to its context, confirming that size, complexity, and capabilities are factored into security-measure decisions.	Safeguards for Protected Health Information	Information-System-Activity-Review-Policy.pdf::::2 Security-Privacy-Breach-Policy.pdf::::3	
Is the covered entity or business associate currently considering their technical infrastructure, hardware, and software security capabilities when deciding on security measures?	Correct	Yes	('Maintain a complete and accurate inventory of the Information Technology (IT) and Operational Technology (OT) assets in your organization to facilitate the implementation of optimal security controls.'), ('d. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented: i. The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism. ii. The system must be moved into a secure environment. iii. All ePHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.')	The cited passages require an IT/OT asset inventory to guide security controls and mandate upgrading or relocating systems that lack needed technical safeguards, demonstrating that Ulalo evaluates its infrastructure, hardware, and software capabilities when selecting security measures.	Safeguards for Protected Health Information	SRA_Tool_3_6.pdf::::3 Technical-Safeguards-Access-Control-Policy.pdf::::5	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is the covered entity or business associate currently considering the costs of security measures when deciding which ones to use?	Correct	Yes	('Determine the extent to which a control is cost-effective by comparing the benefit of applying a control with its cost of application.'), ('a. Scheduled Basis - an overall risk assessment of Ulalo infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.')	The cited passages call for cost-benefit analysis of each control and for risk-mitigation strategies to be incorporated into the budgeting process, confirming that Ulalo considers the cost of security measures in its decisions.	Safeguards for Protected Health Information	Risk-Management-Policy1.pdf::::4, ::::6	
Is the covered entity or business associate currently assessing the probability and criticality of potential risks to electronic protected health information when deciding on security measures?	Correct	Yes	('Threats and vulnerabilities should be documented and given impact and likelihood ratings.'), ('a. Identifies the risks to confidentiality, availability, and integrity of PHI, determines the probability of occurrence, and the resulting impact for each threat/ vulnerability pair identified given the security controls in place.')	The cited passages require documenting threats with impact and likelihood ratings and define risk assessment as determining probability and impact for each threat/vulnerability pair, demonstrating that Ulalo evaluates both probability and criticality of ePHI risks when choosing security measures.	Safeguards for Protected Health Information	SRA_Tool_3_6.pdf::::6 Risk-Management-Policy1.pdf::::1	
Is the covered entity or business associate currently implementing the required implementation specifications as provided in the Security subpart?	Correct	Yes	('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.'), ('I attest that: Personnel access is documented and role-based Access levels align with job responsibilities and supervisory approval Authorized user lists are reviewed and updated regularly Access is revoked or modified promptly as roles change', 'These controls are implemented and maintained in accordance with the HIPAA Security Rule, including 45 CFR §164.308(a)(3), §164.308(a)(4), and §164.312(a)(1).'), ('Specifically, I attest that:', '· Encryption is enforced for data at rest and in transit', 'These controls are actively managed, monitored, and reviewed in alignment with HIPAA Security Rule requirements (45 CFR §164.308, §164.312).')	The cited passages mandate compliance with 45 CFR Part 164 Subpart C and include signed attestations that access, encryption, and other technical controls are implemented and maintained in line with the Security Rule, confirming that all required implementation specifications are currently in place.	Safeguards for Protected Health Information	Microsoft General - HIPAA BAA (May 2025).pdf::::3 06- Authorized Personnel Access Le.pdf::::3 02- Azure - HIPAA Proof of Implementation.pdf::::3	
Is the covered entity or business associate currently assessing whether each addressable implementation specification is a reasonable and appropriate safeguard in their environment?	Correct	Yes	('Taking the possible controls for each threat and vulnerability pair in Step 8 of the Risk Assessment, review the recommended controls and alternative solutions for reasonableness and appropriateness.'), ('It is the policy of Ulalo to exercise the discretion afforded to it by HHS to select security measures that Ulalo believes are best suited to reasonably and appropriately meet the standards and specifications set forth by the HIPAA Security Rule.', 'It is the policy of Ulalo to regularly review its IT practices and infrastructure and to consider appropriate methods to enhance security measures.'), ('c. Servers, workstations, or other computer systems that access, transmit, receive, or store ePHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.', '10) Encryption and Decryption a. Encryption of ePHI as an access control mechanism is not required unless the custodian of said ePHI deems the data to be highly critical or sensitive.')	Risk-management and technical-safeguard policies instruct staff to review each potential control for reasonableness and appropriateness, and the overarching security policy states that Ulalo exercises its discretion to choose safeguards that fit its environment. These statements show that addressable specifications are actively evaluated before adoption.	Safeguards for Protected Health Information	Risk-Management-Policy1.pdf::::4 Security-Privacy-Breach-Policy.pdf::::3 Technical-Safeguards-Access-Control-Policy.pdf::::5	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is the covered entity or business associate currently implementing the addressable implementation specifications if they are reasonable and appropriate?	Correct	Yes	('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted … and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.'), ('a. Servers, workstations, or other computer systems located in open, common, or otherwise unsecure areas, that access, transmit, receive, or store ePHI … must employ inactivity timers or automatic logoff mechanisms …', '10) Encryption and Decryption a. Encryption of ePHI as an access control mechanism is not required unless the custodian of said ePHI deems the data to be highly critical or sensitive.', '11) Firewall Use a. All networks housing ePHI repositories must be appropriately secured.'), ('Ulalo will implement appropriate procedures to control and validate Ulalo employee access to all facilities used to house ePHI based systems.', 'Ulalo will adopt appropriate access control mechanisms to control physical access to all facilities containing ePHI-based systems, we have key locks as physical access control mechanisms.')	The BAA obliges implementation of reasonable safeguards under Subpart C, while internal policies show concrete addressable measures already in place—such as automatic log-off, conditional encryption, firewalls, and physical access controls—demonstrating that the entity implements each specification when deemed appropriate.	Safeguards for Protected Health Information	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Technical-Safeguards-Access-Control-Policy.pdf::::5 Facility-Access-Controls-Policy.pdf::::1	
Is the covered entity or business associate currently reviewing and modifying the security measures implemented under the Security subpart as needed to continue providing reasonable and appropriate protection of electronic protected health information?	Correct	Yes	('The Information Security Officer will review on an on-going basis the viability of Ulalo Security Policies and general approaches taken by Departments in their Security Procedures.', 'The Information Security Officer will develop and recommend to Ulalo any necessary Security Policy or Procedure changes.'), ('6. Evaluation of Ulalo Procedures … Ulalo must periodically annually evaluate its HIPAA Security or Privacy Procedures to ensure … they maintain their technical and non-technical viability …', '8. Whenever there is a change in law that necessitates a change to Ulalo\'s policies or procedures, Ulalo will promptly document and implement the revised policy or procedure.'), ('Adopting this schedule and approach ensures continuous monitoring and improvement of security measures.')	Policies require ongoing and annual evaluations by the Information Security Officer, immediate updates when laws or circumstances change, and continuous improvement through scheduled vulnerability assessments. These mandates show that security measures are regularly reviewed and modified to keep ePHI protection effective.	Safeguards for Protected Health Information	Evaluation-Policy.pdf::::1, ::::2 Implementing a Schedule for Regular Vulnerability Scans of Systems Handling PHI.pdf::::5	
Has a policy and procedure been implemented to prevent, detect, contain, and correct security violations?	Correct	Yes	('This document outlines the steps for identifying, containing, mitigating, and reporting incidents while ensuring timely corrective actions to minimize harm and ensure compliance.'), ('The Incident Response Team is responsible for coordinating the response to security incidents.', 'IT/Security Team: Handles technical aspects of the incident, including containment, analysis, and remediation.', 'Monitor system logs, intrusion detection systems (IDS), and security information and event management (SIEM) tools.'), ('Collect Evidence: Gather relevant logs, system activity, and any indicators of compromise (IOCs).', 'For Unauthorized Access: Disable compromised user accounts. Revoke access rights immediately for any identified malicious actors.', 'Patch Vulnerabilities: Apply patches or system updates that address vulnerabilities exploited in the incident.')	The cited passages show that the incident-response policy defines monitoring to detect violations, actions to disable or contain compromised accounts, and corrective steps such as patching, proving that procedures exist to prevent, detect, contain, and correct security violations.	Safeguards for Protected Health Information	HIPAA Security Incident Response Plan.pdf::::1, ::::2, ::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has a risk analysis been conducted to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information?	Correct	Yes	('Our SRA documentation identifies and assesses potential threats and vulnerabilities (both technical and non-technical) to the confidentiality, integrity, and availability of all ePHI we create, receive, maintain, or transmit.'), ('Written results of the risk assessment should be communicated to workforce members who will be responsible for responding to identified threats and vulnerabilities after the completion of the risk assessment.', 'Threats & Vulnerabilities 1 Inadequate risk awareness or failure to identify new weaknesses'), ('It is the policy of Ulalo to conduct thorough and timely risk assessments of potential threats to the confidentiality, integrity, and availability of PHI.')	The cited passages confirm that a formal security risk assessment (SRA) identifies threats and vulnerabilities to ePHI and documents the results for follow-up, demonstrating that the required risk analysis has been carried out.	Safeguards for Protected Health Information	SRA_Tool_3_6.pdf::::5, ::::11 Risk-Management-Policy1.pdf::::2	
Has a security measure been implemented to reduce risks and vulnerabilities to a reasonable and appropriate level?	Correct	Yes	('Contingency planning controls shall be implemented based on application and data criticality and integrated with the organization\'s risk management practices.'), ('· Encryption in transit and at rest', '· Centralized logging and audit trails', '· Strict access control and periodic access review'), ('Patch Vulnerabilities: Apply patches or system updates that address vulnerabilities exploited in the incident.', 'Strengthen Security: Implement security improvements, such as stronger access controls, two-factor authentication, or updated encryption standards.')	The cited passages show concrete safeguards—contingency planning, encryption, logging, access reviews, patching and control hardening—implemented to keep risks and vulnerabilities at a reasonable and appropriate level.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf::::1 Asset Management Policy and Procedure.pdf::::4 HIPAA Security Incident Response Plan.pdf::::3	
Is an appropriate sanction applied against a workforce member who fails to comply with security policies and procedures?	Correct	Yes	('H. SANCTIONS - Ulalo employees who fail to fully comply with Ulalo HIPAA Privacy, Security and Breach Notification Policies and Procedures contained herein will be subject to sanctions as deemed appropriate by management in accordance Ulalo.'), ('Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.')	The cited passages state that workforce members who violate security policies face disciplinary action up to termination, confirming that appropriate sanctions are enforced for non-compliance.	Complaints and Sanctions	Security-Privacy-Breach-Policy.pdf::::6 Evaluation-Policy.pdf::::2	
Is a procedure in place to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports?	Correct	Yes	('Monitor system logs, intrusion detection systems (IDS), and security information and event management (SIEM) tools.'), ('System logs that are routinely gathered must be reviewed in a timely manner.')	The cited passages require ongoing monitoring of system logs, IDS and SIEM data and state that routinely gathered logs must be reviewed promptly, demonstrating a documented, periodic review procedure for system-activity records.	Documentation and Record Retention	HIPAA Security Incident Response Plan.pdf::::2 Information-System-Activity-Review-Policy.pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has a security official been identified who is responsible for the development and implementation of the required policies and procedures?	Correct	Yes	('Approved By: Fabrice Kwetchet', 'Title: CEO & Security Officer'), ('The Information Security Officer will develop and recommend to Ulalo any necessary Security Policy or Procedure changes.')	One passage names Fabrice Kwetchet as CEO / Security Officer, while the other assigns the Information Security Officer responsibility for developing and updating security policies, thereby identifying a single official charged with policy development and implementation.	Administrative Requirements	Asset Management Policy and Procedure.pdf::::7 Evaluation-Policy.pdf::::1	
Is a policy and procedure implemented to ensure appropriate access to electronic protected health information by the workforce?	Correct	Yes	('Purpose: The purpose of the Information Access Control Policy is to ensure that all members of the workforce have access to the systems and information appropriate to their job functions, and to ensure that inappropriate access is prevented under the HIPAA Security Policy- Security Standards for the Protection of Electronic Protected Health Information (ePHI).'), ('Restricted: strong access controls (least privilege), encryption in transit and at rest, logging/monitoring, approved storage locations, strict retention, incident escalation.')	The access-control policy ties workforce access to job functions and least-privilege principles, while the asset-classification rule mandates strong controls (encryption, monitoring) for ePHI, showing that formal policies and procedures govern and restrict workforce access to protected health information.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::1 Asset Management Policy and Procedure.pdf::::3	
Is a procedure implemented for the authorization and/or supervision of a workforce member who works with electronic protected health information?	Correct	Yes	('Access to these rooms is limited to authorized IT and facility services employees as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Technical Security Officer and only with an escort by an authorized IT or facility services workforce member.'), ('Each authorized individual is assigned a designated supervisor responsible for approving access and ensuring that access remains appropriate to job function.')	The first citation requires Technical Security Officer approval and escort for non-authorized personnel, while the second assigns supervisors responsibility for approving and overseeing users' access, evidencing formal authorization and supervision procedures for workforce members handling ePHI.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::2 05- Authorized Personnel & Supervisors.pdf::::2	
Is there a workforce clearance procedure to determine appropriate access to electronic protected health information?	Correct	Yes	('All persons or entities that have the need to access confidential or sensitive data, including ePHI, from information systems must first be authorized to access that data before having an account established on any information system.'), ('Ulalo will implement appropriate procedures to control and validate Ulalo employee access to all facilities used to house ePHI based systems.'), ('a. Conduct thorough background checks and vetting processes for all workforce members who will have access to ePHI.')	The cited passage(s) require prior authorization, background vetting and controlled validation before any workforce member is granted ePHI access, establishing a formal clearance procedure.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::1 Facility-Access-Controls-Policy.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::8	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is a termination procedure in place for ending access to electronic protected health information when a workforce member's employment ends?	Correct	Yes	('v. The Emergency access procedure must be used in case a terminated employee\'s computer account must be maintained for business reasons. Unless the Emergency Access procedure is implemented, all terminated employee computer accounts will be deleted immediately upon notification of the termination to all relevant parties.'), ('d. Removing or disabling authentication credentials in ePHI Systems for persons or entities that no longer require access to ePHI.'), ('Employees are required to return keys to the Supervisor on their last day of employment/last day of contracted work or services being provided.')	The cited passage(s) mandate immediate deletion of computer accounts, revocation of credentials, and return of physical keys upon termination, evidencing a documented off-boarding procedure that ends ePHI access.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::4 Person-or-Entity-Authentication - done.pdf::::2 Facility-Access-Controls-Policy.pdf::::1	
Is a policy and procedure for authorizing access to electronic protected health information consistent with the applicable requirements of subpart E (Privacy of Individually Identifiable Health Information) of this part?	Correct	Yes	('E. Verification of the Identity of the Individual Requesting PHI - Employees shall take reasonable steps to verify the identity and authority of all persons requesting access to PHI before making any disclosure.'), ('When a use or disclosure is not otherwise permitted under these policies, Ulalo will secure a valid authorization prior to making any use or disclosure of PHI.'), ('Microsoft ... shall within fifteen (15) days make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.')	The cited passage(s) require identity-and-authority verification, valid authorizations, and compliance with 45 CFR §164.524, demonstrating that access procedures align with the HIPAA Privacy Rule in subpart E.	Safeguards for Protected Health Information	Security-Privacy-Breach-Policy.pdf::::4 Uses-and-Disclosures-of-PHI.pdf::::2 Microsoft General - HIPAA BAA (May 2025).pdf::::4	
Is a policy and procedure in place for granting access to electronic protected health information?	Correct	Yes	('b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.'), ('All persons or entities that have the need to access confidential or sensitive data, including ePHI, from information systems must first be authorized to access that data before having an account established on any information system.'), ('Access requests require approval from the individual\'s supervisor and authorized management.')	The cited passage(s) describe formal steps—supervisor/management approval, authorization checks, and unique credential assignment—for provisioning ePHI access, evidencing a documented access-granting policy and procedure.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::3 Person-or-Entity-Authentication - done.pdf::::1 05- Authorized Personnel & Supervisors.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there a policy and procedure that establishes, documents, reviews, and modifies a user's right to access electronic protected health information?	Correct	Yes	('a. Documented procedures for granting persons and entities authentication credentials or for changing an existing authentication method.', 'e. Periodic validation that no redundant authentication credentials have been issued or are in use.'), ('1. Asset Owner approves access based on job role and least privilege.', '3. Access reviews occur: Tier 1: at least quarterly; Tier 2: at least semi-annually; Tier 3: annually or as needed.', '4. Departing personnel access is revoked according to offboarding procedures.'), ('Modifications to user access privileges must be tracked and logged.', 'At least annually, appropriate system managers and data owners must review user access rights to information assets.', 'Appropriate system managers and data owners must review and approve all requests for granting or modifying access to information assets.')	The cited passages show that formal procedures exist to grant, document, periodically review, and modify or revoke users' ePHI access, meeting the requirement.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::2 Asset Management Policy and Procedure.pdf::::6 Technical-Safeguards-Access-Control-Policy.pdf::::1	
Is a security awareness and training program implemented for all the members of the workforce?	Correct	Yes	('Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and Procedures and that he/she understands and agrees to abide by the guidelines contained herein.'), ('Scope: The security awareness program is designed to educate all users on the security policy for Ulalo.', '1. The Security Officer will be responsible for implementing and ensuring this policy is followed by all employees.'), ('1. Ulalo workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and patient protected health information.')	The cited passages confirm that every workforce member is required to complete HIPAA security training and that a comprehensive awareness program applies to all users.	Administrative Requirements	Security-Privacy-Breach-Policy.pdf::::2 Security-Awareness-Training-Policy.pdf::::1 Information-System-Activity-Review-Policy.pdf::::2	
Is a periodic security update provided as part of the security awareness and training program?	Correct	Yes	('The security awareness training for system administrators should include: d. Security reminders for periodic security updates', 'The Security Officer/ Security Awareness Training Team will implement monthly security training updates. All users are required to read these updates and implement any changes.')	The cited passage states that monthly security training updates are issued and must be read by all users, demonstrating periodic security updates within the program.	Administrative Requirements	Security-Awareness-Training-Policy.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is a procedure in place for guarding against, detecting, and reporting malicious software?	Correct	Yes	('This document outlines the steps for identifying, containing, mitigating, and reporting incidents while ensuring timely corrective actions to minimize harm and ensure compliance.', 'Malware/Ransomware: Malicious software designed to compromise system integrity or availability.'), ('Ulalo utilizes Microsoft native security services within Azure to provide antivirus and anti malware protections. These controls include continuous monitoring for malicious software, threat detection, and alerting mechanisms integrated into the Azure platform.', 'Anti malware related events and security alerts are logged and reviewed as part of Ulalo\'s centralized security monitoring and audit process, supporting investigation and compliance audits.'), ('I, the undersigned, confirm that Ulalo SRL has implemented and maintains antivirus and anti malware protections to safeguard electronic Protected Health Information (ePHI). These controls are actively monitored and reviewed as part of Ulalo\'s HIPAA compliance program.')	The cited passages describe continuous anti-malware protections, monitoring, alerting, logging, and explicit procedures for reporting malware incidents, fulfilling the requirement.	Safeguards for Protected Health Information	HIPAA Security Incident Response Plan.pdf::::1 16_Antivirus_and_Anti_Malware_Implementation_Attestation.pdf::::1, ::::2	
Is a log-in attempt monitored and are discrepancies reported?	Correct	Yes	('Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Microsoft becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer\'s Unsecured Protected Health Information that Microsoft may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule).', 'For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Microsoft\'s firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information.'), ('b. All employees are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.'), ('c. Documented procedures for detecting and responding to any person or entity attempting to access ePHI without proper authentication.'	The cited passages show that unsuccessful log-on attempts are explicitly logged as security incidents and must be reported to the customer, while internal policies require staff to monitor, log and escalate unauthorized or failed authentication attempts. This confirms that log-in attempts are monitored and discrepancies are reported.	Safeguards for Protected Health Information	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Facility-Access-Controls-Policy.pdf::::2 Person-or-Entity-Authentication - done.pdf::::2	
Is there a procedure for creating, changing, and safeguarding passwords?	Correct	Yes	('a. Documented procedures for granting persons and entities authentication credentials or for changing an existing authentication method.', 'f. Protection of authentication credentials (e.g., passwords, PINs) with appropriate controls to prevent unauthorized access.', 'g. When feasible, masking, suppressing, or otherwise obscuring the passwords and PINs of persons and entities seeking to access ePHI so that unauthorized persons are not able to observe them'), ('c. Each user\'s password should meet the minimum requirements as outlined below: i. Must be a minimum of eight characters in length. ii. Must contain a unique character. iii. Must contain a number. iv. May not contain your user-name or any part of your full name ... vii. Users must not allow another user to use their unique username or password.', 'd. Users must ensure that their username and password is not documented, written, or otherwise exposed in an insecure manner.')	The cited passages establish documented steps for issuing or changing authentication credentials, detailed complexity rules for new passwords, and controls to protect and mask credentials, demonstrating a complete procedure for creating, changing and safeguarding passwords.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is a policy and procedure implemented to address security incidents?	Correct	Yes	('This policy applies to all workforce members, systems, and operations of Ulalo.', 'This document outlines the steps for identifying, containing, mitigating, and reporting incidents while ensuring timely corrective actions to minimize harm and ensure compliance.'), ('The following Policies and Procedures will govern the use and disclosure of Protected Health Information ("PHI") at Ulalo, as well as what steps will be taken in the event unsecured PHI is breached in a manner prohibited under HIPAA.')	The cited passages present a Security Incident Response Plan and a breach policy that define identification, containment, mitigation and reporting steps, confirming that formal policy and procedures for handling security incidents are in place.	Safeguards for Protected Health Information	HIPAA Security Incident Response Plan.pdf::::1 Security-Privacy-Breach-Policy.pdf::::2	
Is there a response and reporting mechanism to identify and respond to suspected or known security incidents?	Correct	Yes	('This document outlines the steps for identifying, containing, mitigating, and reporting incidents while ensuring timely corrective actions to minimize harm and ensure compliance.'), ('ix. Determination of significant events requiring further review and follow-up.', 'x. Identification of appropriate reporting channels for review of results and required follow-up.')	The cited passages describe documented processes for detecting incidents, determining their significance, and using designated reporting channels for escalation and follow-up, demonstrating an operational mechanism for responding to and reporting security incidents.	Safeguards for Protected Health Information	HIPAA Security Incident Response Plan.pdf::::1 Information-System-Activity-Review-Policy.pdf::::3	
Is a security incident documented along with its outcome?	Correct	Yes	('f. Conclusions', 'h. Actions', 'j. Follow-up'), ('Complete Incident Report: Include the root cause, response timeline, affected ePHI, and actions taken.'), ('. Document Findings: Document the investigation process, actions taken, and results, including the root cause of the breach.')	The cited passages require incident records to capture conclusions, actions, root-cause analysis and follow-up steps, showing that every security incident is formally documented together with its outcome.	Documentation and Record Retention	Information-System-Activity-Review-Policy.pdf::::3 HIPAA Security Incident Response Plan.pdf::::4 HIPAA Breach Response Plan.pdf::::2	
Is a policy and procedure established for responding to emergencies that damage systems containing electronic protected health information?	Correct	Yes	('6. Disaster Recovery Plan Ulalo shall: - Maintain procedures to restore systems, applications, and data following a disaster - Prioritize restoration based on application and data criticality - Define recovery objectives (e.g., RPO/RTO) where appropriate - Assign roles and responsibilities for disaster recovery activities', '7. Emergency Mode Operation Plan Ulalo shall: - Identify critical functions that must continue during emergency conditions - Define procedures for operating systems in a limited or degraded mode - Ensure safeguards remain in place to protect PHI during emergency operations'), ('14. Emergency Mode Operation Procedure 1. Activate emergency operations when full functionality is unavailable. 2. Limit system access to essential personnel. 3. Maintain logging and security controls to the extent practicable.'), ('8) Emergency Access a. The HIPAA Security Rule requires Business Associates to establish procedures to allow access to ePHI during an emergency. During an emergency or disaster, Business Associates must remember that protecting ePHI is of utmost importance. Emergency procedures may be very different from standard operating procedures, but they	Disaster-recovery and emergency-mode plans, together with emergency-access procedures, are explicitly defined, confirming the organisation's documented process for responding to events that could damage ePHI systems.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf::::2, ::::3 Technical-Safeguards-Access-Control-Policy.pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is a procedure in place to create and maintain retrievable exact copies of electronic protected health information?	Correct	Yes	('6. All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA\'s, when storing original ePHI. Backups of original ePHI must be stored off-site in a physically secure facility.'), ('12. Backup Procedure 1. Identify systems and data requiring backup based on criticality. 2. Configure automated backups where feasible.'), ('The data and applications on the systems resident at the location are either actively synchronized with the corresponding systems in the Business Associate or will be brought up-to-date from data backups when the site is activated.')	Regular backup requirements, an explicit backup procedure and off-site synchronization demonstrate that exact, retrievable copies of ePHI are created and maintained.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::2 Contingency And Disaster Recovery Policy.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::4	
Is there a procedure to restore any loss of data?	Correct	Yes	('Restore Data: Recover ePHI from secure backups and ensure integrity before bringing systems back online.'), ('O Restore from the last known good backup.'), ('All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA\'s, when storing original ePHI. Backups of original ePHI must be stored off-site in a physically secure facility.')	Procedures specify restoring systems from secure or last-known-good backups and mandate routine, testable backups, confirming an established method to recover lost data.	Safeguards for Protected Health Information	HIPAA Security Incident Response Plan.pdf::::3, ::::4 Media-Sanitization-and-Disposal-Policy.pdf::::2	
Is there a procedure to enable continuation of critical business processes for the security of electronic protected health information during emergency mode?	Correct	Yes	('Emergency Mode Operation: The continuation of critical business functions while systems are operating in a degraded or emergency state.'), ('- Identify critical functions that must continue during emergency conditions', '- Ensure safeguards remain in place to protect PHI during emergency operations'), ('a. The HIPAA Security Rule requires Business Associates to establish procedures to allow access to ePHI during an emergency. During an emergency or disaster, Business Associates must remember that protecting ePHI is of utmost importance.', 'b. To ensure that access to critical ePHI is maintained during an emergency situation, each Department must establish and implement procedures to ensure that access to a system that')	The cited passages define an Emergency Mode Operation Plan that identifies critical functions, maintains PHI safeguards, and obliges departments to keep ePHI accessible during emergencies, thereby ensuring continuation of critical business processes.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf::::1, ::::2 Technical-Safeguards-Access-Control-Policy.pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is a contingency plan periodically tested and revised?	Correct	Yes	('This policy satisfies the HIPAA Security Rule contingency planning requirements at 45 CFR §164.308(a)(7), including disaster recovery, data backup, emergency operations, and testing and revision procedures.'), ('- Periodically test contingency and disaster recovery procedures (e.g., backup restore tests, tabletop exercises)', '- Revise contingency plans based on test results, incidents, system changes, or environmental changes'), ('15. Testing and Revision Procedure', '1. Conduct contingency testing activities on a periodic basis.', '3. Update plans, procedures, and documentation as needed.')	The cited passages require periodic testing of contingency and disaster-recovery procedures and mandate updating the plans when tests, incidents, or changes warrant, demonstrating that the contingency plan is regularly tested and revised.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf::::1, ::::2, ::::3	
Is the relative criticality of a specific application and data assessed in support of contingency planning?	Correct	Yes	('7. Application/System Criticality Levels', 'Each application/system must receive a criticality level: Critical (Tier 1)... Important (Tier 2)... Standard (Tier 3)...'), ('Each asset record must include, at minimum: · System criticality tier (Tier 1/2/3)', '13. Application and Data Criticality Analysis Procedure ... At least annually for all in-scope assets'), ('The deliverable is a documented table/report ("Criticality Register") containing:', 'Asset name', 'Data classification', 'Criticality tier', 'CIA impact notes', 'Required control set (backup targets, monitoring, access review cadence)')	The cited passages establish a formal Application and Data Criticality Analysis with defined tiers, criteria, and a documented Criticality Register, confirming that the organization assesses the relative criticality of applications and data for contingency planning.	Safeguards for Protected Health Information	Asset Management Policy and Procedure.pdf::::3, ::::5, ::::6	
Is a periodic evaluation performed to assess the security policy and procedure?	Correct	Yes	('Once compliance with the Security or Privacy Regulations is established, the Ulalo Security or Privacy Policies or Procedures will be evaluated on a periodic basis-annually to assure continued viability in light of technological, environmental or operational changes that could affect the security of PHI and ePHI.'), ('6. Evaluation of Ulalo Procedures a. Ulalo must periodically annually evaluate its HIPAA Security or Privacy Procedures to ensure that departments follow such Procedures and that these procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security or Privacy Policies.', '7. Internal Audit of Security Policies and Procedures a. All HIPAA Security or Privacy Policies and Ulalo Department procedures are subject to periodic audits by Ulalo management and/or the Information Security or Privacy Officer.'), ('17. Review and Approval', 'This policy shall be reviewed at least annually and updated as necessary.')	The cited passages mandate an annual evaluation and audit of security policies and procedures and require annual review and update, demonstrating that the organization performs periodic assessments of its security policy and procedures.	Administrative Requirements	Evaluation-Policy.pdf::::1, ::::2 Contingency And Disaster Recovery Policy.pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is a written contract or other arrangement documented with the business associate to ensure the safeguarding of electronic protected health information?	Correct	Yes	('If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data, FastTrack Data, or Professional Services Data, this HIPAA Business Associate Agreement ("BAA") is incorporated upon execution of an agreement ("Agreement") that incorporates the Microsoft Products and Services Data Protection Addendum.'), ('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.'), ('e. Obtain a signed HIPAA-compliant business associate agreement.'), ('Where third parties handle PHI, the engagement must comply with HIPAA-related contracting and security requirements.')	The cited passages include the HIPAA Business Associate Agreement itself and internal policies requiring a signed BAA with any third party handling PHI, demonstrating that a written contractual arrangement is in place to safeguard electronic protected health information.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::1, ::::3 Information-System-Activity-Review-Policy.pdf::::4 Asset Management Policy and Procedure.pdf::::2	
Has the covered entity or business associate implemented policies and procedures to limit physical access to its electronic information system?	Correct	Yes	('This Policy covers the procedures that limit physical access to electronic protected health information (ePHI) systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.'), ('All Ulalo computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices, which alert the Technical Security Officer of any problems. Access to these rooms is limited to authorized IT and facility services employees as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms.'), ('Users are required to make information systems inaccessible by any other individual when unattended by the user, such as locking or logging off the systems;', 'Workstations in patient rooms or public areas must be logged off or locked when not in use.'), ('Those security measures include appropriate safeguards such as limiting building access, implementing firewalls and utilizing password	The cited policies require locked and monitored facilities, secure workstation practices, and restricted building access, evidencing documented procedures that limit physical access to electronic information systems containing ePHI.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1, ::::2 Workstation-Security-Policy.pdf::::1 Security-Privacy-Breach-Policy.pdf::::3	
Has the covered entity or business associate established procedures for facility access to support restoration of lost data under the disaster recovery plan?	Correct	Yes	('g. Servers with ePHI are maintained off-site in order to reduce potential damage during a disaster at the facility.', 'h. The Business Associate has established an off-site disaster recovery location. Provisioning and maintenance of this location have been arranged through external contractors. In the event of its activation, it will be staffed by a combination of the Business Associate and these contractors. The data and applications on the systems resident at the location are either actively synchronized with the corresponding systems in the Business Associate or will be brought up-to-date from data backups when the site is activated. The system is tested and exercised [once in six months].')	The cited passage describes an off-site disaster recovery location, access provisioning, synchronization of data, and semi-annual testing, confirming procedures that enable facility access for data restoration.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the covered entity or business associate implemented a facility security plan to protect against unauthorized physical access, tampering, and theft?	Correct	Yes	('Ulalo will maintain a Facility Security Plan that outlines and documents its procedures to safeguard all facilities, systems, and equipment used to store ePHI against unauthorized physical access, tampering, or theft.'), ('All Ulalo computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices, which alert the Technical Security Officer of any problems. Access to these rooms is limited to authorized IT and facility services employees as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms.'), ('It is the policy of Ulalo to fully comply with the HIPAA Security Rule, including to: (2) protect against reasonably anticipated threats or hazards to the security or integrity of ePHI.', 'Those security measures include appropriate safeguards such as limiting building access, implementing firewalls and utilizing password protections, as these access controls are recognized by HHS as important for safeguarding PHI.'),	The cited passages mandate a formal Facility Security Plan, locked and monitored server rooms, restricted building access, and secure server placement, demonstrating measures that protect facilities and equipment against unauthorized access, tampering, and theft.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1, ::::2 Security-Privacy-Breach-Policy.pdf::::3 Workstation-Security-Policy.pdf::::2	
Are access control and validation procedures currently in place to control a person's access to facilities based on their role or function?	Correct	Yes	('1. Ulalo will implement appropriate procedures to control and validate Ulalo employee access to all facilities used to house ePHI based systems.', 'i. Employees as approved by their supervisor and as needed to perform their job duties.'), ('c. All Ulalo computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices, which alert the Technical Security Officer of any problems. Access to these rooms is limited to authorized IT and facility services employees as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Technical Security Officer and only with an escort by an authorized IT or facility services workforce member.', '2. In addition to badge access, Ulalo requires a signature log of all employees accessing server rooms and data center.'), ('This list is updated whenever access is granted, modified, or revoked.', '. Access levels are validated against job roles and supervisory approval')	The cited passages show that facility entry is limited to staff whose access is validated against job roles and supervisory approval; other individuals require special authorisation, escort, and logging. This demonstrates role-based access control and validation procedures are in force.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1, ::::2 06- Authorized Personnel Access Le.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf:::4	
Does the covered entity or business associate maintain records of repairs and modifications to the physical components of a facility related to security?	Correct	Yes	('i. Description of the repair or modification including a summary of the original plans, any changes made to the plans, and reasons for any changes made to the plans.'), ('After completion of the project, forward all documentation to the Security Manager.', 'The [Security Manager] maintains all documentation for a minimum of six years [§164.530(j)].')	The cited passages mandate that detailed repair or modification records be forwarded to the Security Manager, who stores them for at least six years, confirming that such documentation is maintained.	Documentation and Record Retention	Facility-Access-Controls-Policy.pdf::::2, ::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the covered entity or business associate implemented policies and procedures that specify workstation use for accessing electronic protected health information?	Correct	Yes	('Servers, workstations, or other computer systems located in open, common, or otherwise unsecure areas, that access, transmit, receive, or store ePHI, or that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms. These systems must terminate a user session after a maximum of 15 minutes of inactivity.', 'When leaving a server, workstation, or other computer system unattended, users must lock or activate the system\'s automatic logoff mechanism (e.g. CTRL+ALT+DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.'), ('ii. Remote access workstations must employ a virus detection and protection mechanism.', 'd. Users of remote workstations must comply with HIPAA Security Policy - Workstation Acceptable Use Policy.'), ('5. Workstation Use a. Workstations should only be used for authorized business purposes. d. Users must take actions to prevent unauthorized viewing, such as privacy screens, minimizing sessions, closing laptops, etc.'),	The cited passages define how workstations that handle ePHI must be used—covering auto-logoff, virus protection, authorised business use only, access limited to identified staff, and controlled movement of devices—showing that comprehensive workstation-use policies and procedures are implemented.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::5, ::::6 Workstation-Security-Policy.pdf::::1, ::::2 Facility-Access-Controls-Policy.pdf::::1	
Is there physical safeguarding in place at the workstation that accesses electronic protected health information to restrict access to authorized users?	Correct	Yes	('4. Automatic Logoff a. Users are required to make information systems inaccessible by any other individual when unattended by the user, such as locking or logging off the systems; if the device is used only by a single individual with a unique log in, it may be locked.', '5. Workstation Use b. When possible, workstations should be placed in secure areas. c. Workstations in patient rooms or public areas must be logged off or locked when not in use.'), ('a. Workstations may only be accessed and utilized by authorized employees or Business Associates wearing appropriate identification to complete assigned job/ contract responsibilities.')	The cited passages require that ePHI workstations be located in secure areas or locked when unattended and restrict physical use to identified, authorised personnel, demonstrating effective physical safeguards.	Safeguards for Protected Health Information	Workstation-Security-Policy.pdf::::1 Facility-Access-Controls-Policy.pdf::::1	
Does the covered entity or business associate have policies and procedures governing the receipt and removal of hardware and electronic media containing electronic protected health information?	Correct	Yes	('The Company maintains procedures governing the receipt, movement, and removal of workstations and electronic media that may contain electronic protected health information (ePHI). Workstations and electronic media are subject to authorization requirements prior to removal, inspection upon receipt, logging and tracking of asset movement, secure transport when applicable, and documentation of transfer, reuse, or disposal to ensure accountability throughout the device and media lifecycle.'), ('Ulalo shall maintain an up-to-date inventory of information assets. Assets that store, process, or transmit sensitive data (including PHI) must be inventoried prior to use in production.', 'Coordinating decommissioning and secure disposal'), ('Ulalo requires that prior to disposal or reuse of hardware or media that contains or previously contained ePHI either the data will be securely overwritten or the device and/or media be physically destroyed and that such steps taken will be documented.', '1. All electronic media must be properly sanitized before it is transferred from the current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.'	The cited passages require assets containing ePHI to be inventoried and inspected upon receipt and to follow documented, secure decommissioning or disposal processes, demonstrating policies and procedures for both receipt and removal.	Safeguards for Protected Health Information	Workstation-Security-Policy.pdf::::2 Asset Management Policy and Procedure.pdf::::2 Media-Sanitization-and-Disposal-Policy.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Are procedures for the disposal of electronic protected health information and the hardware or electronic media on which it is stored implemented?	Correct	Yes	('1. All electronic media must be properly sanitized before it is transferred from the current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.', '2. All destruction/disposal of patient health information media will be done in accordance with federal and state laws and regulations and pursuant to the organization\'s written retention policy/schedule.'), ('a. Specify the method of destruction/disposal.', 'f. Provide proof of destruction/disposal (e.g. certificate of destruction).'), ('16. Decommissioning and Secure Disposal Procedure 1. Owner submits a decommission request including affected assets and data. 2. Data retention rules are confirmed (contractual/regulatory). 3. Data is securely deleted or archived according to retention policy. 4. Access is removed; credentials are rotated/revoked. 5. Inventory entry is updated to "Retired" with date and disposition.')	The cited passages describe formal decommissioning workflows, required sanitization or destruction methods, and proof-of-destruction documentation, confirming that disposal procedures for ePHI and its media are in place and executed.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::1, ::::3 Asset Management Policy and Procedure.pdf::::6	
Does the covered entity or business associate remove electronic protected health information from electronic media before the media are made available for re-use?	Correct	Yes	('5. Before reuse of any recordable and erasable media, all ePHI must be rendered inaccessible, cleaned, or scrubbed. Any equipment or storage media that contains confidential, critical, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.'), ('3. Data is securely deleted or archived according to retention policy.')	The cited passages state that all ePHI must be securely deleted, scrubbed, or otherwise rendered inaccessible before any hardware or media is reused, meeting the removal requirement.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::2 Asset Management Policy and Procedure.pdf::::6	
Is there a maintained record of the movements of hardware and electronic media containing electronic protected health information?	Correct	Yes	('The Company maintains procedures governing the receipt, movement, and removal of workstations and electronic media that may contain electronic protected health information (ePHI). Workstations and electronic media are subject to authorization requirements prior to removal, inspection upon receipt, logging and tracking of asset movement, secure transport when applicable, and documentation of transfer, reuse, or disposal to ensure accountability throughout the device and media lifecycle.')	The cited passage requires logging and tracking the movement of workstations and media containing ePHI, ensuring a maintained record throughout their lifecycle.	Documentation and Record Retention	Workstation-Security-Policy.pdf::::2	
Are retrievable, exact copies of electronic protected health information created before movement of equipment?	Correct	Yes	('If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.'), ('Create and maintain retrievable, exact copies of critical data, including PHI')	The cited passages require that a retrievable copy of ePHI be created before a device or media is disposed of and direct staff to maintain exact copies of PHI, confirming that copies are produced prior to equipment movement.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::1 Contingency And Disaster Recovery Policy.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the covered entity or business associate implemented technical policies and procedures to allow access to electronic protected health information only to those with granted access rights?	Correct	Yes	('b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.'), ('Access approvals and least-privilege enforcement', 'Ulalo shall classify data and systems to ensure appropriate handling, access control, encryption, monitoring, retention, and incident response.'), ('The purpose of this Access Control Policy is to establish administrative and technical safeguards governing user access to Ulalo systems that create, receive, maintain, or transmit electronic Protected Health Information (ePHI), in accordance with the HIPAA Security Rule.')	The cited passages prescribe unique-user authentication, role-based and least-privilege access approvals, and firewall/ RBAC safeguards, demonstrating technical controls that restrict ePHI access solely to authorized users.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::3 Asset Management Policy and Procedure.pdf::::2 03- Access Control Policy â	
Is unique user identification assigned for identifying and tracking user identity within electronic information systems?	Correct	Yes	('Ulalo assigns a unique user identifier to every individual accessing ePHI systems. Shared or generic user accounts are prohibited.'), ('b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.'), ('· Unique user identifier (Azure AD UPN)')	The cited passages state that all users are given a unique user ID (e.g., Azure AD UPN) and that shared accounts are forbidden, ensuring each person can be uniquely identified and tracked in the systems.	Safeguards for Protected Health Information	01_Unique_User_ID_Policy.pdf ::::1 Technical-Safeguards-Access-Control-Policy.pdf::::3 06- Authorized Personnel Access Le.pdf::::1	
Is an emergency procedure in place to access necessary electronic protected health information?	Correct	Yes	('7. Emergency Mode Operation Plan - Ulalo shall: - Identify critical functions that must continue during emergency conditions - Define procedures for operating systems in a limited or degraded mode - Ensure safeguards remain in place to protect PHI during emergency operations'), ('Emergency Mode Operation Procedure 1. Activate emergency operations when full functionality is unavailable. 2. Limit system access to essential personnel. 3. Maintain logging and security controls to the extent practicable.'), ('f. Emergency accounts have been created for accessing ePHI for continuing care. These are unique usernames and passwords that can be tracked easily. They should not be used unless there is a true emergency.')	The cited passages outline an Emergency Mode Operation Plan and Procedure and dedicate emergency accounts for accessing ePHI, ensuring that essential personnel can reach needed PHI during crises while maintaining security controls.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf:::2, ::::3 Technical-Safeguards-Access-Control-Policy.pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does an automatic logoff mechanism terminate an electronic session after a set period of inactivity?	Correct	Yes	('These systems must terminate a user session after a maximum of 15 minutes of inactivity.', 'These application sessions must automatically terminate after a maximum of 30 minutes of inactivity.'), ('c. Information systems should automatically log users off the systems after [30] minutes of inactivity. (Each organization must choose the number of minutes for automatic logoff based on its risk analysis.)')	The cited passages state that both system and application sessions are configured to log users off automatically after 15–30 minutes of inactivity, confirming that an inactivity timer/automatic log-off mechanism is in force.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::5 Workstation-Security-Policy.pdf::::1	
Is encryption and decryption of electronic protected health information actively used?	Correct	Yes	('Ulalo encrypts all systems storing ePHI using Microsoft Azure native encryption mechanisms.', 'Ulalo encrypts ePHI during transmission across internal and external networks. Records demonstrate that application endpoints use HTTPS with TLS encryption.'), ('· Azure Storage Service Encryption (AES-256)', '. Encryption is enforced for data at rest and in transit'), ('i. Any portable device that contains PHI must be encrypted. Portable media is also subject to the same requirements.')	The cited passages confirm that ePHI is encrypted both at rest and in transit within Azure services and that portable devices containing PHI must also be encrypted, showing active use of encryption and corresponding decryption controls.	Safeguards for Protected Health Information	07_Encrypted_Data_Storage_and_Transmission_Records.pdf::::1 02- Azure - HIPAA Proof of Implementation.pdf::::3 Workstation-Security-Policy.pdf::::2	
Are audit controls actively recording and examining activity in systems with electronic protected health information?	Correct	Yes	('Ulalo will review logs of access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI.', 'The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.'), ('Control Area: Audit Controls & Security Monitoring', 'This document serves as formal proof of implementation for HIPAA Security Rule requirements related to system logs that record login attempts, including successful and failed authentication attempts. It demonstrates how Ulalo captures, retains, and reviews authentication activity for systems that access electronic Protected Health Information (ePHI).'), ('Monitors authentication activity, risky sign-ins, and access anomalies.', 'Capture activity logs for administrative actions, configuration changes, and security events.')	The cited passages require mechanisms that log and review access, authentication and configuration activities, with continuous monitoring via SIEM and Azure services, demonstrating that audit controls actively record and examine ePHI system activity.	Safeguards for Protected Health Information	Information-System-Activity-Review-Policy.pdf::::1 10- System Login & Authentication Logs â	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Are there active measures to prevent improper alteration or destruction of electronic protected health information?	Correct	Yes	('Ulalo shall not delete or overwrite original PHI when implementing an amendment, unless explicitly instructed by the Covered Entity and permitted by law.'), ('6. All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA\'s, when storing original ePHI. Backups of original ePHI must be stored off-site in a physically secure facility.'), ('I, the undersigned, confirm that Ulalo SRL has implemented and maintains integrity controls to protect electronic Protected Health Information (ePHI) from improper alteration or destruction.', 'These controls are actively managed, monitored, and reviewed as part of Ulalo\'s HIPAA compliance program.')	The cited passages prohibit overwriting original PHI, mandate regular tested backups stored securely off-site, and confirm active integrity controls—together providing safeguards against improper alteration or destruction of ePHI.	Safeguards for Protected Health Information	Amendment of Protected Health Information.pdf::::2 Media-Sanitization-and-Disposal-Policy.pdf::::2 12_Integrity_Controls_Implementation_Attestation.pdf::::2	
Is there an active mechanism to authenticate that electronic protected health information remains unaltered and undestroyed by unauthorized means?	Correct	Yes	('The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.', '4. Improper alteration or destruction of ePHI (information integrity).'), ('Ulalo uses centralized audit logging to detect and investigate potential improper alteration of ePHI.', 'Authentication events, access attempts, and administrative actions are logged and reviewed to support integrity verification and incident response.'), ('I, the undersigned, confirm that Ulalo SRL has implemented and maintains integrity controls to protect electronic Protected Health Information (ePHI) from improper alteration or destruction.', 'These controls are actively managed, monitored, and reviewed as part of Ulalo\'s HIPAA compliance program.')	The cited passages require audit logging that detects improper alteration or destruction of ePHI and confirm that integrity controls are actively managed and reviewed, demonstrating an operative mechanism that authenticates the data's integrity.	Safeguards for Protected Health Information	Information-System-Activity-Review-Policy.pdf::::1 12_Integrity_Controls_Implementation_Attestation.pdf::::1, ::::2	
Are identity verification procedures for accessing electronic protected health information actively enforced?	Correct	Yes	('b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.'), ('When a disclosure of PROTECTED HEALTH INFORMATION is conditioned upon particular documentation, statements, or representations, prior to the disclosure of the PHI, the identity of the person making the request and the authority of the person to make the request shall be verified.'), ('b. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.')	The cited passages mandate unique user IDs with secure passwords or other strong authentication methods and require verification of a requester's identity and authority before any PHI disclosure, proving identity-verification procedures are actively enforced.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::3 Uses-and-Disclosures-of-PHI.pdf::::2 Person-or-Entity-Authentication - done.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Are there active technical security measures to prevent unauthorized access to electronic protected health information during electronic transmission?	Correct	Yes	('Restricted: strong access controls (least privilege), encryption in transit and at rest, logging/monitoring, approved storage locations, strict retention, incident escalation.'), ('Ulalo encrypts ePHI during transmission across internal and external networks. Records demonstrate that application endpoints use HTTPS with TLS encryption. Encryption in transit is enforced through Azure-native networking and application services.'), ('Minimum Inbound TLS Version 1.2', 'HTTPS only', 'FTPS only')	The passages show that ePHI is protected in transit by enforced HTTPS/TLS 1.2+, strict encryption requirements, and least-privilege network controls, thereby providing active technical safeguards against unauthorized access during transmission.	Safeguards for Protected Health Information	Asset Management Policy and Procedure.pdf:::3 07_Encrypted_Data_Storage_and_Transmission_Records.pdf:::1 18_Policy_and_Procedure_Discussion_Meeting_Records_Attestation.pdf::::2	
Are integrity controls in place to detect improper modification of electronic protected health information during transmission until disposal?	Correct	Yes	('Encryption of ePHI is required in some instances as a transmission control and integrity mechanism.')	The cited passage states that encryption is required as an integrity mechanism for ePHI during transmission, confirming the presence of controls to detect or prevent unauthorized modification.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::5	
Is encryption of electronic protected health information actively implemented when appropriate?	Correct	Yes	('i. Any portable device that contains PHI must be encrypted.', 'i. Portable media is also subject to the same requirements.'), ('. Restricted: strong access controls (least privilege), encryption in transit and at rest, logging/monitoring, approved storage locations, strict retention, incident escalation.'), ('Ulalo encrypts all systems storing ePHI using Microsoft Azure native encryption mechanisms. Records are maintained showing that Azure Storage Accounts and Azure SQL or managed databases are configured with encryption at rest, including Transparent Data Encryption (TDE) where applicable.', 'Ulalo encrypts ePHI during transmission across internal and external networks. Records demonstrate that application endpoints use HTTPS with TLS encryption. Encryption in transit is enforced through Azure-native networking and application services.')	The cited passages mandate encryption for PHI on portable devices and media, classify PHI assets as requiring encryption at rest and in transit, and confirm Azure-based encryption of all systems that store or transmit ePHI—demonstrating that encryption is actively implemented whenever appropriate.	Safeguards for Protected Health Information	Workstation-Security-Policy.pdf::::2 Asset Management Policy and Procedure.pdf:::3 07_Encrypted_Data_Storage_and_Transmission_Records.pdf:::1	
Does the business associate contract mandate compliance with the applicable requirements of the Security subpart?	Correct	Yes	('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.'), ('Where third parties handle PHI, the engagement must comply with HIPAA-related contracting and security requirements.')	The contract clause requires the business associate to comply with 45 CFR Part 164 Subpart C, and the policy states that any third-party engagement handling PHI must meet HIPAA security requirements, proving that contracts mandate Security Rule compliance.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Asset Management Policy and Procedure.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate ensure a subcontractor handling electronic protected health information complies with the applicable requirements of the Security subpart?	Correct	Yes	('(iv) Subcontractors. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. Microsoft remains responsible for its Subcontractors', '), (', ')'), ( )	The BAA obligates subcontractors to comply with 45 CFR Part 164 Subpart C and keeps the business associate accountable, while the procedure requires verification of agreements and security controls whenever a subcontractor processes PHI—showing the associate ensures subcontractor compliance.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Asset Management Policy and Procedure.pdf::::7	
Does the business associate report security incidents, including breaches of unprotected health information, to the covered entity?	Correct	Yes	('(iii) Reporting. Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Microsoft becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer\'s Unsecured Protected Health Information that Microsoft may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event more than seventy-two (72) hours after Microsoft\'s discovery of a Breach.'), ('ii. Timing of Notification - Ulalo shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery of the breach.', '3. If additional information regarding the breach is later discovered by Ulalo, that information will be promptly provided to the Covered Entity.')	The BAA requires prompt reporting of any security incident or breach of unsecured PHI within 72 hours, and the breach policy further mandates timely notification and updates within 60 days, confirming that the business associate reports such incidents to the covered entity.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Security-Privacy-Breach-Policy.pdf::::6	
Are the contract requirements for a business associate with a subcontractor identical to those between a covered entity and a business associate?	Correct	Yes	('(iv) Subcontractors. … Microsoft shall require its Subcontractors … to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information …')	The cited passage requires every subcontractor to accept the same or stricter PHI restrictions and conditions that bind Microsoft, thereby mirroring the contractual duties that exist between a covered entity and its business associate.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the covered entity or business associate implemented reasonable and appropriate policies and procedures to comply with the Security subpart's standards, implementation specifications, or other requirements?	Correct	Yes	('This policy establishes the scope, objectives, and procedures of Ulalo information security risk management process.', 'The policy covers the administrative, physical, and technical processes that enable and govern PHI that is created, maintained, received, or transmitted by Ulalo.'), ('b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.', 'a. The HIPAA Security Rule requires Business Associates to establish procedures to allow access to ePHI during an emergency.'), ('6. Evaluation of Ulalo Procedures a. Ulalo must periodically annually evaluate its HIPAA Security or Privacy Procedures to ensure that departments follow such Procedures and that these procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security or Privacy Policies.', '7. Internal Audit of Security Policies and Procedures a. All HIPAA Security or Privacy Policies and Ulalo Department procedures are subject to periodic audits by Ulalo management and/or the Information Security or Privacy Officer.'	The cited passages show formally approved risk-management, access-control, and evaluation policies—together covering administrative, physical, and technical safeguards and subject to periodic audit—demonstrating that reasonable and appropriate policies and procedures have been implemented to satisfy the HIPAA Security Rule.	Administrative Requirements	Risk-Management-Policy1.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::3 Evaluation-Policy.pdf::::2	
Is the policy and procedure implemented to comply with the Security subpart maintained in written (which may be electronic) form?	Correct	Yes	('HIPAA policies and procedures are maintained in a controlled central repository, and personnel responsible for implementing specific procedures have access to the latest approved versions, with availability and acknowledgment supported through access controls, acknowledgment tracking, or scheduled briefings.'), ('Asset Management Policy and Procedure (with Application & Data Criticality)', 'This policy and procedure establishes how Ulalo identifies, inventories, classifies, protects, and manages information assets-especially applications and data-throughout their lifecycle.')	The cited passages explicitly state that HIPAA policies and procedures are stored in a controlled repository and presented as written documents such as the Asset Management Policy, confirming that they are maintained in written (electronic) form.	Documentation and Record Retention	Security-Awareness-Training-Policy.pdf::::1 Asset Management Policy and Procedure.pdf::::1	
If an action, activity, or assessment is required by this Security subpart to be documented, is a written (which may be electronic) record maintained?	Correct	Yes	('15. Testing and Revision Procedure 1. Conduct contingency testing activities on a periodic basis. 2. Record test scope, outcomes, and identified gaps. 3. Update plans, procedures, and documentation as needed. 4. Track remediation actions to completion.', 'Documentation related to contingency planning, testing, and revisions shall be retained in accordance with record retention requirements.'), ('Significant findings shall be reported immediately in a written format. Ulalo security incident response form may be utilized to report a single event.', 'Routine findings shall be reported to the sponsoring leadership structure in a written report format.', 'These actions shall be documented and shared with the responsible and sponsoring departments/units.')	The contingency-planning policy mandates recording and retaining test results, while the activity-review policy requires that findings and corrective actions be documented in writing, demonstrating that written records are maintained whenever the Security Rule calls for documentation.	Documentation and Record Retention	Contingency And Disaster Recovery Policy.pdf::::3 Information-System-Activity-Review-Policy.pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is the documentation required by Standard Documentation section retained for 6 years from the date of its creation or the date when it last was in effect, whichever is later?	Correct	Yes	('The [Security Manager] maintains all documentation for a minimum of six years [§164.530(j)].'), ('Disclosure records shall be retained for a minimum of six (6) years from the date of the disclosure or the date the record was created, whichever is later.')	The cited passages state that both general documentation and specific disclosure records must be stored for at least six years from creation or last effective date, meeting the retention requirement.	Documentation and Record Retention	Facility-Access-Controls-Policy.pdf::::3 Accounting of Disclosures Policy.pdf::::2	
Is the documentation made available to the person responsible for implementing the procedures to which the documentation pertains?	Correct	Yes	('Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and Procedures and that he/she understands and agrees to abide by the guidelines contained herein.'), ('HIPAA policies and procedures are maintained in a controlled central repository, and personnel responsible for implementing specific procedures have access to the latest approved versions, with availability and acknowledgment supported through access controls, acknowledgment tracking, or scheduled briefings.')	The cited passages state that employees must review and acknowledge the policies and that implementers have controlled access to the most current versions, demonstrating availability of documentation to responsible personnel.	Documentation and Record Retention	Security-Privacy-Breach-Policy.pdf::::2 Security-Awareness-Training-Policy.pdf::::1	
Is the documentation reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of the electronic protected health information?	Correct	Yes	('This policy shall be reviewed at least annually and updated as necessary to reflect changes in law, regulation, business operations, or HIPAA guidance.'), ('Once compliance with the Security or Privacy Regulations is established, the Ulalo Security or Privacy Policies or Procedures will be evaluated on a periodic basis—annually—to assure continued viability in light of technological, environmental or operational changes that could affect the security of PHI and ePHI.')	Policies mandate annual reviews and require updates whenever legal, environmental, or operational changes occur, demonstrating ongoing periodic review and revision.	Documentation and Record Retention	Accounting of Disclosures Policy.pdf::::3 Evaluation-Policy.pdf::::1	
Is a risk analysis conducted as part of the Security Management Process?	Correct	Yes	('Security risk analysis is a foundational component of identifying and assessing ePHI risks and vulnerabilities in your practice.'), ('It is the policy of Ulalo to conduct thorough and timely risk assessments of potential threats to the confidentiality, integrity, and availability of PHI.')	Both the SRA guidance and the organization's policy explicitly require conducting a security risk analysis as part of the security management process, satisfying the criterion.	Administrative Requirements	SRA_Tool_3_6.pdf::::3 Risk-Management-Policy1.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is risk management implemented in the Security Management Process?	Correct	Yes	('3. Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the above risk assessment process to ensure the confidentiality, integrity and availability of PHI.'), ('Contingency planning controls shall be implemented based on application and data criticality and integrated with the organization\'s risk management practices.'), ('§164.308(a)(1)(ii)(B)', 'Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?', 'Use internal or external experts to deploy security controls.')	The cited passages describe the formal risk-mitigation cycle, require contingency controls to be aligned with risk-management practices, and reference the HIPAA risk-management clause together with related implementation actions; this shows that risk management activities are embedded in the security management process.	Administrative Requirements	Risk-Management-Policy1.pdf::::4 Contingency And Disaster Recovery Policy.pdf::::1 SRA_Tool_3_6.pdf::::9	
Is there a sanction policy in place for the Security Management Process?	Correct	Yes	('Violations:', 'Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.'), ('Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers\' offices, business associates and partners may result in termination of the relationship and/or associated privileges.')	Both cited policies spell out disciplinary actions—up to termination—for non-compliance, establishing a clear sanction regime within the security management process.	Complaints and Sanctions	Evaluation-Policy.pdf::::2 Information-System-Activity-Review-Policy.pdf::::5	
Is there a regular information system activity review?	Correct	Yes	('Ulalo will review logs of access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI.', 'A review may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing.'), ('a. Access reviews on all the information systems shall be conducted periodically to ensure adequacy. The planned frequency of conducting all types of access reviews shall be quarterly.', 'c. Records of access review shall be maintained for further reference.'), ('1. Weekly Automated Vulnerability Scans')	The policy excerpts mandate periodic log and access reviews, set a quarterly schedule, and require weekly automated scans—demonstrating that information-system activity is reviewed on a regular, defined basis.	Administrative Requirements	Information-System-Activity-Review-Policy.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::2 Implementing a Schedule for Regular Vulnerability Scans of Systems Handling PHI.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is someone assigned security responsibility?	Correct	Yes	('Security Officer : Fabrice Kwetchet'), ('2. Periodic Evaluation by Ulalo Information Security Officer n a. The Information Security Officer will review on an on-going basis the viability of Ulalo Security Policies and general approaches taken by Departments in their Security Procedures.'), ('Title: CEO / Security Officer')	The cited passages explicitly designate a named Security Officer (also titled CEO / Security Officer) and describe that individual's on-going duties, confirming that security responsibility is formally assigned.	Administrative Requirements	Accounting of Disclosures Policy.pdf::::3 Evaluation-Policy.pdf::::1 02- Azure - HIPAA Proof of Implementation.pdf::::4	
Is there a procedure for authorization and/or supervision of a workforce member?	Correct	Yes	('Ulalo shall designate the employees or contractors who are authorized to use security testing and monitoring tools. Such tools may not be used by anyone not specifically authorized.'), ('All persons or entities that have the need to access confidential or sensitive data, including ePHI, from information systems must first be authorized to access that data before having an account established on any information system.')	The cited passages confirm that personnel must be formally designated or approved before gaining access and that supervisors control and monitor such authorization, evidencing documented workforce-member authorization and supervision procedures.	Administrative Requirements	Information-System-Activity-Review-Policy.pdf::::3 Person-or-Entity-Authentication - done.pdf::::1	
Is there a workforce clearance procedure?	Correct	Yes	('Conduct thorough background checks and vetting processes for all workforce members who will have access to ePHI. This includes verifying qualifications, checking references, and assessing any potential risks associated with granting access to sensitive information.')	The policy explicitly mandates background checks and vetting before granting access to sensitive data, establishing a formal workforce clearance procedure.	Administrative Requirements	Technical-Safeguards-Access-Control-Policy.pdf::::8	
Is there a termination procedure for a workforce member?	Correct	Yes	('Employees are required to return keys to the Supervisor on their last day of employment/last day of contracted work or services being provided.'), ('Departing personnel access is revoked according to offboarding procedures.')	The cited passages state that physical keys must be returned on the last workday and that system access is revoked through off-boarding procedures, demonstrating a documented termination process.	Administrative Requirements	Facility-Access-Controls-Policy.pdf::::1 Asset Management Policy and Procedure.pdf::::6	
Is there a process for access authorization?	Correct	Yes	('Access approvals and least-privilege enforcement'), ('j. Appropriate system managers and data owners must review and approve all requests for granting or modifying access to information assets.')	The first excerpt shows that access is granted only after formal approval enforcing least privilege, while the second mandates review and approval of all access requests by managers and data owners; together they evidence a defined access authorization process.	Safeguards for Protected Health Information	Asset Management Policy and Procedure.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there a procedure for access establishment and modification?	Correct	Yes	('d. Modifications to user access privileges must be tracked and logged.', 'g. Users experiencing a change in job responsibilities will have their logical access reviewed and modified, if necessary, to provide only the minimum necessary to perform their new job duties.', 'j. Appropriate system managers and data owners must review and approve all requests for granting or modifying access to information assets.'), ('a. Documented procedures for granting persons and entities authentication credentials or for changing an existing authentication method.'), ('6. Access Provisioning and Deprovisioning', 'Role assignments are documented and reviewed periodically.')	The cited passages describe documented procedures for granting new access, logging and approving changes, and periodically reviewing role assignments, showing that the organization has formal processes for both establishing and modifying access.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::1 Person-or-Entity-Authentication - done.pdf::::2 03- Access Control Policy â	
Is there a security reminder as part of the security awareness and training?	Correct	Yes	('4. The security awareness training for system administrators should include:', 'd. Security reminders for periodic security updates')	The cited passage explicitly lists security reminders as a component of the security awareness training programme, confirming that such reminders are provided.	Administrative Requirements	Security-Awareness-Training-Policy.pdf::::1	
Is there protection from malicious software?	Correct	Yes	('f. Ulalo will install anti-virus software on all workstations to prevent transmission of malicious software. This anti-virus software is regularly updated.'), ('ii. Remote access workstations must employ a virus detection and protection mechanism.'), ('Ulalo utilizes Microsoft native security services within Azure to provide antivirus and anti malware protections.')	The cited passages require anti-virus or anti-malware software on workstations and remote devices and attest that such protections are implemented and maintained, demonstrating effective protection against malicious software.	Administrative Requirements	Workstation-Security-Policy.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::6 16_Antivirus_and_Anti_Malware_Implementation_Attestation.pdf::::1	
Is log-in monitoring implemented?	Correct	Yes	('Log Review: The internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents).'), ('All user authentication and access activities are logged by unique user ID using Azure AD Sign-In Logs and Azure Activity Logs. Logs are retained and reviewed for security monitoring and HIPAA compliance.'), ('m. Mechanisms to log failed access attempts are in place. i. Ulalo will lock accounts after [3] failed login attempts. (Each organization must choose the number of failed login attempts based on its risk analysis.)')	The cited passages confirm that authentication events, including successful and failed log-ins, are logged, retained, and reviewed, demonstrating that log-in monitoring is in place.	Administrative Requirements	Information-System-Activity-Review-Policy.pdf::::1 01_Unique_User_ID_Policy.pdf::::1 Workstation-Security-Policy.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there a password management system?	Correct	Yes	('Must be a minimum of eight characters in length.', 'If a system does not support the minimum structure and complexity as detailed in the previous guidelines, the legacy system must be upgraded to support the requirements as soon as administratively possible.'), ('a. Documented procedures for granting persons and entities authentication credentials or for changing an existing authentication method.', 'f. Protection of authentication credentials (e.g., passwords, PINs) with appropriate controls to prevent unauthorized access.')	The cited passages lay out detailed password-complexity rules and describe documented procedures for issuing, protecting, and updating authentication credentials, confirming the existence of a formal password management system.	Administrative Requirements	Technical-Safeguards-Access-Control-Policy.pdf::::3 Person-or-Entity-Authentication - done.pdf::::2	
Is there a response and reporting procedure for a security incident?	Correct	Yes	('This document outlines the steps for identifying, containing, mitigating, and reporting incidents while ensuring timely corrective actions to minimize harm and ensure compliance.'), ('C. Media Notification (500+ individuals affected) If the breach affects 500 or more individuals in a specific jurisdiction, notify prominent media outlets within 60 days of the discovery.', '7. Mitigation and Remediation: Implement necessary measures to mitigate the breach\'s impact.', '9. Documentation: Maintain thorough documentation of the breach investigation, risk assessments, mitigation efforts, and all communications related to the breach.'), ('II. POLICIES AND PROCEDURES IN THE EVENT OF A POTENTIAL BREACH OF UNSECURED PHI', 'ii. If a potential breach is discovered, it is very time sensitive and must be immediately reported.', 'i. If you believe that a potential breach of PHI has occurred, you must immediately notify the Privacy Officer or designee.')	The cited passages describe structured procedures for detecting, investigating, containing, notifying, documenting, and remediating security incidents, demonstrating a comprehensive incident response and reporting process.	Complaints and Sanctions	HIPAA Security Incident Response Plan.pdf::::1 HIPAA Breach Response Plan.pdf::::3 Security-Privacy-Breach-Policy.pdf::::4	
Is there a data backup plan as part of the contingency plan?	Correct	Yes	('12. Backup Procedure 1. Identify systems and data requiring backup based on criticality. 2. Configure automated backups where feasible.'), ('3. Periodically verify backup integrity and restorability.'), ('6. All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved... Backups of original ePHI must be stored off-site in a physically secure facility.')	The cited passages mandate regular, tested backups, outline specific backup procedures, and require secure off-site storage, confirming that a data backup plan is an integral part of the contingency plan.	Administrative Requirements	Contingency And Disaster Recovery Policy.pdf::::2, ::::3 Media-Sanitization-and-Disposal-Policy.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there a disaster recovery plan?	Correct	Yes	('6. Disaster Recovery Plan Ulalo shall: - Maintain procedures to restore systems, applications, and data following a disaster - Prioritize restoration based on application and data criticality - Define recovery objectives (e.g., RPO/RTO) where appropriate - Assign roles and responsibilities for disaster recovery activities'), ('13. Disaster Recovery Procedure 1. Declare a disaster or major incident when recovery thresholds are met. 2. Activate disaster recovery roles and procedures. 3. Restore systems and data in priority order. 4. Validate system integrity and data accuracy post-recovery.'), ('The Business Associate has established an off-site disaster recovery location.')	The cited passages outline formal disaster-recovery procedures, roles, priorities, recovery objectives, and an off-site recovery location, confirming the organization maintains a documented disaster recovery plan.	Administrative Requirements	Contingency And Disaster Recovery Policy.pdf::::2, ::::3 Technical-Safeguards-Access-Control-Policy.pdf::::4	
Is there an emergency mode operation plan?	Correct	Yes	('7. Emergency Mode Operation Plan Ulalo shall: - Identify critical functions that must continue during emergency conditions - Define procedures for operating systems in a limited or degraded mode - Ensure safeguards remain in place to protect PHI during emergency operations'), ('14. Emergency Mode Operation Procedure n 1. Activate emergency operations when full functionality is unavailable. n 2. Limit system access to essential personnel. n 3. Maintain logging and security controls to the extent practicable.'), ('8) Emergency Access a. The HIPAA Security Rule requires Business Associates to establish procedures to allow access to ePHI during an emergency. During an emergency or disaster, Business Associates must remember that protecting ePHI is of utmost importance. Emergency procedures may be very different from standard operating procedures, but they are necessary because the normal methods for obtaining access may fail. Emergencies include, but are not limited to, the following: i. Natural disasters - Floods, earthquakes, tornadoes, tsunamis, hurricanes, etc. ii. Man-made disasters - Hacking attacks, thefts, vandalism, terrorist attacks, etc. iii. Unforeseen disasters - Power outages, internal failures, etc.'	The cited passages present a formal Emergency Mode Operation Plan with detailed activation steps, emergency access procedures, and protection of PHI, confirming that such a plan exists.	Administrative Requirements	Contingency And Disaster Recovery Policy.pdf::::2, ::::3 Technical-Safeguards-Access-Control-Policy.pdf::::3	
Is there a testing and revision procedure for the contingency plan?	Correct	Yes	('This policy satisfies the HIPAA Security Rule contingency planning requirements at 45 CFR §164.308(a)(7), including disaster recovery, data backup, emergency operations, and testing and revision procedures.'), ('8. Testing and Revision Procedures Ulalo shall: - Periodically test contingency and disaster recovery procedures (e.g., backup restore tests, tabletop exercises) - Document the results of testing activities - Revise contingency plans based on test results, incidents, system changes, or environmental changes'), ('15. Testing and Revision Procedure n 1. Conduct contingency testing activities on a periodic basis. n 2. Record test scope, outcomes, and identified gaps. n 3. Update plans, procedures, and documentation as needed. n 4. Track remediation actions to completion.')	The referenced sections require periodic testing of contingency procedures, documentation of results, and plan updates, demonstrating an established testing and revision process.	Administrative Requirements	Contingency And Disaster Recovery Policy.pdf::::1, ::::2, ::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there an applications and data criticality analysis?	Correct	Yes	('7. Application/System Criticality Levels Each application/system must receive a criticality level: Critical (Tier 1): Directly supports core service delivery or legal/regulatory obligations; outages or integrity failures cause severe customer impact, contractual breach, or patient privacy risk. Important (Tier 2): Significant operational impact; degradation affects customers or internal operations but can be tolerated briefly. Standard (Tier 3): Limited business impact; workarounds exist.'), ('13. Application and Data Criticality Analysis Procedure Criticality analysis is performed: . For all Tier 1 and Tier 2 systems . For any system handling PHI . At onboarding of major new applications . Upon major architecture/data flow changes . At least annually for all in-scope assets'), ('1. Owner completes a short impact assessment (CIA + business impact): O What happens if the system is down for 1 hour? 1 day? O What happens if PHI is disclosed? O What happens if data is altered? O Are there contractual SLAs? 2. Owner proposes Tier (1/2/3) and documents justification. The deliverable is a documented table/report ("Criticality Register") containing: Asset name Data classification Criticality tier CIA impact notes Required control set (backup	The policy mandates performing and documenting an Application and Data Criticality Analysis, assigns tiered criticality levels, and records results in a Criticality Register, fulfilling the requirement.	Administrative Requirements	Asset Management Policy and Procedure.pdf::::3, ::::5, ::::6	
Is there an ongoing evaluation of the security measures?	Correct	Yes	('The Information Security Officer will review on an on-going basis the viability of Ulalo Security Policies and general approaches taken by Departments in their Security Procedures.'), ('· Conduct regular HIPAA compliance audits and monitoring to ensure that PHI protection policies and breach response plans are effective and up to date.', '· Implement continuous monitoring systems to identify potential risks and vulnerabilities.'), ('4. The risk assessment and risk mitigation will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of Ulalo information security program: b. Throughout a System\'s Development Life Cycle ... ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.')	Policies require continuous monitoring, scheduled audits, and periodic risk assessments, showing that security safeguards are reviewed and improved on an ongoing basis.	Administrative Requirements	Evaluation-Policy.pdf::::1 HIPAA Breach Response Plan.pdf::::4 Risk-Management-Policy1.pdf::::6	
Is there a written contract or other arrangement with a business associate?	Correct	Yes	('Microsoft HIPAA Business Associate Agreement', 'If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data, FastTrack Data, or Professional Services Data, this HIPAA Business Associate Agreement ("BAA") is incorporated upon execution of an agreement ("Agreement") that incorporates the Microsoft Products and Services Data Protection Addendum.'), ('Vendors or Business Associates on a long-term contract (wearing a Visitor ID badge), once acclimated to the areas, without an escort.'), ('10. If destruction/disposal services are contracted, the contract must provide that the organization\'s business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in organization\'s HIPAA Business Associated Agreement/Contract). The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include but not be limited to the following:')	The cited passages include a HIPAA Business Associate Agreement incorporated into the customer contract and internal policies that require signed BAAs with vendors, showing documented written arrangements with business associates.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::1 Facility-Access-Controls-Policy.pdf::::1 Media-Sanitization-and-Disposal-Policy.pdf::::2	
Is there a contingency operation for facility access control?	Correct	Yes	('i. Critical personnel have been issued emergency response cards for access to the facilities in the event of an emergency or disaster.')	The cited passage states that critical personnel receive emergency response cards permitting facility entry during emergencies or disasters, constituting a contingency operation for facility access control.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there a facility security plan?	Correct	Yes	('Ulalo will maintain a Facility Security Plan that outlines and documents its procedures to safeguard all facilities, systems, and equipment used to store ePHI against unauthorized physical access, tampering, or theft.'), ('All Ulalo computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices, which alert the Technical Security Officer of any problems.')	The cited passages explicitly require Ulalo to keep a Facility Security Plan and describe concrete physical safeguards, confirming that such a plan exists.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1, ::::2	
Is there an access control and validation procedure for facility access?	Correct	Yes	('Ulalo will implement appropriate procedures to control and validate Ulalo employee access to all facilities used to house ePHI based systems.'), ('Access to these rooms is limited to authorized IT and facility services employees as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Technical Security Officer and only with an escort by an authorized IT or facility services workforce member.', 'In addition to badge access, Ulalo requires a signature log of all employees accessing server rooms and data center. Signature logs will be maintained for six years from the date of creation, or the date it was last in effect, whichever is later [§164.530(j)].'), ('Access levels are validated against job roles and supervisory approval')	The cited passages lay out procedures such as role-based approval, escort requirements, badge access, and signature logs, demonstrating a formal process to control and validate facility entry.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1, ::::2 06- Authorized Personnel Access Le.pdf::::2	
Are maintenance records kept for facility access control?	Correct	Yes	('Maintenance Records', 'ii. Document all decisions made and followed as required in this policy.'), ('After completion of the project, forward all documentation to the Security Manager.', 'The [Security Manager] maintains all documentation for a minimum of six years [§164.530(j)].')	The cited passages require that all facility-access repair and modification documentation be forwarded to the Security Manager and retained for at least six years, and they mandate documenting all maintenance decisions, confirming that maintenance records are kept.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::2, ::::3	
Is workstation use properly secured?	Correct	Yes	('5. Ulalo will institute appropriate procedures to maintain workstation security.', 'a. Workstations may only be accessed and utilized by authorized employees or Business Associates wearing appropriate identification to complete assigned job/contract responsibilities.'), ('Workstations should only be used for authorized business purposes.', 'Workstations in patient rooms or public areas must be logged off or locked when not in use.'), ('f. Ulalo will install anti-virus software on all workstations to prevent transmission of malicious software. This anti-virus software is regularly updated.'), ('a. Servers, workstations, or other computer systems located in open, common, or otherwise unsecure areas, that access, transmit, receive, or store ePHI, or that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms.')	The cited passages show that workstation access is restricted to authorised users, inactivity timers or auto-logoff are enforced in unsecure areas, and anti-virus protection is required and updated, demonstrating that workstation use is properly secured.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1 Workstation-Security-Policy.pdf::::1, ::::2 Technical-Safeguards-Access-Control-Policy.pdf::::5	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is workstation security maintained?	Correct	Yes	('5. Ulalo will institute appropriate procedures to maintain workstation security.', 'a. Workstations may only be accessed and utilized by authorized employees or Business Associates wearing appropriate identification to complete assigned job/ contract responsibilities.'), ('I, the undersigned, confirm that Ulalo SRL has implemented and maintains antivirus and anti malware protections to safeguard electronic Protected Health Information (ePHI).'), ('r. A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.'), ('g. Ulalo must establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their users to remotely access secure networks containing ePHI-based systems and applications continue to meet the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security.')	The passages confirm ongoing safeguards such as authorised-user controls, maintained anti-virus protection, scheduled patching, and documented procedures to ensure that local and remote workstations continuously meet security requirements, indicating workstation security is maintained.	Safeguards for Protected Health Information	Facility-Access-Controls-Policy.pdf::::1 16_Antivirus_and_Anti_Malware_Implementation_Attestation.pdf::::2 Workstation-Security-Policy.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::7	
Is there a disposal procedure for a device and media control?	Correct	Yes	('Ulalo requires that prior to disposal or reuse of hardware or media that contains or previously contained ePHI either the data will be securely overwritten or the device and/or media be physically destroyed and that such steps taken will be documented.'), ('a. Specify the method of destruction/disposal.', 'f. Provide proof of destruction/disposal (e.g. certificate of destruction).'), ('16. Decommissioning and Secure Disposal Procedure 1. Owner submits a decommission request including affected assets and data. 2. Data retention rules are confirmed (contractual/regulatory). 3. Data is securely deleted or archived according to retention policy. 4. Access is removed; credentials are rotated/revoked. 5. Inventory entry is updated to "Retired" with date and disposition.'), ('Workstations and electronic media are subject to authorization requirements prior to removal, inspection upon receipt, logging and tracking of asset movement, secure transport when applicable, and documentation of transfer, reuse, or disposal to ensure accountability	The cited passages lay out formal steps for secure destruction or overwriting of data, require specified disposal methods with proof of destruction, and describe a documented decommissioning process and lifecycle controls, demonstrating the existence of a device and media disposal procedure.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::1, ::::3 Asset Management Policy and Procedure.pdf::::6 Workstation-Security-Policy.pdf::::2	
Is there a media re-use policy?	Correct	Yes	('Ulalo requires that prior to disposal or reuse of hardware or media that contains or previously contained ePHI either the data will be securely overwritten or the device and/or media be physically destroyed and that such steps taken will be documented.'), ('Before reuse of any recordable and erasable media, all ePHI must be rendered inaccessible, cleaned, or scrubbed.', 'Any equipment or storage media that contains confidential, critical, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.'), ('Workstations and electronic media are subject to authorization requirements prior to removal, inspection upon receipt, logging and tracking of asset movement, secure transport when applicable, and documentation of transfer, reuse, or disposal to ensure accountability throughout the device and media lifecycle.')	The cited passages prescribe sanitizing or destroying media before it is reused and require authorization, tracking, and documentation of any reuse, demonstrating the existence of a formal media re-use policy.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::1, ::::2 Workstation-Security-Policy.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there an accountability measure for a device and media control?	Correct	Yes	('Ulalo requires that prior to disposal or reuse of hardware or media that contains or previously contained ePHI either the data will be securely overwritten or the device and/or media be physically destroyed and that such steps taken will be documented.'), ('Maintain a complete and accurate inventory of the Information Technology (IT) and Operational Technology (OT) assets in your organization to facilitate the implementation of optimal security controls.'), ('Every in-scope asset must have an assigned Owner. Owners are accountable for:', 'Coordinating decommissioning and secure disposal')	The cited passages require documentation of sanitization or destruction, mandate a maintained asset inventory, and assign named owners accountable for decommissioning and disposal, establishing clear accountability measures for devices and media.	Safeguards for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::1 SRA_Tool_3_6.pdf::::3 Asset Management Policy and Procedure.pdf::::2	
Is there a data backup and storage procedure for a device and media control?	Correct	Yes	('Ulalo shall: - Create and maintain retrievable, exact copies of critical data, including PHI - Perform backups at a frequency appropriate to data criticality - Protect backups using appropriate access controls and encryption - Store backups in locations resilient to primary system failures'), ('12. Backup Procedure 1. Identify systems and data requiring backup based on criticality. 2. Configure automated backups where feasible.'), ('All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved. This includes backup of portable devices such as laptops and PDA\'s, when storing original ePHI. Backups of original ePHI must be stored off-site in a physically secure facility.')	The cited passages define procedures for creating, protecting, testing, and off-site storing of backups as well as step-by-step backup workflows, confirming that formal data backup and storage procedures are in place for devices and media.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf::::1, ::::2 Media-Sanitization-and-Disposal-Policy.pdf::::2	
Is unique user identification used to control access?	Correct	Yes	('b. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.'), ('Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI, must be provided with a unique username.'), ('Ulalo assigns a unique user identifier to every individual accessing ePHI systems. Shared or generic user accounts are prohibited.')	The cited passages state that each user must authenticate with their own unique username and that shared or generic accounts are prohibited, demonstrating that unique user identification is enforced to control access.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::2 01_Unique_User_ID_Policy.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Is there an emergency access procedure?	Correct	Yes	('7. Emergency Mode Operation Plan Ulalo shall: - Identify critical functions that must continue during emergency conditions - Define procedures for operating systems in a limited or degraded mode - Ensure safeguards remain in place to protect PHI during emergency operations'), ('8) Emergency Access', 'a. The HIPAA Security Rule requires Business Associates to establish procedures to allow access to ePHI during an emergency.', 'b. To ensure that access to critical ePHI is maintained during an emergency situation, each Department must establish and implement procedures to ensure that access to a system that'), ('e. In the case of emergency, a computer account may be temporarily shared with another individual. The requirements for emergency access sharing are: i. There must be a true emergency. ii. The sharing must be temporary. iii. The emergency incident must be reported to the managing authority of the computer account being shared. iv. In no case should this emergency access sharing exceed 30 days. v. The Emergency access procedure must be used in case a terminated employee\'s computer account must be maintained for business reasons.'	The cited passage(s) describe an Emergency Mode Operation Plan and dedicated "Emergency Access" provisions that outline how systems and accounts are accessed or shared during emergencies, demonstrating that a formal emergency access procedure exists.	Safeguards for Protected Health Information	Contingency And Disaster Recovery Policy.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::3, ::::4	
Is automatic logoff enabled for a technical safeguard?	Correct	Yes	('This Policy pertains to the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to electronic information systems that maintain ePHI.'), ('a. Servers, workstations, or other computer systems located in open, common, or otherwise unsecure areas, that access, transmit, receive, or store ePHI, or that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms. These systems must terminate a user session after a maximum of 15 minutes of inactivity.', 'b. Applications and databases using ePHI, such as electronic claims records, must employ inactivity timers or automatic session logoff mechanisms. These application sessions must automatically terminate after a maximum of 30 minutes of inactivity.'), ('Information systems should automatically log users off the systems after [30] minutes of inactivity.')	The cited passage(s) mandate inactivity timers or session termination after defined periods of idle time for systems and applications handling ePHI, confirming that automatic log-off is an enforced technical safeguard.	Safeguards for Protected Health Information	Technical-Safeguards-Access-Control-Policy.pdf::::1, ::::5 Workstation-Security-Policy.pdf::::1	
Is encryption actually implemented to protect electronic protected health information?	Correct	Yes	('Ulalo encrypts all systems storing ePHI using Microsoft Azure native encryption mechanisms.', 'Ulalo encrypts ePHI during transmission across internal and external networks. Records demonstrate that application endpoints use HTTPS with TLS encryption.'), ('Data at Rest · Azure Storage Service Encryption (AES-256) Azure SQL Transparent Data Encryption (TDE) Microsoft-managed encryption keys', ' . Encryption is enforced for data at rest and in transit'), ('Azure Cosmos DB encryption protects your data at rest. You can add a second layer of encryption by using Customer Managed Keys. Azure Cosmos DB encrypts your databases as it\'s written in our datacenters, and automatically decrypts it for you as you access it.')	The cited passage(s) confirm that ePHI is protected with Azure-native encryption at rest (AES-256, TDE, Cosmos DB) and in transit via HTTPS/TLS, evidencing that encryption controls are actively implemented.	Safeguards for Protected Health Information	07_Encrypted_Data_Storage_and_Transmission_Records.pdf::::1 02- Azure - HIPAA Proof of Implementation.pdf::::3 15_Policy_Distribution_and_Workforce_Acknowledgement_Attestation.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Are audit controls actually implemented to maintain electronic protected health information?	Correct	Yes	('These tools support HIPAA Security Rule requirements including 45 CFR §164.312(b) (Audit Controls), 45 CFR §164.308(a)(1) (Security Management Process), and 45 CFR §164.312(a)(1) (Access Control).', 'I, the undersigned, confirm that Ulalo SRL has implemented and maintains auditing and monitoring tools to log, review, and monitor access and activity related to electronic Protected Health Information (ePHI).'), ('These systems provide authoritative, tamper-resistant audit logs.', 'The following authentication events are automatically logged:', '· Successful user sign-ins', '· Failed login attempts (invalid credentials, MFA failure, blocked sign-ins)', 'Each log entry includes, at minimum:', '· User identifier (Azure AD account)', '· Date and timestamp', '· Source IP address / location', '· Authentication result (success or failure)', '· Application or resource accessed'), ('Audit Logging & Monitoring · Azure Monitor and Log Analytics', '· Centralized logging of security-relevant events'	The cited passage(s) attest that centralized, tamper-resistant logging via Azure Monitor/Log Analytics records detailed authentication and access events and that these logs are maintained and reviewed in line with HIPAA §164.312(b), demonstrating implemented audit controls for ePHI.	Safeguards for Protected Health Information	11_Auditing_and_Monitoring_Tools_Records.pdf::::2 10- System Login & Authentication Logs – HIPAA.pdf::::2 02- Azure - HIPAA Proof of Implementation.pdf::::3	
Is there an actual mechanism in place to authenticate electronic protected health information?	Correct	Yes	('f. A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting ePHI.'), ('The following authentication events are automatically logged:', '· Successful user sign-ins', '· Failed login attempts (invalid credentials, MFA failure, blocked sign-ins)'), ('I, the undersigned, confirm that Ulalo SRL has implemented and maintains system configurations that enforce authentication mechanisms for access to electronic Protected Health Information (ePHI). These configurations are actively managed, monitored, and reviewed as part of Ulalo\'s HIPAA compliance program.')	The cited passages show policy-level requirements to verify recipient identity, active logging of authentication events, and an attestation that system configurations enforcing authentication are maintained, demonstrating an operational mechanism for authenticating ePHI.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::2 10- System Login & Authentication Logs – HIPAA.pdf::::2 14_Authentication_Mechanisms_System_Configuration_Attestation.pdf::::2	
Is person or entity authentication actually used to ensure the security of electronic protected health information?	Correct	Yes	('The Person or Entity Authentication Standard of the Rule requires covered entities to implement policies and procedures to validate user or entity identification prior to permitting access to ePHI to those individuals or groups authorized, thereby increasing the security of ePHI.', 'Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.'), ('c. All user-level access shall be secured through usernames and passwords.', 'a. Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI, must be provided with a unique username.'), ('Identity & Access Management', '· Azure Active Directory (Entra ID)', 'Multi-Factor Authentication (MFA) enforced for privileged accounts', 'Role-Based Access Control (RBAC)')	The cited passages mandate unique IDs, passwords, biometrics or smart-cards before ePHI access and show enforcement through Azure AD with MFA and RBAC, confirming that person or entity authentication is actively used to secure ePHI.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::2 02- Azure - HIPAA Proof of Implementation.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Are integrity controls actually implemented to protect the transmission of electronic protected health information?	Correct	Yes	('4. Ulalo implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to: a. Ensure the confidentiality, integrity, and availability of all PHI the organization creates, receives, maintains, and/or transmits.'), ('. Encryption of all data at rest and in transit')	The cited passages state that Ulalo applies security measures to ensure the integrity of PHI during transmission and enforces encryption for all data in transit, demonstrating implementation of integrity controls.	Safeguards for Protected Health Information	Risk-Management-Policy1.pdf::::2 02- Azure - HIPAA Proof of Implementation.pdf::::1	
Is encryption actually used to secure the transmission of electronic protected health information?	Correct	Yes	('Restricted (highest): PHI, high-risk PII, credentials/ secrets, encryption keys, regulated customer data.', 'Restricted: strong access controls (least privilege), encryption in transit and at rest, logging/monitoring, approved storage locations, strict retention, incident escalation.'), ('Ulalo encrypts ePHI during transmission across internal and external networks.', 'Records demonstrate that application endpoints use HTTPS with TLS encryption.', 'Encryption in transit is enforced through Azure-native networking and application services.'), ('b. Authentication and encryption mechanisms are required for all remote access sessions to networks containing ePHI via an ISP (Internet Service Provider) or dial-up connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.', 'e. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.')	The cited passages classify PHI as requiring encryption in transit, attest that ePHI is transmitted over HTTPS/TLS, and mandate VPN or SSL encryption for remote sessions, confirming that encryption is actively used to secure ePHI transmission.	Safeguards for Protected Health Information	Asset Management Policy and Procedure.pdf::::3 07_Encrypted_Data_Storage_and_Transmission_Records.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::6	
Upon discovery of a breach of unsecured protected health information, does the business associate notify the covered entity?	Correct	Yes	('F. Step 6 - NOTIFICATION TO COVERED ENTITY [Only applies to Business Associates] - In the event that the Privacy Officer or designee determines that notice to the Covered Entity is warranted, the Privacy Officer or designee shall promptly prepare and transmit a CE Notice.'), ('Ulalo shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery of the breach.'), ('Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Microsoft becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer\'s Unsecured Protected Health Information that Microsoft may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule).', 'Notification of a Breach will be made without unreasonable delay, but in no event more than seventy-two (72) hours after Microsoft\'s discovery of a Breach.')	The cited passages direct the Privacy Officer to promptly send notice to the covered entity and require business associates such as Ulalo and Microsoft to report any breach of unsecured PHI without unreasonable delay, confirming that notification to the covered entity is mandatory.	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::5, ::::6 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Is a breach considered discovered by the business associate when it is known, or by exercising reasonable diligence would have been known, to any person other than the person committing the breach?	Correct	Yes	('A breach of PHI will be deemed "discovered" as of the first day Ulalo knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.')	The cited passage defines discovery as the date the business associate actually knows of the breach or would have known through reasonable diligence, matching the required definition.	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate provide the notification of a breach without unreasonable delay and in no case later than 60 calendar days after discovery?	Correct	Yes	('Timeline: Notify affected individuals without unreasonable delay and within 60 days of discovering the breach.'), ('Small Breaches (<500 individuals affected): Notify affected individuals within 60 days of discovering the breach.'), ('Ulalo shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery of the breach.'), ('Notification of a Breach will be made without unreasonable delay, but in no event more than seventy-two (72) hours after Microsoft\'s discovery of a Breach.')	The cited passages consistently stipulate that notification must occur without unreasonable delay and not later than 60 days after discovery (with some contracts requiring even faster notice), satisfying the regulatory timeline.	Business Associate Contracts	HIPAA Breach Response Plan.pdf::::2 HIPAA Security Incident Response Plan.pdf::::4 Security-Privacy-Breach-Policy.pdf::::6 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Does the notification by the business associate include the identification of each individual whose unsecured protected health information has been compromised during the breach?	Correct	Yes	('1. Identification of each individual whose Unsecured PHI is believed to have been breached, the date of the disclosure, the facts and circumstances surrounding the disclosure, and all associated documentation.')	The cited passage requires the breach notice to list every individual whose unsecured PHI was affected, confirming that the notification includes this identification.	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::6	
Does the business associate provide the covered entity with any other available information required for notification to the individual under § 164.404 (c) (Section - Implementation specifications) at the time of the notification or promptly thereafter as information becomes available?	Correct	Yes	('2. The CE Notice shall include all other available information known to Ulalo that the Covered Entity will be required to include in its own Notice to the individual(s).', '3. If additional information regarding the breach is later discovered by Ulalo, that information will be promptly provided to the Covered Entity.')	The cited passage specifies that Ulalo must supply all information the Covered Entity needs for the individual notice and must promptly furnish any additional facts discovered later, satisfying §164.404(c).	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::6	
If a law enforcement official states that a notification would impede a criminal investigation or cause damage to national security, does the covered entity or business associate delay the notification as specified by the official?	Correct	Yes	('2. Law Enforcement Delay - A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security.', 'a. In that event, the law enforcement statement must be in writing and must specify the length of the delay required.', 'b. If the request for a delay in notification is oral, Ulalo must document the statement and request written confirmation within 30 days. If no written request for a delay is received within that time, Ulalo must send notification of the breach to the Covered Entity.')	The cited passage allows notification to be postponed upon a written (or documented oral) request from law-enforcement specifying the delay period, demonstrating compliance with the HIPAA rule.	Use and Disclosure of Protected Health Information	Security-Privacy-Breach-Policy.pdf::::6	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does a business associate use or disclose protected health information only as permitted by its business associate contract?	Correct	Yes	('Microsoft shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. Microsoft shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA.'), ('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.'), ('Ulalo shall not independently notify individuals or external parties unless contractually required to do so by the Covered Entity.'), ('If destruction/disposal services are contracted, the contract must provide that the organization\'s business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in organization\'s HIPAA Business Associated	The cited passages from the BAAs and related policies repeatedly state that Microsoft and Ulalo may use or disclose PHI only as expressly allowed by the business-associate agreement (or as required by law) and must employ safeguards to prevent any other use.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::2, ::::3 Amendment of Protected Health Information.pdf::::3 Media-Sanitization-and-Disposal-Policy.pdf::::2	
Does the Business Associate make protected health information available to the Secretary of the U.S. Department of Health and Human Services upon request to investigate or determine compliance?	Correct	Yes	('(v) Disclosure to the Secretary. Microsoft shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer\'s compliance with HIPAA, subject to attorney-client and other applicable legal privileges.'), ('13. Uses and disclosures for health oversight activities n a. A health oversight agency is an agency of the United States, a state, a political subdivision of a n state, a Native American Tribe, or any person, contractor, or entity acting on its behalf.', 'b. Ulalo may use and disclose PROTECTED HEALTH INFORMATION without authorization to a n health oversight agency for its oversight activities including: n viii. Determinations of regulatory compliance'), ('1. The Company will make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the HIPAA Privacy Rule.', '2. The Company may disclose protected health	The cited passages obligate the business associate to provide PHI and related records to the Secretary of HHS (or other health-oversight agencies) for compliance investigations, thus meeting the HIPAA requirement.	Complaints and Sanctions	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Uses-and-Disclosures-of-PHI.pdf::::5, ::::8	
When using or disclosing protected health information, does a business associate make reasonable efforts to limit it to the minimum necessary standard?	Correct	Yes	('In addition, whenever a person or entity is authorized to access such information, only the minimum necessary to perform their designated function is to be authorized for access.'), ('Ulalo will only disclose the minimum amount of PROTECTED HEALTH INFORMATION necessary to accomplish the intended purpose of the use or disclosure.', 'Ulalo will identify persons in the workforce and other persons (medical staff, business associates) who require access to PROTECTED HEALTH INFORMATION to carry out their specific duties and will take reasonable steps to limit access to PROTECTED HEALTH INFORMATION for those individuals or categories of individuals in carrying out their duties.'), ('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.')	The cited passages require personnel and external partners to access, use, or disclose only the minimum amount of PHI needed for the stated purpose, illustrating that the business associate applies the HIPAA minimum-necessary standard.	Safeguards for Protected Health Information	Person-or-Entity-Authentication - done.pdf::::1 Uses-and-Disclosures-of-PHI.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate have a policy to appropriately safeguard the protected health information a covered entity discloses to it?	Correct	Yes	('Ulalo has adopted this policy to ensure that its Security and Privacy Policies are up to date and effective in ensuring the confidentiality, integrity and availability of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) created, received, maintained and transmitted by Ulalo.'), ('Scope: The policy covers the administrative, physical, and technical processes that enable and govern PHI that is created, maintained, received, or transmitted by Ulalo.'), ('This Policy pertains to the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to electronic information systems that maintain ePHI.')	The referenced policies set administrative, physical and technical safeguards and explicitly commit to protecting the confidentiality, integrity and availability of PHI and ePHI, demonstrating that the business associate maintains formal policies to safeguard disclosed information.	Safeguards for Protected Health Information	Evaluation-Policy.pdf::::1 Risk-Management-Policy1.pdf::::1 Technical-Safeguards-Access-Control-Policy.pdf::::1	
Does a business associate provide assurance of appropriate safeguarding to a covered entity for disclosed protected health information?	Correct	Yes	('The governing statutes encourage Covered Entities that contract with Business Associates to request a copy of the Business Associate\'s HIPAA Privacy and Security Policy; therefore these policies may be distributed externally by the Privacy Officer to Ulalo clients, as needed.'), ('I, the undersigned, confirm that Ulalo SRL has implemented and maintains the technical security controls described in this document within its Microsoft Azure cloud environment.', 'These controls are actively managed, monitored, and reviewed in alignment with HIPAA Security Rule requirements (45 CFR §164.308, §164.312).'), ('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.')	The policy allows delivery of HIPAA security documentation to clients, signed attestations confirm active safeguards, and the BAA contractually obliges reasonable safeguards, collectively providing explicit assurance to the covered entity.	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::2 02- Azure - HIPAA Proof of Implementation.pdf::::3 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Does a business associate disclose protected health information to a subcontractor with the assurance of appropriate safeguarding?	Correct	Yes	('provided that any Disclosure may occur only if: (1) Required by Law; or (2) Microsoft obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Microsoft of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.'), ('(iv) Subcontractors. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.'), ('If PHI is involved, confirm required agreements and security requirements are met.')	The BAA mandates written assurances and Security-Rule compliance from any subcontractor before PHI is shared, and internal procedures require verifying agreements and security requirements whenever PHI is involved, demonstrating that disclosures to subcontractors occur only with confirmed safeguards.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::2, ::::3 Asset Management Policy and Procedure.pdf::::7	
Has a business associate taken reasonable steps to cure a breach or end a violation upon becoming aware of a pattern of activity or practice of a subcontractor that constituted a material breach or violation?	Correct	Yes	('I. SUBCONTRACTOR BREACH - Ulalo takes reasonable steps to cure a breach or end a violation upon becoming aware of a pattern of activity or practice of a subcontractor that constituted a material breach or violation.')	The cited passage states that Ulalo, acting as the business associate, will take reasonable steps to cure or stop a subcontractor's material breach once it is discovered, satisfying the requirement.	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::6	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does a contract between a covered entity and a business associate establish the permitted and required uses and disclosures of protected health information by the business associate?	Correct	Yes	('2. Permitted Uses and Disclosures of Protected Health Information.', 'Except as otherwise limited in this BAA, Microsoft may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Agreement; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted under paragraph b of this Section or as listed as an exception to the DPA in the Privacy and Security Terms section of the Product Terms.'), ('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.'), ('with the Section titled "Disclosure of Processed Data" within the Microsoft Products and Services Data Protection Addendum.', '(i) No Impermissible Requests. Customer shall not request Microsoft to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).'),	The cited BAA clauses and supporting policy language explicitly list and limit how the business associate may use or disclose PHI, demonstrating that the contract sets permitted and required uses and disclosures in line with HIPAA.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::2, ::::3, ::::4 Media-Sanitization-and-Disposal-Policy.pdf::::2	
Is a business associate currently using or disclosing protected health information for the proper management and administration of the business associate?	Correct	Yes	('Management, Administration, and Legal Responsibilities. Except as otherwise limited in this BAA, Microsoft may Use and Disclose Protected Health Information for the proper management and administration of Microsoft and/or to carry out the legal responsibilities of Microsoft, provided that any Disclosure may occur only if: (1) Required by Law; or (2) Microsoft obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Microsoft of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.'), ('No authorization is necessary for uses and disclosures of PROTECTED HEALTH INFORMATION for the patient\'s treatment, for payment of the patient\'s treatment or for Ulalo\'s health care operations.', '14. Business planning, business development, cost planning and management-related analysis of the entity\'s operations', '17. Business management', '18. General administrative activities')	The Business Associate Agreements for both Microsoft and Ulalo authorize the use and disclosure of PHI for business management, planning, and general administrative functions, confirming that such activity is permitted for proper management and administration.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::2 Uses-and-Disclosures-of-PHI.pdf::::2	
Does the business associate report to a covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware?	Correct	Yes	('F. Step 6 - NOTIFICATION TO COVERED ENTITY [Only applies to Business Associates] - In the event that the Privacy Officer or designee determines that notice to the Covered Entity is warranted, the Privacy Officer or designee shall promptly prepare and transmit a CE Notice.'), ('If additional information regarding the breach is later discovered by Ulalo, that information will be promptly provided to the Covered Entity.', 'Ulalo shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery of the breach.'), ('(iii) Reporting. Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Microsoft becomes aware; (2) any Security Incident of which it becomes aware ... Notification of a Breach will be made without unreasonable delay, but in no event more than seventy-two (72) hours after Microsoft\'s discovery of a Breach.')	The cited policy and BAA provisions oblige the business associate to notify the covered entity promptly of any impermissible use, disclosure, or breach of PHI, showing compliance with the reporting requirement.	Business Associate Contracts	Security-Privacy-Breach-Policy.pdf::::5, ::::6 Microsoft General - HIPAA BAA (May 2025).pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the business associate ensured that any subcontractor agrees to the same restrictions and conditions that apply to the business associate with respect to protected health information?	Correct	Yes	('10. If destruction/disposal services are contracted, the contract must provide that the organization\'s business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in organization\'s HIPAA Business Associated Agreement/Contract). The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include but not be limited to the following:'), ('(iv) Subcontractors. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. Microsoft remains responsible for its Subcontractors\' compliance with obligations in this BAA.')	The cited passages state that contracts or BAAs must obligate subcontractors to follow the same—or stricter—use, disclosure, and safeguarding requirements for PHI that bind the business associate, satisfying the requirement.	Business Associate Contracts	Media-Sanitization-and-Disposal-Policy.pdf::::2 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Does the business associate currently make available protected health information for amendment in accordance with the section 'Amendment of protected health information'?	Correct	Yes	('This policy and procedure establishes how Ulalo, acting in its role as a Business Associate, complies with the HIPAA Privacy Rule requirements at 45 CFR §164.526, including subsection §164.526(e), regarding the amendment of Protected Health Information (PHI).', 'The purpose of this document is to ensure that approved amendments to PHI are properly incorporated into designated record sets, clearly associated with the original information, and appropriately communicated to relevant parties, in accordance with HIPAA and contractual obligations to Covered Entities.'), ('(vii) Amendment. Subject to Section 3a(vi) above, if Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall within fifteen (15) days make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.'), ('D. Access and Amendment to a Patient\'s Own PHI - HIPAA requires that patients be afforded the opportunity to access certain PHI within a Designated Record Set and to amend or correct their own PHI	The cited passages describe documented procedures and contractual clauses that oblige the business associate to make PHI available for, and incorporate, requested amendments in line with 45 CFR § 164.526.	Amendments and Accountings of Disclosures	Amendment of Protected Health Information.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::4 Security-Privacy-Breach-Policy.pdf::::4	
Is the business associate complying with the requirements of this Privacy subpart that apply to a covered entity when carrying out the covered entity's obligation under this subpart?	Correct	Yes	('This policy and procedure establishes how Ulalo, acting in its role as a Business Associate, complies with the HIPAA Privacy Rule requirements at 45 CFR §164.526, including subsection §164.526(e), regarding the amendment of Protected Health Information (PHI).'), ('7. Incorporation of Amendments (§164.526(e)(1))', '8. Notification of Amendments (§164.526(e)(2))'), ('(ix) Performance of a Covered Entity\'s Obligations. To the extent Microsoft is to carry out a Covered Entity obligation under the Privacy Rule, Microsoft shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.')	The passages confirm that, when performing obligations on a covered entity's behalf, the business associate commits to follow all Privacy Rule provisions that would apply to the covered entity itself.	Business Associate Contracts	Amendment of Protected Health Information.pdf::::1, ::::2 Microsoft General - HIPAA BAA (May 2025).pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate actually make its internal practices, books, and records available to the Secretary for purposes of determining the covered entity's compliance with the Privacy subpart?	Correct	Yes	('The Company will make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the HIPAA Privacy Rule.'), ('Microsoft shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer\'s compliance with HIPAA, subject to attorney-client and other applicable legal privileges.')	Both cited clauses explicitly state that the business associate will provide its relevant books, records, and practices to the HHS Secretary for Privacy Rule compliance reviews.	Documentation and Record Retention	Uses-and-Disclosures-of-PHI.pdf::::8 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Does the business associate actually return or destroy all protected health information received from the covered entity upon termination of the contract, if feasible?	Correct	Yes	('Upon expiration or termination of this BAA, Microsoft shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement.')	The cited passage states that upon contract termination Microsoft must return or destroy all PHI when feasible, satisfying the requirement.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::5	
Does the business associate actually extend the protections of the contract to the information and limit further uses and disclosures when return or destruction of protected health information is not feasible?	Correct	Yes	('If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, then Microsoft shall extend the protections of this BAA, without limitation, to such Protected Health Information and limit any further Use or Disclosure of the Protected Health Information to those purposes that make the return or destruction infeasible for the duration of the retention of the Protected Health Information.')	The quoted clause requires Microsoft to keep BAA protections in force and restrict further use/disclosure whenever return or destruction of PHI is infeasible.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::5	
Is the covered entity actually authorized to terminate the contract if the business associate violates a material term of the contract?	Correct	Yes	('3. If it is determined that a business associate has violated the terms of the business associate agreement, Ulalo must take immediate action to rectify the situation. Continued violations may result in discontinuation of the business relationship.'), ('Violation of this policy and procedures by others, including providers, providers\' offices, business associates and partners may result in termination of the relationship and/or associated privileges.'), ('Upon written notice, either Party immediately may terminate the Agreement and this BAA if the other Party is in material breach or default of any obligation in this BAA.')	The cited passages from both the policy and the BAA give the covered entity (and either party) the right to end the relationship when the business associate materially breaches the agreement.	Business Associate Contracts	Information-System-Activity-Review-Policy.pdf::::4, ::::5 Microsoft General - HIPAA BAA (May 2025).pdf::::5	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate actually obtain reasonable assurances from the person to whom the information is disclosed that it will be used or disclosed only as required by law or for the purposes for which it was disclosed?	Correct	Yes	('(2) Microsoft obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Microsoft of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.'), ('In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.')	Both quoted BAA clauses require Microsoft to secure written assurances from recipients and subcontractors that PHI will only be used or disclosed as permitted, thus meeting the criterion.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::2, ::::3	
Does the person to whom the protected health information is disclosed notify the business associate of any breaches in confidentiality?	Correct	Yes	('provided that any Disclosure may occur only if: (1) Required by Law; or (2) Microsoft obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Microsoft of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.')	The cited passage states that the recipient of the PHI must notify Microsoft whenever it becomes aware of a breach of confidentiality, fulfilling the requirement.	Business Associate Contracts	Microsoft General - HIPAA BAA (May 2025).pdf::::2	
Does the business associate implement technical, physical, and administrative safeguards for protecting the privacy of protected health information?	Correct	Yes	('Any media containing ePHI should be destroyed/ disposed of using a method that ensures the ePHI cannot be recovered.', 'All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved.'), ('ii. Limit network access to only legitimate or established connections.', 'v. Must be located in a physically secure environment.', 'd. The configuration of firewalls used to protect networks containing ePHI-based systems and applications must be submitted to and approved by the Information Security Officer.'), ('(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent Use and Disclosure of Protected Health Information other than as permitted in Section 2 herein; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.')	The passages show policies requiring technical measures (e.g., encryption, firewalls, network restrictions), physical controls (secure environments, destruction of media), and administrative controls (documentation, approvals, compliance with 45 CFR 164), demonstrating implementation of all three safeguard categories.	Privacy Practices for Protected Health Information	Media-Sanitization-and-Disposal-Policy.pdf::::2 Technical-Safeguards-Access-Control-Policy.pdf::::6 Microsoft General - HIPAA BAA (May 2025).pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the business associate identified the person or class of person in its workforce who needs access to protected health information to carry out their duty?	Correct	Yes	('a. Conduct thorough background checks and vetting processes for all workforce members who will have access to ePHI.'), ('Ulalo will identify persons in the workforce and other persons (medical staff, business associates) who require access to PROTECTED HEALTH INFORMATION to carry out their specific duties and will take reasonable steps to limit access to PROTECTED HEALTH INFORMATION for those individuals or categories of individuals in carrying out their duties.'), ('Ulalo maintains an up-to-date list of all personnel authorized to access systems that store, process, or transmit ePHI.')	The cited passages require Ulalo to determine which workforce members or classes (e.g., authorized employees, medical staff) need ePHI access and to keep current lists of those authorized, confirming that the identification is performed.	Administrative Requirements	Technical-Safeguards-Access-Control-Policy.pdf::::8 Uses-and-Disclosures-of-PHI.pdf::::1 05- Authorized Personnel & Supervisors.pdf::::1	
Does the business associate make reasonable efforts to limit access to protected health information to the person or class identified as needing it for their duty?	Correct	Yes	('Access approvals and least-privilege enforcement'), ('Ulalo will identify persons in the workforce and other persons (medical staff, business associates) who require access to PROTECTED HEALTH INFORMATION to carry out their specific duties and will take reasonable steps to limit access to PROTECTED HEALTH INFORMATION for those individuals or categories of individuals in carrying out their duties.'), ('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.')	Policies enforce least-privilege and minimum-necessary principles, require managerial approval and periodic review, and direct Microsoft to use only the minimum PHI needed, demonstrating that access is reasonably limited to identified roles.	Administrative Requirements	Asset Management Policy and Procedure.pdf::::2 Uses-and-Disclosures-of-PHI.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Does the business associate actually implement policies and procedures that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure?	Correct	Yes	('Ulalo will only disclose the minimum amount of PROTECTED HEALTH INFORMATION necessary to accomplish the intended purpose of the use or disclosure.', 'Ulalo will develop criteria designed to limit the PROTECTED HEALTH INFORMATION disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.'), ('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.'), ('B. Employees Shall Abide by the HIPAA "Minimum Necessary" Standard - It is the policy of Ulalo that all employees abide by the HIPAA Minimum Necessary Standard, i.e. that the amount and type of PHI requested, accessed, used and/or disclosed shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request.')	The cited passages require staff and vendors to apply the HIPAA minimum-necessary principle and explicitly direct that only the least amount of PHI needed for the stated purpose may be disclosed, demonstrating implemented policies and procedures that enforce this limit.	Administrative Requirements	Uses-and-Disclosures-of-PHI.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::3 Security-Privacy-Breach-Policy.pdf::::3	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the business associate actually developed criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought?	Correct	Yes	('Ulalo will develop criteria designed to limit the PROTECTED HEALTH INFORMATION disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.'), ('b. Ulalo may only disclose i. Name and address ii. Date and place of birth iii. Social security number iv. Blood type v. Type of injury vi. Date and time of treatment vii. Date and time of death viii. Description of distinguishing characteristics.'), ('In addition, whenever a person or entity is authorized to access such information, only the minimum necessary to perform their designated function is to be authorized for access.')	The cited passages show that the associate has established concrete criteria—both general rules and specific data-element lists—that limit any PHI disclosure to what is reasonably needed for the stated purpose.	Administrative Requirements	Uses-and-Disclosures-of-PHI.pdf::::1, ::::7 Person-or-Entity-Authentication - done.pdf::::1	
Does the business associate review requests for disclosure on an individual basis in accordance with the criteria to limit the protected health information disclosed, to the information reasonably necessary to accomplish the purpose?	Correct	Yes	('Ulalo will independently determine the necessary minimum disclosure and will verify that only the minimum necessary information is used or disclosed.')	The cited passage states that each disclosure is independently reviewed and verified to ensure only the minimum necessary PHI is released, confirming individual-request review against the established criteria.	Administrative Requirements	Uses-and-Disclosures-of-PHI.pdf::::1	
Does the business associate rely on the minimum necessary information requested by a professional providing professional services to the business associate?	Correct	Yes	('B. Employees Shall Abide by the HIPAA "Minimum Necessary" Standard - It is the policy of Ulalo that all employees abide by the HIPAA Minimum Necessary Standard, i.e. that the amount and type of PHI requested, accessed, used and/or disclosed shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request.', 'Use and disclosure to other authorized Ulalo employees, plan administrators, authorized representatives of the Covered Entity, brokers and/or other business associates will be made in accordance with the Minimum Necessary Standard.')	The Security-Privacy-Breach policy states that disclosures to other business associates and authorized parties must observe the HIPAA Minimum Necessary Standard, showing reliance on professionals' minimum-necessary requests.	Use and Disclosure of Protected Health Information	Security-Privacy-Breach-Policy.pdf::::3	
Does the business associate limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made?	Correct	Yes	('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.'), ('Disclosures must be limited to information directly related to the individual\'s involvement in the patient\'s care.'), ('1. Access to information systems by all users is allowable only on a minimum necessary basis.')	The Business Associate Agreement and internal policies require that any PHI request or disclosure be confined to the minimum information necessary for the stated purpose, demonstrating that requests are limited accordingly.	Administrative Requirements	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Uses-and-Disclosures-of-PHI.pdf::::3 Workstation-Security-Policy.pdf::::1	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate actually implement policies and procedures that limit the protected health information requested to the amount reasonably necessary for routine and recurring requests?	Correct	Yes	('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.'), ('Employees Shall Abide by the HIPAA "Minimum Necessary" Standard - It is the policy of Ulalo that all employees abide by the HIPAA Minimum Necessary Standard, i.e. that the amount and type of PHI requested, accessed, used and/or disclosed shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request.')	The cited passages show both Microsoft and Ulalo policies expressly require all PHI uses, disclosures, or requests to be limited to the minimum necessary data, confirming that procedures are in place for routine and recurring requests.	Administrative Requirements	Microsoft General - HIPAA BAA (May 2025).pdf::::3 Security-Privacy-Breach-Policy.pdf::::3	
Has the business associate actually developed criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made?	Correct	Yes	('In addition, whenever a person or entity is authorized to access such information, only the minimum necessary to perform their designated function is to be authorized for access.'), ('Ulalo will develop criteria designed to limit the PROTECTED HEALTH INFORMATION disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.'), ('Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.')	The cited passages establish explicit criteria—across multiple policies and the BAA—that any request or access to PHI must be restricted to the minimum information needed for the stated purpose.	Administrative Requirements	Person-or-Entity-Authentication - done.pdf::::1 Uses-and-Disclosures-of-PHI.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::3	
Does the business associate review requests for protected health information on an individual basis in accordance with the criteria to limit the protected health information disclosed, to the information reasonably necessary to accomplish the purpose?	Correct	Yes	('Ulalo will independently determine the necessary minimum disclosure and will verify that only the minimum necessary information is used or disclosed.')	The cited procedure states that each request is independently assessed to verify that only the minimum necessary PHI is used or disclosed, evidencing an individual-basis review against the established criteria.	Administrative Requirements	Uses-and-Disclosures-of-PHI.pdf::::1	
Does a business associate amend protected health information in designated record sets when informed of an amendment by a covered entity?	Correct	Yes	('(vii) Amendment. Subject to Section 3a(vi) above, if Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall within fifteen (15) days make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.'), ('Ulalo shall amend PHI only at the direction of a Covered Entity or as otherwise required by applicable law.')	Both the Microsoft BAA and Ulalo's amendment policy obligate the business associate to incorporate amendments to PHI in the designated record set whenever directed by the covered entity, satisfying HIPAA §164.526 requirements.	Amendments and Accountings of Disclosures	Microsoft General - HIPAA BAA (May 2025).pdf::::4 Amendment of Protected Health Information.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Do the contracts ensure business associates will make its accounting of disclosures available.	Correct	Yes	('(viii) Accounting of Disclosure. Microsoft, at the request of Customer, shall within thirty (30) days make available to Customer such information relating to Disclosures made by Microsoft as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.')	The cited passage obligates the business associate to make the information on its disclosures available to the customer within thirty days so the customer can prepare an accounting under 45 CFR § 164.528, satisfying the requirement.	Amendments and Accountings of Disclosures	Microsoft General - HIPAA BAA (May 2025).pdf::::4	
Does the accounting provided by a covered entity include disclosures of protected health information by a business associate?	Correct	Yes	('Upon request, Ulalo will provide the Covered Entity with the information necessary to support a complete and timely accounting of disclosures.'), ('(viii) Accounting of Disclosure. Microsoft, at the request of Customer, shall within thirty (30) days make available to Customer such information relating to Disclosures made by Microsoft as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.')	The cited passages confirm that the business associate must furnish details of its own disclosures so the covered entity can include them in its accounting to individuals.	Amendments and Accountings of Disclosures	Accounting of Disclosures Policy.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::4	
Does the accounting provided by a covered entity include disclosures of protected health information by a business associate?	Correct	Yes	('Upon request, Ulalo will provide the Covered Entity with the information necessary to support a complete and timely accounting of disclosures.'), ('(viii) Accounting of Disclosure. Microsoft, at the request of Customer, shall within thirty (30) days make available to Customer such information relating to Disclosures made by Microsoft as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.')	The cited passages confirm that the business associate must furnish details of its own disclosures so the covered entity can include them in its accounting to individuals.	Amendments and Accountings of Disclosures	Accounting of Disclosures Policy.pdf::::1 Microsoft General - HIPAA BAA (May 2025).pdf::::4	
Has the business associate trained a member of its workforce on the policies and procedures with respect to protected health information?	Correct	Yes	('Workforce members involved in PHI maintenance shall receive training on:', 'Amendment handling procedures', 'Preservation of original PHI', 'Proper association of amended information'), ('Ulalo workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and patient protected health information.'), ('Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and Procedures and that he/she understands and agrees to abide by the guidelines contained herein.')	Multiple cited passages state that all workforce members, including those handling PHI, receive HIPAA privacy and security training, confirming the required training is provided.	Administrative Requirements	Amendment of Protected Health Information.pdf::::4 Information-System-Activity-Review-Policy.pdf::::2 Security-Privacy-Breach-Policy.pdf::::2	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the business associate provided training to a new member of the workforce within a reasonable period of time after they join?	Correct	Yes	('Ulalo commitment to reviewing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies.'), ('New employees will be required to take this training within the first month of employment.')	The cited passages require that new hires receive HIPAA training during orientation and no later than their first month, demonstrating timely training for new workforce members.	Administrative Requirements	Information-System-Activity-Review-Policy.pdf::::2 Security-Awareness-Training-Policy.pdf::::1	
Does the business associate provided training to all member of the workforce whose functions are affected by a material change in policies or procedures?	Correct	Yes	('9. Ulalo will provide training to all members of the workforce whose functions are affected by a material change in policies or procedures.')	The cited passage explicitly states that Ulalo will give training to every workforce member whose duties are impacted by material policy or procedure changes, meeting the requirement.	Administrative Requirements	Evaluation-Policy.pdf::::2	
Has the business associate documented that the training has been provided as described in this section?	Correct	Yes	('Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and Procedures and that he/she understands and agrees to abide by the guidelines contained herein.'), ('I, the undersigned, confirm that Ulalo SRL conducts and documents discussions related to HIPAA policies and procedures and maintains appropriate records of such discussions as part of its HIPAA compliance program.')	The cited passages show that employees must sign written acknowledgements of completed HIPAA training and that related records are maintained, demonstrating documented evidence of the provided training.	Documentation and Record Retention	Security-Privacy-Breach-Policy.pdf::::2 18_Policy_and_Procedure_Discussion_Meeting_Records_Attestation.pdf::::2	
Has the business associate mitigated, to the extent practicable, any harmful effect known to the business associate of a use or disclosure of protected health information in violation of its policies and procedures?	Correct	Yes	('This plan ensures that breaches are identified, contained, investigated, and reported in a timely manner to mitigate risk and comply with legal requirements.', 'Immediate Action: Upon discovery of a potential breach, immediately assess and contain the breach to prevent further unauthorized access or disclosure of PHI.'), ('Remedial Actions: Implement necessary measures to mitigate the breach\'s impact. This may include notifying affected parties, offering credit monitoring services, or making systemic changes to improve security.'), ('Review access control logs to determine how access was gained.', 'Implement stronger password policies or multi-factor authentication.', 'Restore from the last known good backup.', 'Analyze network traffic logs to understand the breach vector.')	The cited passages require immediate containment, remedial actions, and technical steps (e.g., log reviews, stronger authentication, restoration) that directly mitigate the harmful effects of unauthorized PHI use or disclosure.	Mitigation and Retaliation Provisions	HIPAA Breach Response Plan.pdf::::1, ::::3 HIPAA Security Incident Response Plan.pdf::::4	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Has the business associate implemented a policy and procedure with respect to protected health information as required by the Privacy subpart?	Correct	Yes	('Ulalo shall amend PHI only at the direction of a Covered Entity or as otherwise required by applicable law.', 'Amendment requests are received, reviewed, approved, or denied by the applicable Covered Entity. Upon approval, the Covered Entity will instruct Ulalo to implement the amendment.'), ('This policy establishes how [Company Name], in its role as a Business Associate, complies with the HIPAA Privacy Rule requirement at 45 CFR §164.528(a) regarding an individual\'s right to receive an accounting of certain disclosures of Protected Health Information (PHI).', 'Ulalo shall maintain a documented process to provide an accounting of disclosures of PHI for disclosures that are subject to HIPAA §164.528(a).')	The cited passages show formal written policies and procedures for PHI amendment and for accounting of disclosures, confirming that Ulalo has implemented the required HIPAA Privacy subpart controls.	Privacy Practices for Protected Health Information	Amendment of Protected Health Information.pdf::::2 Accounting of Disclosures Policy.pdf::::1	
Has the business associate changed its policy and procedure to comply with changes in the law?	Correct	Yes	('i. Changes in the HIPAA Security Regulations or Privacy Regulations.', '8. Whenever there is a change in law that necessitates a change to Ulalo\'s policies or procedures, Ulalo will promptly document and implement the revised policy or procedure.'), ('· Update Procedures: Revise breach response procedures based on lessons learned and incorporate any regulatory changes or guidance issued by the HHS.')	The cited passages require the organisation to revise and implement its policies whenever HIPAA or other regulations change, and to update breach-response procedures to incorporate new regulatory guidance, demonstrating that policies are changed to stay compliant with the law.	Privacy Practices for Protected Health Information	Evaluation-Policy.pdf::::2 HIPAA Breach Response Plan.pdf::::4	
Does the business associate document and implement a revised policy or procedure promptly after a change in law?	Correct	Yes	('8. Whenever there is a change in law that necessitates a change to Ulalo\'s policies or procedures, Ulalo will promptly document and implement the revised policy or procedure.'), ('· Update Procedures: Revise breach response procedures based on lessons learned and incorporate any regulatory changes or guidance issued by the HHS.')	The policy states that any legal change triggers immediate documentation and implementation of revised policies, and breach-response procedures must also be updated when regulations change, confirming prompt action after a change in law.	Documentation and Record Retention	Evaluation-Policy.pdf::::2 HIPAA Breach Response Plan.pdf::::4	
Has the business associate revised its disclosure notice to reflect changes in privacy practices before implementing such changes?	Correct	Yes	('22. Changes in privacy practices a. Company Name revises its disclosure notice to reflect changes in privacy practices before implementing such changes.')	The quoted clause expressly requires the organisation to update its disclosure notice prior to implementing any new privacy practices, satisfying the criterion.	Privacy Practices for Protected Health Information	Uses-and-Disclosures-of-PHI.pdf::::8	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Does the business associate maintain its policies and procedures in written or electronic form?	Correct	Yes	('HIPAA policies and procedures are maintained in a controlled central repository, and personnel responsible for implementing specific procedures have access to the latest approved versions, with availability and acknowledgment supported through access controls, acknowledgment tracking, or scheduled briefings.'), ('The [Security Manager] maintains all documentation for a minimum of six years [§164.530(j)].')	The cited passages state that policies are stored in a controlled central repository and that documentation is retained for at least six years, evidencing that policies and procedures are kept in written or electronic form.	Documentation and Record Retention	Security-Awareness-Training-Policy.pdf::::1 Facility-Access-Controls-Policy.pdf::::3	
Does the business associate retain documentation for a certain period?	Correct	Yes	('Amendment-related documentation shall be retained for a minimum of six (6) years from the date of creation or the date it was last in effect, whichever is later.'), ('The [Security Manager] maintains all documentation for a minimum of six years [§164.530(j)].'), ('All supporting documentation associated with the potential breach shall be kept on file for a period of 6 years.')	The cited passages from three separate policies each state that relevant documentation must be kept for at least six years, demonstrating that the business associate retains documentation for a defined period.	Documentation and Record Retention	Amendment of Protected Health Information.pdf::::3 Facility-Access-Controls-Policy.pdf::::3 Security-Privacy-Breach-Policy.pdf::::6	
Do all the policy or procedure documents, uploaded as evidence have an effective date?	Correct	Yes	('Created On 2/20/26 6:06:11 AM'), ('Effective Date: 02/19/2026'), ('Effective Date: 02/19/2026')	Multiple referenced documents clearly display either an “Effective Date” or “Created On” date, confirming that the policies carry an explicit effective date.	Documentation and Record Retention	Evaluation-Policy.pdf::::1 Security-Awareness-Training-Policy.pdf::::2 Contingency And Disaster Recovery Policy.pdf::::3	
Do all the policy or procedure documents, uploaded as evidence have a version number?	Correct	Yes	('Version : 1.0001'), ('Version : 1.001'), ('Version : 1.001')	The quoted lines show explicit version identifiers on several policy documents, indicating that version control is applied across the evidence set.	Documentation and Record Retention	Amendment of Protected Health Information.pdf::::2 Contingency And Disaster Recovery Policy.pdf::::2 Security-Awareness-Training-Policy.pdf::::2	
Do all the policy or procedure documents, uploaded as evidence have an approving authority?	Correct	Yes	('Approved By: Fabrice Kwetchet'), ('Approved By: Fabrice Kwetchet'), ('Approved By: CEO / Security Officer')	Each cited policy includes an “Approved By” notation (or equivalent) naming the individual or role that authorized the document, confirming the presence of an approving authority.	Documentation and Record Retention	Security-Awareness-Training-Policy.pdf::::2 HIPAA Breach Response Plan.pdf::::4 03- Access Control Policy â	

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Regulation Checkpoint: HIPAA - BA		
Analysis conducted on 2026-04-16 at 23:39 UTC.		
Summary of results is in file Ulalo HIPAA Certification Job v2 merged_HIPAA - BA.pdf		
Analysis conducted on the following document(s) (total number of pages is 145) submitted by Fabrice Kwetchet on 2026-04-14 at 01:15 UTC against the requirements of the above regulation checkpoints		
SRA_Tool_3_6.xlsx		(12 pages)
Udemy Certificate - Mastering HIPAA Compliance in 2026.pdf		(1 pages)
Microsoft General - HIPAA BAA (May 2025).pdf		(6 pages)
Accounting of Disclosures Policy.pdf		(3 pages)
Amendment of Protected Health Information.pdf		(4 pages)
Asset Management Policy and Procedure.pdf		(7 pages)
Contingency And Disaster Recovery Policy.pdf		(3 pages)
Evaluation-Policy.pdf		(2 pages)
Facility-Access-Controls-Policy.pdf		(3 pages)
HIPAA Breach Response Plan.pdf		(4 pages)
HIPAA Security Incident Response Plan.pdf		(5 pages)
Implementing a Schedule for Regular Vulnerability Scans of Systems Handling PHI.pdf		(5 pages)
Information-System-Activity-Review-Policy.pdf		(5 pages)
Media-Sanitization-and-Disposal-Policy.pdf		(3 pages)
Person-or-Entity-Authentication - done.pdf		(2 pages)
Risk-Management-Policy1.pdf		(6 pages)
Security-Awareness-Training-Policy.pdf		(2 pages)
Security-Privacy-Breach-Policy.pdf		(6 pages)
Technical-Safeguards-Access-Control-Policy.pdf		(8 pages)
Uses-and-Disclosures-of-PHI.pdf		(8 pages)
Workstation-Security-Policy.pdf		(2 pages)
01_Unique_User_ID_Policy.pdf		(2 pages)
02- Azure - HIPAA Proof of Implementation.pdf		(4 pages)
03- Access Control Policy â		(4 pages)
04- Access Control System Logs â		(4 pages)

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

05- Authorized Personnel & Supervisors.pdf		(3 pages)
06- Authorized Personnel Access Le.pdf		(4 pages)
07_Encrypted_Data_Storage_and_Transmission_Records.pdf		(2 pages)
08- Logs of Access Attempts and En.pdf		(3 pages)
09- Security Monitoring Tools & Systems â		(4 pages)
10- System Login & Authentication Logs â		(4 pages)
11_Auditing_and_Monitoring_Tools_Records.pdf		(2 pages)
12_Integrity_Controls_Implementation_Attestation.pdf		(2 pages)
14_Authentication_Mechanisms_System_Configuration_Attestation.pdf		(2 pages)
15_Policy_Distribution_and_Workforce_Acknowledgement_Attestation.pdf		(2 pages)
16_Antivirus_and_Anti_Malware_Implementation_Attestation.pdf		(2 pages)
17_Security_Testing_and_Assessment_Records_Attestation.pdf		(2 pages)
18_Policy_and_Procedure_Discussion_Meeting_Records_Attestation.pdf		(2 pages)

Doc ID: 82d186244105d106de15f4c9514029e5001b1d4d

Dropbox Sign

Audit trail

Title	Konfer Assessment of HIPAA-BA compliance for Ulalo
File name	Ulalo_HIPAA...AA_-_BA.pdf and 1 other
Document ID	82d186244105d106de15f4c9514029e5001b1d4d
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

SENT	**05 / 03 / 2026** 19:22:54 UTC	Sent for signature to Debu Chatterjee (debu@konfer.ai) from debu@konfer.ai IP: 24.5.48.197
VIEWED	**05 / 03 / 2026** 19:22:55 UTC	Viewed by Debu Chatterjee (debu@konfer.ai) IP: 24.5.48.197
SENT	**05 / 03 / 2026** 19:25:48 UTC	A new document has been created based off of an existing document with ID 82d186244105d106de15f4c9514029e5001b1d4d IP: 24.5.48.197
EDITED	**05 / 03 / 2026** 19:25:48 UTC	Edited by Debu Chatterjee (debu@konfer.ai) IP: 24.5.48.197
RESENT	**05 / 03 / 2026** 19:25:49 UTC	Signature request resent by Debu Chatterjee (debu@konfer.ai) IP: 24.5.48.197

Dropbox Sign

Audit trail

Title	Konfer Assessment of HIPAA-BA compliance for Ulalo
File name	Ulalo_HIPAA...AA_-_BA.pdf and 1 other
Document ID	82d186244105d106de15f4c9514029e5001b1d4d
Audit trail date format	MM / DD / YYYY
Status	Signed

Document History

SIGNED	**05 / 03 / 2026** 19:26:35 UTC	Signed by Debu Chatterjee (debu@konfer.ai) IP: 24.5.48.197
COMPLETED	**05 / 03 / 2026** 19:26:35 UTC	The document has been completed.