Scribeberry Privacy Controls

1. ScribeBerry's Completion of Security Risk Assessment (SRA)

ScribeBerry completed a comprehensive Security Risk Assessment (SRA), aligning with industry best practices and regulatory requirements. This assessment, crucial for maintaining robust security and protecting sensitive information like Electronic Protected Health Information (ePHI), involved evaluating their systems, policies, and procedures to identify and mitigate security risks.

2. ScribeBerry's Review and Update of SRA

ScribeBerry reviews and updates the Security Risk Assessment annually. This ensures that their security measures remain effective against the latest technological advancements and evolving cyber threats. These reviews assess the efficacy of existing security controls and implement updates to enhance security posture and regulatory compliance.

3. Frequency of ScribeBerry's SRA Review and Update

ScribeBerry conducts its Security Risk Assessment review and update annually. This frequency balances ongoing vigilance with practicality, aligning with their internal audit cycle and regulatory reporting requirements, ensuring that their security strategies remain current with best practices and standards.

4. Inclusion of All Information Systems in ScribeBerry's SRA

ScribeBerry includes all information systems handling Electronic Protected Health Information (ePHI) in its Security Risk Assessment. This includes their primary web application and ancillary data processing and storage services, ensuring comprehensive coverage of all potential vulnerabilities.

5. ScribeBerry's Compliance with HIPAA and PIPEDA Security

To comply with HIPAA and PIPEDA security regulations, ScribeBerry implements a multi-faceted approach. This includes regular policy reviews by a privacy regulatory officer, a privacy impact assessment, and an external audit by a privacy expert, ensuring compliance and recommendations for enhancements.

6. Content of ScribeBerry's SRA Documentation

ScribeBerry's Security Risk Assessment documentation includes risk identification, analysis, and mitigation strategies, continuous monitoring, detailed documentation and reporting, and periodic review and update. It covers risks associated with third-party services like Microsoft

Azure's OpenAI (amongst others) and internal processes, ensuring comprehensive risk management.

7. ScribeBerry's Response to Threats and Vulnerabilities

ScribeBerry, while not having faced an actual breach, has established mechanisms to address potential risks. This includes bi-weekly meetings to address risks, aiming to close any scanned potential vulnerabilities within 1-2 weeks of identification, ensuring up-to-date and effective security measures.

8. Personnel Involvement in SRA Threats and Vulnerabilities Response at ScribeBerry

Dr. Zaahir Moloo plays a key role in overseeing and mitigating threats and vulnerabilities identified in ScribeBerry's Security Risk Assessment, ensuring an expert approach to managing security issues.

9. Communication of SRA Results to ScribeBerry Personnel

ScribeBerry ensures staff awareness of Security Risk Assessment results through direct communication, either in person or via audio calls. This strategy promotes a culture of security awareness throughout the team

10. Communication Methods for SRA Results at ScribeBerry

ScribeBerry uses direct communication channels, such as in-person meetings and audio calls, to communicate results of Security Risk Assessments regarding identified threats and vulnerabilities. This ensures prompt and clear dissemination of important information, keeping all relevant personnel informed about security concerns and mitigation steps, and fostering a collaborative and responsive security environment.

11. Maintenance of Documentation for Risk Assessment, Risk Management, and Information Security Activities at ScribeBerry

ScribeBerry maintains comprehensive documentation of all policies and procedures related to risk assessment, risk management, and information security activities. This serves as a central reference for their security practices and includes detailed records of risk assessments, mitigation strategies, incident response plans, and employee training programs. The documentation is regularly reviewed and updated to ensure it reflects the latest best practices and regulatory requirements.

12. ScribeBerry's Review and Update of Security Documentation

ScribeBerry regularly reviews and updates its security documentation, including policies and procedures, to ensure robust and effective security measures. Updates respond to technological changes, emerging security threats, new regulatory requirements, or significant operational changes, maintaining the relevance and accuracy of their documentation.

13. Process for Updating Security Program Documentation at ScribeBerry

ScribeBerry follows a structured process for updating its security program documentation. This involves collaborative reviews by IT, security, and compliance teams, with updates made following internal review meetings or regulatory changes. Revised documentation is then shared and stored in a central repository, accessible to all team members.

14. Involvement of Security Officer in Updates at ScribeBerry

The Security Officer at ScribeBerry plays an integral role in updating security policies and procedures. Their expertise ensures that updates reflect a deep understanding of the security landscape, align with regulatory requirements and best practices, and maintain the integrity of the security program.

15. Alignment of Documentation with Actual Business Practices at ScribeBerry

ScribeBerry ensures a stringent alignment between documented risk management and security procedures and their actual business practices. This is verified through internal audits, reviews, and the practical application of policies, ensuring that documented procedures are actively practiced and ingrained in their organizational culture.

16. Retention Period for Information Security Management and Risk Management Documents at ScribeBerry

ScribeBerry maintains its information security management and risk management documents indefinitely. This perpetual retention policy provides a complete historical record of their security practices, aiding in ongoing analysis and compliance with long-term regulatory requirements.

17. Availability of Information Security and Risk Management Documentation at ScribeBerry

ScribeBerry prioritizes the availability of its information security and risk management documentation, maintaining a controlled-access system for efficient and secure access upon request by relevant stakeholders, while preserving the confidentiality of sensitive information.

18. Ensuring Accessibility of Security and Risk Management Documentation at ScribeBerry

ScribeBerry has implemented a comprehensive dashboard to centralize and provide easy access to security and risk management documentation. This user-friendly platform enhances their security governance and compliance transparency.

19. Responsibility for Developing and Implementing Information Security Policies and Procedures at ScribeBerry

Dr. Zaahir Moloo and Amaan Rattansi are responsible for developing and implementing ScribeBerry's information security policies and procedures. Dr Moloo’s expertise ensures robust, compliant security strategies that effectively safeguard patient and company data, shaping their security framework to the highest standards.

20. Documentation of Security Officer's Role and Responsibilities at ScribeBerry

The role and responsibilities of ScribeBerry's Security Officer, Dr. Zaahir Moloo, are clearly documented. His duties include overseeing security policy development, managing risk assessments, ensuring regulatory compliance, and leading incident response efforts, ensuring a high level of organizational security and accountability.

21. Qualifications of ScribeBerry's Security Officer

Dr. Zaahir Moloo, ScribeBerry's Security Officer, is qualified, with knowledge and experience in healthcare and information security. His qualifications include a background in medicine and an understanding of cybersecurity risks and mitigation strategies, ensuring that ScribeBerry's security measures align with healthcare sector needs and regulations.

22. Workforce Awareness of the Security Officer at ScribeBerry

All ScribeBerry workforce members are aware of Dr. Zaahir Moloo as their Security Officer. His role is communicated during the onboarding process and through regular internal communications, ensuring staff members promptly and correctly direct any security concerns or incidents to him.

23. Workforce Knowledge on Contacting the Security Officer at ScribeBerry

ScribeBerry's workforce is well-informed about contacting the Security Officer. Dr. Zaahir Moloo's contact details are readily available, and the protocols for reporting security concerns are outlined in the security policies, fostering open communication of any security issues.

24. Contact for Security Considerations in Absence of Security Officer at ScribeBerry

In Dr. Zaahir Moloo's absence, Mr. Amaan Rattansi handles security considerations at ScribeBerry. As a knowledgeable member of the technical team, he effectively manages security concerns, with his role as an alternate point of contact known to all staff members.

25. Definition of Roles and Job Duties Regarding ePHI Access at ScribeBerry

ScribeBerry does not grant ePHI access to any staff members, minimizing direct interaction with sensitive patient data. Operations are designed for ePHI to be processed and transmitted without direct access by team members, reducing unauthorized access or data breach risks.

26. Screening of Workforce Members for Trustworthiness at ScribeBerry

ScribeBerry emphasizes the trustworthiness of workforce members, implementing a rigorous screening process that includes non-disclosure agreements and background checks. This comprehensive screening maintains the integrity and security of the sensitive data they handle.

27. Process of Screening Workforce Members at ScribeBerry

ScribeBerry's screening process for workforce members involves reviewing professional history, conducting reference checks, and performing criminal background checks as appropriate. This process, along with mandatory NDAs, ensures the reliability and integrity of employees in handling sensitive data.

28. Ensuring Security Training for All Workforce Members at ScribeBerry

ScribeBerry prioritizes security training for all workforce members, including management. Their comprehensive training program covers HIPAA compliance, data privacy, and cybersecurity best practices, and is mandatory for all employees.

29. Process to Ensure Workforce Members Receive Security Training at ScribeBerry

ScribeBerry maintains a systematic approach to ensure all workforce members receive security training. This includes scheduled training sessions during onboarding and periodic updates, utilizing a mix of in-house and external resources.

30. Record-Keeping of Workforce Member Security Training at ScribeBerry

ScribeBerry keeps any records of security training completed by workforce members, including training dates, content, and assessment results if applicable. This record-keeping tracks compliance with internal policies and demonstrates their commitment to ongoing security and privacy education.

31. Monitoring of Log-in Attempts and Reporting Discrepancies at ScribeBerry

ScribeBerry monitors log-in attempts and reports any discrepancies. Their system detects and logs all access attempts, and the logs are actively monitored for unusual or unauthorized patterns. Suspicious activity triggers an immediate alert to the security team, facilitating early detection of potential security incidents and strengthening overall security posture.

32. Protection from Malicious Software at ScribeBerry

ScribeBerry prioritizes protection against malicious software. All devices have the latest antivirus and malware protection software, regularly updated to counter new threats. Periodic security audits check for vulnerabilities, ensuring the effectiveness of protective measures and safeguarding systems and data from cyber threats.

33. Password Security Training Elements at ScribeBerry

ScribeBerry's security training program includes modules on password security. Workforce members are educated on creating strong, unique passwords and changing them regularly. They use Google's authentication services, secured by a Business Associate Agreement (BAA), ensuring password policies and practices meet high security and compliance standards.

34. Ongoing Awareness of Security Requirements Among Workforce at ScribeBerry

ScribeBerry maintains ongoing awareness of security requirements among workforce members through regular meetings and updates on security policies and practices. This approach includes formal training sessions and regular communications, fostering a culture of security within the organization.

35. Ensuring Workforce Awareness of Security Requirements at ScribeBerry

ScribeBerry regularly disseminates updates and reminders about security protocols and new threats through various channels, including team meetings. Keeping security a constant topic of discussion and education aims to keep all employees vigilant and informed about their role in data integrity and confidentiality.

36. Sanction Policy for Enforcing Security Procedures at ScribeBerry

ScribeBerry has a stringent sanction policy to enforce security procedure adherence. This policy holds personnel accountable for non-compliance with security protocols. Breaches, whether intentional or negligent, result in disciplinary actions ranging from warnings and retraining to suspension or termination, depending on the severity.

37. Inclusions in Sanction Policy to Hold Personnel Accountable at ScribeBerry

ScribeBerry's sanction policy includes measures for holding personnel accountable for security policy violations. It outlines consequences for violations, detailing steps for infractions like retraining, warnings, suspension, and termination. Regular reviews update the policy to align with regulatory requirements and best practices.

38. Management and Control of Personnel Access to ePHI, Systems, and Facilities at ScribeBerry

ScribeBerry rigorously manages and controls personnel access, with no one in the organization having access to ePHI. They implement strict access controls and regularly review access rights, ensuring only authorized personnel have access to sensitive systems. Their access control policies minimize potential risks by providing the least privilege necessary for each role.

39. Process for Managing and Controlling Personnel Access at ScribeBerry

ScribeBerry's process for managing and controlling personnel access involves multi-factor authentication, using only BAA-approved providers, role-based access control, and regular access log reviews. Periodic reviews of access rights ensure alignment with current job responsibilities, and any role changes trigger an immediate reassessment of access privileges.

40. Authorizing, Establishing, and Modifying Access to ePHI at ScribeBerry

ScribeBerry's process for authorizing, establishing, and modifying access to ePHI is governed by strict protocols. Personnel do not have direct access to ePHI, and access to systems handling ePHI is tightly controlled and monitored. Requests for system and server access are thoroughly vetted and require approval from designated authorities. Access is granted on a need-to-know basis and is promptly modified or revoked if an individual’s role changes or they leave the organization, ensuring security even within secured environments.

41. Access to ePHI Granted to Users or Other Entities at ScribeBerry

ScribeBerry regulates access to ePHI, ensuring it's only accessible to authorized users, specifically for healthcare-related duties. They have a Business Associate Agreement (BAA) with Microsoft Azure and Anthropic, safeguarding PHI and preventing unwarranted access. The BAA delineates permissible access and usage of ePHI, complying with HIPAA regulations and PIPEDA regulations.

42. Identification of Users Accessing ePHI at ScribeBerry

ScribeBerry takes user identification for ePHI access seriously, using robust authentication mechanisms provided by Microsoft. Secure login protocols and authentication checks verify each user's identity, preventing unauthorized access to sensitive health information.

43. Ensuring Workforce Members Have Appropriate Access to ePHI at ScribeBerry

ScribeBerry ensures no ePHI access for workforce members through stringent access controls and regular audits. Access policies provide the least privilege necessary, aligning with specific job roles and responsibilities to minimize unauthorized access or data breaches.

44. Consistency and Appropriateness of Workforce's Access to ePHI at ScribeBerry

ScribeBerry maintains consistency and appropriateness in workforce ePHI access through rigorous access management. They have indirect interactions with ePHI through partners, governed by strict access protocols. Regular reviews ensure access rights reflect job function changes, maintaining ePHI access control integrity.

45. Use of Encryption to Control Access to ePHI at ScribeBerry

Encryption is a key tool for ScribeBerry in controlling ePHI access. They employ end-to-end encryption to protect ePHI during transmission and processing, making data unreadable to unauthorized individuals. Their encryption protocols adhere to healthcare industry standards.

46. Procedures for Encrypting ePHI at ScribeBerry

ScribeBerry has procedures for encrypting ePHI, employing advanced encryption technologies for data transmission. This encryption adheres to healthcare standards, protecting ePHI during processing and transit. They continuously evaluate and update encryption methodologies to align with data security advancements.

47. Alternative Safeguards in Place of Encryption at ScribeBerry

Besides encryption, ScribeBerry implements alternative safeguards like firewall protections against unauthorized access and intrusion attempts. They recognize the need for a multi-layered security approach, assessing and integrating complementary security measures for comprehensive ePHI protection.

48. Documentation of Alternative Safeguards When Encryption is Not Implemented at ScribeBerry

ScribeBerry documents the use of alternative safeguards when encryption is not implemented. This includes detailing the rationale for choosing alternative methods and outlining specific security measures employed, ensuring these alternatives provide comparable security to encryption as per HIPAA requirements.

49. Evaluation of Encryption Solutions in the Local Environment at ScribeBerry

Given their reliance on cloud storage and processing via Microsoft Azure's HIPAA-compliant and PIPEDA compliant environment, ScribeBerry minimizes the need for local encryption solutions. This cloud-based approach ensures data security through robust encryption protocols managed by their cloud service provider, reducing the necessity for full disk encryption or encryption of external media.

50. Evaluation of Encryption Solutions for Cloud Services at ScribeBerry

ScribeBerry rigorously evaluates encryption solutions for cloud services to ensure data security. They use Google for business platforms under a Business Associate Agreement (BAA), aligning their data storage practices with HIPAA and PIPEDA standards. Their focus is on securing business communications and operations within these platforms. These are not used for sharing PHI.

51. Evaluation of Encryption Solutions for Data in Transit at ScribeBerry

ScribeBerry employs robust encryption solutions for securing data in transit, including VPNs and HTTPS protocols for web traffic. They also use region-locked servers for Azure services, ensuring data processing within the same geographical region as the user. This approach enhances data security and complies with regional regulations.

52. Periodic Review of Information Systems for Security Settings Implementation at ScribeBerry

ScribeBerry conducts bi-weekly reviews of their information systems, ensuring that security settings are optimized to effectively safeguard ePHI. This dynamic review process helps maintain a strong defense against evolving cyber threats by continuously evaluating and adjusting security configurations.

53. Awareness of Security Settings in Information Systems at ScribeBerry

ScribeBerry maintains constant awareness of the security settings within their information systems. Regular reviews examine and verify security configurations, keeping the team informed on the latest security best practices and technological advancements for maximum security and compliance.

54. Use of Security Settings and Mechanisms to Record System Activity at ScribeBerry

ScribeBerry utilizes security settings and mechanisms, including a comprehensive dashboard, to record system activity. This monitoring capability provides real-time insights into system usage and potential security events, enabling early detection and prompt response to unusual activities and potential security incidents.

55. Mechanisms in Place to Monitor and Log System Activity at ScribeBerry

ScribeBerry employs Microsoft’s logging tools to monitor and log system activity. These mechanisms offer detailed insights into system usage, access patterns, and user behaviors, aiding in the identification and response to security incidents and ensuring the protection of sensitive health information in transit to and from third-party providers.

56. Monitoring and Tracking of ePHI System Activity at ScribeBerry

ScribeBerry has systems to monitor and track activities related to ePHI. While direct access to ePHI is not available, they monitor usage patterns to ensure appropriate use by authorized individuals. This monitoring respects user privacy and data protection regulations, maintaining ePHI confidentiality and integrity.

57. Implementation of Automatic Logoff on Devices Accessing ePHI at ScribeBerry

ScribeBerry has implemented an automatic logoff mechanism for devices accessing ePHI, using Google's secure authentication services. This feature, terminating sessions after inactivity, reduces unauthorized access risks if a device is left unattended.

58. Verification of Users Accessing ePHI at ScribeBerry

ScribeBerry ensures that users accessing ePHI are verified through robust authentication processes, including Google authentication services. Each user has a secure account, with encrypted and monitored access to prevent unauthorized use, maintaining ePHI confidentiality and security.

59. Ensuring User Identity Verification in ePHI Access at ScribeBerry

ScribeBerry employs stringent user identity verification processes, including google based secure login protocols, supported by Google's authentication services. This ensures thorough verification of each user's identity before granting the individual the ability to input ePHI into the web application

60. Determination of ePHI Access Methods at ScribeBerry

ScribeBerry controls ePHI access through strict protocols. Users access ePHI via individual accounts under comprehensive terms of service and privacy policies. These methods are secure, regulatory-compliant, and aligned with their commitment to safeguarding sensitive health information.

61. Protection of ePHI from Unauthorized Modification or Destruction at ScribeBerry

ScribeBerry employs multiple layers of security controls, including advanced encryption, access controls, and regular system audits, to protect ePHI from unauthorized modification or destruction. This ensures that only authorized healthcare professionals can modify or delete ePHI, maintaining the integrity and confidentiality of patient data.

62. Confirmation of ePHI Integrity at ScribeBerry

ScribeBerry's systems track and log user activities related to ePHI manipulation, ensuring that any modifications or deletions are conducted solely by authorized individuals. Although they do not directly control or access ePHI, their monitoring systems maintain the integrity of ePHI and ensure compliance with HIPAA regulations.

63. Protection Against Unauthorized ePHI Access During Transmission at ScribeBerry

To protect ePHI during electronic transmission, ScribeBerry uses robust encryption protocols, ensuring all ePHI transmitted through their systems is encrypted end-to-end. This prevents potential interception or unauthorized access, demonstrating their commitment to advanced encryption technologies for protecting ePHI.

64. Recording Activity on Information Systems Handling ePHI at ScribeBerry

ScribeBerry has mechanisms to record activity on information systems handling ePHI, enabling comprehensive logs of system activity, including user access and data modifications. Regular reviews of these logs enhance the overall security of their information systems.

65. Management of Facility Access and ePHI Use at ScribeBerry

ScribeBerry adheres to strict security protocols for managing access to facilities and usage of ePHI-housing information systems. They maintain control over server configurations and access permissions, with digital access to these facilities restricted to authorized personnel only.

66. Physical Protections for Facility Security Risks at ScribeBerry

ScribeBerry ensures the security of physical equipment, like laptops used by key personnel. These devices are secured with strong passwords and the latest security software, protecting them against theft, loss, and unauthorized access, even though they do not house ePHI.

67. Restriction of Physical Access to Equipment Housing ePHI at ScribeBerry

Since ScribeBerry’s operational model does not involve housing ePHI on physical devices, there are no requirements for restricting physical access to such equipment. Their focus is on securing the cloud environment where ePHI is processed.

68. Management of Workforce, Visitor, and Third-Party Access to Electronic Devices at ScribeBerry

ScribeBerry controls access to individual, secure digital environments and devices used by team members for professional duties. Policies are in place to ensure no unauthorized personnel access their systems.

69. Physical Protections for Electronic Devices Accessing ePHI at ScribeBerry

While ScribeBerry does not have direct access to ePHI through their devices, all electronic devices used by the team are secured with strong authentication measures, including password protection and, where applicable, encryption.

70. Physical Protection Measures for Devices with ePHI Access at ScribeBerry

ScribeBerry ensures that all personal devices used by their team are equipped with necessary security measures such as password protection and data encryption, despite not directly accessing ePHI.

71. Inventory and Location Record of Electronic Devices at ScribeBerry

ScribeBerry maintains an inventory and location record of all electronic devices used by their team members. Regular audits verify the status of these devices, ensuring they are used in compliance with security policies. This inventory management is crucial for managing risks associated with device loss or unauthorized access.

72. Authorized User for Approving Access Levels within Information Systems and ePHI at ScribeBerry

Dr. Zaahir Moloo is responsible for approving access levels within ScribeBerry's information systems interacting with ePHI. He oversees access control policies, ensuring compliance with necessary security and regulatory standards, and approves changes in access levels.

73. Validation of Personnel Access to Facilities Based on Role or Function at ScribeBerry

As ScribeBerry operates in a cloud-based environment without physical facilities housing ePHI, validating personnel access to physical facilities is not applicable. Their focus is on securing digital access to systems and data, ensuring appropriate access rights based on specific roles and responsibilities.

74. Validation Process for Access to Facility at ScribeBerry

ScribeBerry does not operate physical facilities that require controlled access, thus a validation process for facility access is not applicable. Their security efforts concentrate on managing and securing digital access to cloud-based systems.

75. Access Validation Requirements for Critical Systems at ScribeBerry

ScribeBerry enforces strict access validation requirements for critical systems like IT and software development. Access is based on role-specific needs and is continuously monitored for changes in responsibilities or employment status, ensuring restricted access to authorized individuals.

76. Controlling Access to Software Programs for Testing and Revisions at ScribeBerry

ScribeBerry controls access to software programs during testing and revisions, granting access on a need-to-know basis to development and IT security teams. They utilize role-based access controls to maintain system integrity during the development phase.

77. Procedures for Validating Third-Party Access Based on Role or Function at ScribeBerry

ScribeBerry's procedures for validating third-party access are stringent, granting access based on specific roles or functions and aligning with contractual obligations and security standards. Mr. Amaan Rattansi oversees the approval and review process, with regular audits and logs maintained for compliance.

78. Mechanisms for Recording and Examining Activity on Information Systems with ePHI Access at ScribeBerry

ScribeBerry employs mechanisms to record and examine activity on information systems with ePHI access. Their monitoring systems track user activities, enhancing transparency and enabling prompt detection of unusual or unauthorized actions.

79. Retention Requirements for Audit Reports at ScribeBerry

ScribeBerry maintains audit reports indefinitely, providing a comprehensive historical record of their security posture and aiding compliance with regulatory requirements, as well as offering data for ongoing security assessments and improvements.

80. Maintenance of Records for Physical Changes, Upgrades, and Modifications to Facility at ScribeBerry

As ScribeBerry's operations are cloud-based without a physical facility housing sensitive data or systems, there are no records of physical changes, upgrades, or modifications to such a facility. Their focus is on documenting changes to digital infrastructure and cloud-based systems.

81. Awareness of Movement of Electronic Devices and Media at ScribeBerry

ScribeBerry maintains awareness of the movement of electronic devices and media used by their team. Regular reminders and training sessions reinforce the importance of device security, and an incident response plan is in place for loss or breach incidents.

82. Security of Electronic Devices at ScribeBerry

The security of electronic devices, primarily professional work laptops, is a priority at ScribeBerry. These devices are equipped with strong passwords and the latest security software, and are used exclusively for professional purposes to protect any sensitive information.

83. Backup of ePHI for Device Mobility at ScribeBerry

As ScribeBerry does not store or directly access ePHI, they do not have a process for ePHI backup. Their role in ePHI handling is limited to processing through secure, encrypted channels, maintaining data control with healthcare providers.

84. Sanitization of Devices Handling ePHI at ScribeBerry

ScribeBerry follows best practices for sanitizing devices that are disposed of or repurposed, securely wiping any data and restoring devices to factory settings, despite not directly handling or storing ePHI on these devices.

85. Appropriate Use of Electronic and Network Devices at ScribeBerry

ScribeBerry has established policies for the appropriate use of electronic and network devices, part of staff training, designed to prevent unauthorized access or misuse and to uphold security and privacy standards.

86. Termination of ePHI Access Upon Workforce Member Departure at ScribeBerry

ScribeBerry terminates access to systems transmitting ePHI immediately upon the end of an employment or other arrangement with a workforce member. This is in line with their security protocols, ensuring that indirect interaction with ePHI through their systems is promptly revoked.

87. Procedures for Terminating or Changing Third-Party Access at ScribeBerry

Strict procedures are in place at ScribeBerry for terminating or changing third-party access, including revoking access rights and securely handling any shared data, with regular reviews and updates of all third-party accesses.

88. Media Sanitization Prior to Reuse at ScribeBerry

ScribeBerry adheres to strict protocols for sanitizing media before reuse. Any storage media used within the organization is thoroughly wiped to ensure no residual data remains, although physical media is not typically used in their operations.

89. Contracting with Business Associates or Third-Party Vendors at ScribeBerry

Contracts with business associates and third-party vendors at ScribeBerry are reviewed meticulously to align with security and privacy standards. Each associate or vendor signs a

Business Associate Agreement (BAA) for HIPAA compliance and other data protection regulations.

90. Third-Party Vendor Access to Information Systems and ePHI at ScribeBerry

Third-party vendors are granted access to ScribeBerry’s information systems and ePHI only when necessary, governed by stringent security protocols. Vendors are vetted to meet high standards for data security and privacy.

91. Identification of Business Associates Needing ePHI Access at ScribeBerry

ScribeBerry identifies business associates requiring access to ePHI based on their services. Access is minimal and on a need-to-know basis, ensuring ePHI is accessible only to those absolutely necessary for service functions.

92. Enforcement and Monitoring of Business Associate Access at ScribeBerry

ScribeBerry enforces and monitors access granted to business associates through logging and auditing. Regular reviews of access logs and service scope changes ensure alignment with operational requirements and security standards.

93. Communication of Security Practice Changes by Business Associates at ScribeBerry

Business associates are required to communicate significant changes in their security practices or personnel. ScribeBerry actively reviews these updates to ensure continued alignment with security requirements.

94. Execution of Business Associate Agreements (BAAs) at ScribeBerry

ScribeBerry has executed BAAs with all associates involved in the creation, receipt, maintenance, or transmission of ePHI, ensuring that they adhere to the same privacy and security standards upheld by ScribeBerry.

95. Awareness of Business Associate Security Practices at ScribeBerry

ScribeBerry maintains awareness of their business associates' security practices through BAAs, which detail expected security measures and compliance requirements, providing a framework for ePHI confidentiality and integrity.

96. Inclusion of Safeguards in Business Associate Agreements at ScribeBerry

BAAs at ScribeBerry include assurances on how business associates safeguard ePHI, aligning with HIPAA requirements and ensuring the implementation of appropriate security measures.

97. Terms in BAAs for Subcontractor ePHI Security at ScribeBerry

The terms in ScribeBerry's BAAs stipulate that subcontractors must adhere to the same level of data protection and security as direct business associates, ensuring uniform ePHI security across all service tiers.

98. Requirement for Incident Reporting in BAAs at ScribeBerry

Business Associate Agreements at ScribeBerry require vendors to report any security incidents involving ePHI promptly, allowing for quick action and mitigation of potential breaches or concerns.

99. Updates to BAAs Reflecting Omnibus Rule Requirements at ScribeBerry

Since its inception, ScribeBerry's BAAs have been crafted with the Omnibus Rule updates to HIPAA in mind, ensuring they are current and fully compliant with the latest regulations.

100. Documentation of Business Associates Accessing ePHI at ScribeBerry

ScribeBerry maintains a comprehensive database documenting all business associates that require access to ePHI. This includes details of their access scope, the nature of the services provided, and their compliance status, essential for managing relationships and ensuring oversight of their access and handling of ePHI.

101. Obtaining Business Associate Agreements (BAAs) at ScribeBerry

ScribeBerry obtains BAAs from all business associates who access ePHI on their behalf. These comprehensive documents outline responsibilities and expectations for handling and protecting ePHI, ensuring associates are compliant with HIPAA regulations.

102. Contingency Planning for Emergencies at ScribeBerry

ScribeBerry has developed a robust contingency plan to ensure continuity and security of operations during emergencies. This plan includes data backup, system recovery, and maintaining essential functions, designed to mitigate the impact of various emergencies.

103. Documentation of Contingency Plan at ScribeBerry

The contingency plan at ScribeBerry is thoroughly documented and accessible to relevant personnel. It outlines specific protocols for different emergency scenarios, ensuring a swift and coordinated response, with regular reviews and updates for effectiveness.

104. Periodic Updates to Contingency Plan at ScribeBerry

ScribeBerry regularly updates its contingency plan to reflect changes in the operational environment, technological advancements, and emerging threats. These updates ensure the plan remains relevant and effective.

105. Effectiveness and Appropriateness of Contingency Plan at ScribeBerry

The effectiveness of ScribeBerry's contingency plan is evaluated through drills and exercises, assessing its appropriateness in response to different emergencies. Necessary adjustments are made based on these evaluations.

106. Consideration of Emergencies Affecting Critical Systems at ScribeBerry

In developing their contingency plan, ScribeBerry considers a range of emergencies that could impact critical information systems and access to ePHI, including natural disasters, cyber-attacks, and system failures.

107. Types of Emergencies Considered at ScribeBerry

ScribeBerry's contingency planning considers emergencies like natural disasters, power outages, hardware failures, and cyber-attacks, ensuring preparedness for various scenarios that could disrupt operations or compromise data security.

108. Documentation of Emergency Types and Response Strategies at ScribeBerry

The contingency plan at ScribeBerry includes detailed documentation of various emergency types and specific response strategies, serving as a guideline for effective management of different emergency scenarios.

109. Policies and Procedures for Security Incidents at ScribeBerry

ScribeBerry has comprehensive policies and procedures for preventing, detecting, and responding to security incidents. These include identifying threats, response protocols, and post-incident recovery procedures, ensuring a prompt and effective organizational response.

110. Prevention, Detection, and Response to Security Incidents at ScribeBerry

ScribeBerry uses multiple layers of security measures for preventing, detecting, and responding to security incidents, including advanced monitoring tools, regular security training, and a dedicated incident response team.

111. IIdentification of Incident Response Team at ScribeBerry

ScribeBerry has a designated incident response team led by Dr. Zaahir Moloo and Amaan Rattansi, consisting of individuals who are responsible for security incident management. They coordinate responses to security breaches and ensure effective mitigation measures.

112. Training and Identification of Incident Response Team Members at ScribeBerry

Members of ScribeBerry's incident response team, including leaders Dr. Zaahir Moloo and Amaan Rattansi, are chosen for their expertise in security and emergency response. They receive specialized training to stay adept in handling security incidents.

113. Evaluation of Systems and ePHI for Emergency Continuity at ScribeBerry

ScribeBerry evaluates critical systems and aspects of ePHI necessary for maintaining business operations during emergencies. This evaluation is essential for contingency planning, ensuring essential functions continue and ePHI remains protected.

114. Maintaining ePHI Access in Emergencies at ScribeBerry

ScribeBerry's cloud-based operational model, managed by reliable service providers, ensures continuous access to ePHI during emergencies. Their disaster recovery capabilities allow healthcare providers uninterrupted ePHI access under challenging conditions.

115. Maintaining ePHI Security Before, During, and After an Emergency at ScribeBerry

ScribeBerry employs multiple layers of protection, including redundant systems, data backups, and encryption protocols, to maintain ePHI security before, during, and after emergencies, ensuring patient privacy and data integrity.

116. Data Backup and Restoration Plan at ScribeBerry

While not storing ePHI, ScribeBerry maintains a data backup and restoration plan for operational data and system configurations. This ensures quick system restoration in case of data loss or system failure, minimizing operational disruptions.

117. Activation of Emergency Procedures at ScribeBerry

ScribeBerry activates emergency procedures in response to specific triggers or scenarios. The incident response team evaluates the situation and initiates necessary procedures, ensuring the safety and continuity of operations.

118. Coordination of Facility Access in Emergencies at ScribeBerry

As ScribeBerry operates primarily in a cloud-based environment, coordinating access to physical facilities in emergencies is not applicable. Their focus is on ensuring accessibility and security of cloud-based services in all situations.

119. Termination of Emergency Procedures at ScribeBerry

Once an emergency is resolved, ScribeBerry's incident response team assesses the situation and terminates emergency procedures. A post-incident review is conducted to evaluate the response and identify improvement areas.

120. Formal Evaluation of Security Safeguards at ScribeBerry

ScribeBerry conducts formal evaluations of their security safeguards, including physical safeguards, on a regular basis. These evaluations assess the effectiveness of security measures, identify potential gaps, and make necessary adjustments to enhance overall security posture.

121. Evaluation of Security Safeguards Effectiveness at ScribeBerry

The effectiveness of ScribeBerry's security safeguards is evaluated through internal audits, vulnerability assessments, and periodic reviews of security policies and procedures. Feedback from staff and third-party security experts is also considered to ensure a comprehensive evaluation, helping continuously improve security measures.