Independent Security Risk Assessment (SRA) Report for ScribeBerry

I. Executive Summary

Overview of Assessment

This Security Risk Assessment for ScribeBerry was conducted with a focus on robust security measures and practices surrounding the handling of Electronic Protected Health Information (ePHI). The assessment was meticulously carried out using methodologies, including comprehensive system analyses, interviews with key personnel, and questionnaires and communication in regards to technologies utilized

Key Strengths and Findings

- Advanced Data Protection: The assessment identified that ScribeBerry's encryption protocols for ePHI, both at rest and in transit, are advanced, meeting industry standards. Utilizing current industry leading encryption algorithms ensures maximum security of sensitive health data.

- Dependable Third-Party Management: Scribeberry maintains partnerships with third-party vendors, especially with Microsoft Azure, and are fortified with stringent Business Associate Agreements (BAAs) and regular security audits. These measures have consistently demonstrated reliability and compliance with HIPAA regulations, along with a PIA for PIPEDA and Canadian Healthcare compliance

- Internal Access Controls: ScribeBerry's internal policies for access control were found to be above average. There is a role-based access system, coupled with continuous monitoring and regular reviews, which ensures that only authorized personnel have access to critical systems and ePHI.

- Incident Response and Management: The company's incident response plan is comprehensive and well-practiced, showcasing a preparedness for potential cybersecurity threats. Regular mock sessions have been reportedly carried out - which contribute to a proactive stance on incident management.

- Compliance with HIPAA + PIPEDA + Provincial Healthcare Privacy laws: ScribeBerry exhibits adherence to current privacy standards across the board in the USA and Canada with practices and policies regularly updated to align with the latest regulatory changes. The proactive approach to compliance has been at the forefront of the current AI scribe industry. Scribeberry is one of the only companies to undergo a SRA and review.

Risk Prioritization and Management

The assessment confirmed that the current risk level to ScribeBerry’s ePHI and overall data security is **significantly low.** The few identified risks were mainly associated with potential enhancements in emerging cybersecurity technologies and further fortifying the already strong incident response mechanisms.

Recommendations

Based on the assessment, we recommend continued investment in emerging security technologies and ongoing staff training in advanced cybersecurity awareness. These steps will ensure that ScribeBerry not only maintains its current high standards of data security but also stays ahead in the evolving landscape of cybersecurity threats.

Conclusion

ScribeBerry meets the industry standard for ePHI security and HIPAA/PIPEDA and provincial healthcare compliance. They have shown commitment to continuous improvement in their security posture and they demonstrate adherence to the current standards of data protection.

II. Introduction

Purpose of the Assessment

This Security Risk Assessment (SRA) has been independently conducted by Ingrid Ruys, a renowned Alberta based privacy expert. The primary objective of this assessment is to evaluate ScribeBerry's security infrastructure, policies, and practices, particularly in the handling and protection of Electronic Protected Health Information (ePHI). The goal is to determine ScribeBerry’s compliance with industry standards and regulatory requirements, notably the Health Insurance Portability and Accountability Act (HIPAA) and PIPEDA

Methodology

The methodology adopted for this SRA encompasses a blend of qualitative and quantitative analysis techniques, ensuring a comprehensive evaluation of ScribeBerry's security posture. Key elements of our methodology include:

- System and Network Analysis: A review of ScribeBerry's IT infrastructure descriptions to identify potential vulnerabilities.
- Policy and Procedure Review: Assessment of ScribeBerry's internal security policies, procedures, and practices.
- Compliance Checks: Evaluation of ScribeBerry's alignment with HIPAA standards, PIPEDA, and other relevant regulations.

- Stakeholder Interviews: Discussions with key personnel at ScribeBerry to understand operational practices and security awareness.
- Vulnerability Scanning: Utilization of expertise to detect any potential weaknesses in ScribeBerry's systems.

Scope of the Assessment

The scope of this SRA covers all aspects of ScribeBerry's operations that pertain to the security and privacy of ePHI. This includes, but is not limited to:

- Data Encryption and Protection: Review of the mechanisms in place for encrypting and protecting ePHI.
- Access Control Systems: Examination of the procedures and technologies used to control access to sensitive data and systems.
- Incident Response Protocols: Analysis of the effectiveness of ScribeBerry's incident response strategies.
- Employee Training and Awareness Programs: Evaluation of the training provided to staff regarding data security and privacy.
- Third-Party Vendor Management: Assessment of the processes in place for managing and monitoring third-party vendors who have access to or handle ePHI.

Assessment Rationale

This assessment is conducted to provide an unbiased evaluation of ScribeBerry's adherence to industry best practices and compliance with legal and regulatory requirements. As data security and privacy are paramount in the healthcare industry, this SRA aims to assure stakeholders, including clients and regulatory bodies, of ScribeBerry's commitment to maintaining the highest standards of ePHI security.

III. Regulatory Compliance Overview

Purpose of the Compliance Overview

This section provides an overview of ScribeBerry's compliance with various regulatory standards, with a particular focus on the Health Insurance Portability and Accountability Act (HIPAA), the Personal Information Protection and Electronic Documents Act (PIPEDA), and Provincial Healthcare Privacy Regulations. This assessment is aimed at verifying ScribeBerry's adherence to these regulations and ensuring its alignment with industry best practices in data privacy and security.

Areas Reviewed

HIPAA Compliance

- Adherence to HIPAA Rules: Evaluates ScribeBerry's compliance with the Privacy, Security, and Breach Notification Rules under HIPAA.
- Risk Management Protocols: Analyzes the effectiveness of ScribeBerry's risk management strategies in safeguarding ePHI.
- Staff Training and Awareness: Assesses the quality and comprehensiveness of HIPAA training programs for employees.

PIPEDA Compliance

- Consent and Individual Rights: Reviews ScribeBerry's protocols, terms and services, and privacy policy for its users to obtain consent for the collection, use, and disclosure of personal health information and respecting the rights of individuals as per PIPEDA.
- Data Protection Measures: Examines the security measures in place to protect personal information, particularly ePHI, in compliance with PIPEDA's requirements.
- Accountability and Transparency: Assesses the mechanisms ScribeBerry uses to ensure accountability in its data handling processes and transparency in its privacy policies.

Provincial Healthcare Privacy Regulation

- Alignment with Provincial Laws: Evaluates how ScribeBerry adheres to specific healthcare privacy regulations that vary by province, ensuring comprehensive compliance across Canada.
- Localization of Privacy Practices: Analyzes the company's ability to tailor its privacy practices to meet the unique requirements of each provincial healthcare system.
- Interaction with Provincial Health Records: Reviews procedures and safeguards surrounding the access and handling of provincial health records.

General Compliance Methodology

- Comprehensive Documentation Review: In-depth analysis of ScribeBerry's policy documents, compliance records, and operational procedures.
- Stakeholder Interviews: Written sessions with key ScribeBerry personnel to understand the practical application of compliance policies.
- Procedural Audit: Report based examination of IT infrastructure and data handling processes to ensure they meet regulatory standards.

Assessment Findings

- Strong Regulatory Compliance: ScribeBerry demonstrates robust compliance with HIPAA, PIPEDA, and Provincial Healthcare Privacy Regulations.
- Recommendations for Continued Improvement: While ScribeBerry meets current industry standards, continuous improvement and adaptation to emerging privacy and security challenges are recommended.

IV. Risk Identification

Objective of Risk Identification

This section outlines the key risks identified in ScribeBerry's operations, particularly in the context of ePHI management and cybersecurity. The risks are categorized based on their nature, and the sources of these risks are analyzed to provide a comprehensive understanding of potential vulnerabilities.

Categorization of Identified Risks

1. Technical Risks
   - System Vulnerabilities: Potential weaknesses in ScribeBerry's software or hardware that could be exploited by cyber threats.
   - Data Encryption and Transmission: Risks associated with the encryption protocols used during data transmission and storage.
   - Cloud Service Dependencies: Risks stemming from the reliance on third-party cloud service providers for data storage and processing.

2. Operational Risks
   - User Access Control: Risks related to the management of user access rights to sensitive systems and data.
   - Internal Process Gaps: Any deficiencies in internal procedures that could impact data security or compliance.
   - Incident Response Readiness: The effectiveness of existing plans and procedures to respond to security incidents.

3. Environmental Risks
   - Regulatory Changes: Risks arising from evolving compliance requirements in data protection and privacy laws.
   - Market Dynamics: Impact of industry trends and technological advancements on ScribeBerry's security posture.

Sources of Risk

- External Threats: Including cyber attacks such as phishing, malware, ransomware, and other forms of malicious activities aimed at compromising data security.
- Internal Processes: Potential risks arising from within ScribeBerry's operations, such as human error, inadequate training, or ineffective policy enforcement.
- Technology Vulnerabilities: Inherent risks associated with the use of technology, including software bugs, hardware failures, and inadequate security updates.
- Third-Party Interactions: Risks associated with the engagement of third-party vendors and partners, particularly concerning data sharing and handling.

This comprehensive identification of risks is crucial for ScribeBerry to understand and prepare for potential challenges to its data security and privacy practices. The identified risks will serve as a foundation for the subsequent risk analysis and mitigation strategies.

V. Risk Analysis

Purpose of Risk Analysis

In this section of the SRA, we delve into a detailed analysis of the risks identified in the previous section. Each risk is assessed for its likelihood of occurrence and potential impact on ScribeBerry, particularly in terms of data security, operational integrity, and compliance obligations. The analysis aims to prioritize these risks to guide ScribeBerry in focusing its mitigation efforts effectively.

Analysis and Prioritization of Risks

1. Technical Risks
   - System Vulnerabilities: Likelihood: Moderate; Impact: High. System vulnerabilities can lead to significant data breaches and loss of customer trust.
   - Data Encryption and Transmission: Likelihood: Low; Impact: Very High. Compromise in encryption can result in severe breaches of ePHI.
   - Cloud Service Dependencies: Likelihood: Low; Impact: High. Dependency on third-party cloud services introduces risks related to external control over data security.

2. Operational Risks
   - User Access Control: Likelihood: Moderate; Impact: High. Inadequate access controls can lead to unauthorized access to sensitive data.
   - Internal Process Gaps: Likelihood: Moderate; Impact: Moderate. Process gaps may lead to inefficiencies and potential security oversights.
   - Incident Response Readiness: Likelihood: Low; Impact: Very High. Ineffective incident response can exacerbate the consequences of security incidents.

3. Environmental Risks
   - Regulatory Changes: Likelihood: High; Impact: High. Failure to adapt to new regulations can result in compliance violations and legal repercussions.
   - Market Dynamics: Likelihood: Moderate; Impact: Moderate. Changes in the industry landscape can pose challenges to maintaining a competitive and secure edge.

Risk Severity and Impact Assessment

- High Priority Risks: Include Data Encryption and Transmission, Incident Response Readiness, and Regulatory Changes due to their potential to cause significant disruption, loss, and damage.

- Moderate Priority Risks: System Vulnerabilities, User Access Control, and Market Dynamics are categorized as moderate risks requiring vigilant monitoring and robust control measures.
- Lower Priority Risks: Cloud Service Dependencies and Internal Process Gaps, while important, pose less immediate threats and can be managed with standard risk mitigation strategies.

This risk analysis provides ScribeBerry with a clear understanding of the most significant risks facing the organization. It forms the basis for developing a targeted risk mitigation plan, focusing resources on the areas of highest priority and impact.

VI. Current Security Posture

Objective of Security Posture Assessment

This section aims to provide an overview of ScribeBerry's existing security measures and controls. The assessment evaluates the effectiveness of these practices in safeguarding Electronic Protected Health Information (ePHI) and maintaining compliance with industry standards and regulatory requirements.

Overview of Existing Security Measures

1. Data Encryption and Protection: ScribeBerry employs advanced encryption techniques for data at rest and in transit. This includes industry-standard encryption protocols to secure ePHI from unauthorized access.

2. Access Control Systems: Robust access control measures are in place, involving google based multi-factor authentication, role-based access, and regular reviews of user access rights.

3. Incident Response Plan: A comprehensive incident response plan is established, detailing protocols for handling and mitigating security breaches

4. Compliance Management: Rigorous processes are in place for ensuring compliance with HIPAA, PIPEDA, and other relevant regulations. This includes continuous monitoring and updating of policies to align with regulatory changes.

5. Third-Party Vendor Management: Stringent measures are adopted for managing third-party vendors, including regular security assessments and ensuring compliance through Business Associate Agreements (BAAs).

Assessment of Security Practice Effectiveness

- Data Security: ScribeBerry's data encryption and protection measures are highly effective, providing a solid defense against data breaches and unauthorized access.

- Access Control: The existing access control systems are robust, significantly reducing the risk of internal and external unauthorized access to sensitive systems and data.

- Incident Response: The incident response capabilities of ScribeBerry are well-structured and effectively mitigate the impact of security incidents, ensuring a swift return to normal operations.

- Regulatory Compliance: ScribeBerry demonstrates strong compliance with healthcare data protection regulations. Ongoing efforts to stay abreast of regulatory changes further enhance this posture.

- Vendor Risk Management: The processes for managing third-party vendors are thorough and align with best practices, minimizing risks associated with external entities.

Conclusion

ScribeBerry's current security posture is robust and aligns well with industry best practices and regulatory requirements. The organization has implemented a comprehensive range of security measures that effectively address various cybersecurity challenges. Continuous improvement and adaptation to emerging threats and regulatory changes are recommended to maintain this strong security stance.

VII. Risk Mitigation Strategies

Purpose of Risk Mitigation Strategies

This section outlines strategic recommendations for mitigating the identified risks in ScribeBerry's operations. The suggested strategies are designed to address both short-term and long-term risks, enhancing the overall security posture and compliance of ScribeBerry.

Recommendations for Mitigating Identified Risks

1. Enhanced Data Encryption Protocols
   - Short-Term: Ongoing review and strengthening of existing encryption protocols, especially for data in transit.
   - Long-Term: Continuous evaluation and implementation of advanced encryption technologies as they become available.

2. Robust Third-Party Vendor Management
   - Short-Term: Conduct thorough security assessments of all third-party vendors and update BAAs to include stringent security requirements. - Completed
   - Long-Term: Establish a regular audit and review process for third-party vendors to ensure ongoing compliance and security alignment - In progress

3. Advanced Access Control Measures

- Short-Term: Implement additional layers of access controls, including more stringent multi-factor authentication methods for end users - In progress
- Long-Term: Invest in sophisticated access management systems that utilize AI and machine learning for predictive risk analysis and adaptive authentication.

4. Refined Incident Response Protocols
   - Short-Term: None
   - Long-Term: Develop a comprehensive incident response simulation drill and program for continuous staff preparedness.

5. Proactive Regulatory Compliance Updates
   - Short-Term: None
   - Long-Term: Establish a dedicated regulatory compliance team responsible for staying ahead of legislative developments and integrating them into company policies.

6. Continuous Employee Training and Awareness Programs
   - Short-Term: None
   - Long-Term: Develop an ongoing cybersecurity education program with regular updates, assessments, and certifications.

The implementation of these risk mitigation strategies can help augment ScribeBerry's current practice to address current vulnerabilities and strengthen its defense against future cybersecurity challenges. While these are suggestions, Scribeberry in its current format remains privacy compliant

VIII. Implementation Plan

Purpose of the Implementation Plan

This section provides a detailed action plan for implementing the risk mitigation strategies recommended in the previous section. It includes specific responsibilities assigned to ScribeBerry team members and realistic timelines for each action, ensuring effective execution and monitoring.

Detailed Action Plan

1. Enhanced Data Encryption Protocols
   - Action: Continuous review of encryption protocols for data in transit.
   - Responsibility: IT Security Team/Amaan Rattansi
   - Timeline: Every 3 months, followed by ongoing updates as needed.

2. Robust Third-Party Vendor Management

- Action: Perform security assessments of all third-party vendors and update BAAs.
- Responsibility: Compliance Officer Dr Zaahir Moloo
- Timeline: Initial assessments and updates within 6 months, with semi-annual reviews thereafter.

3. Advanced Access Control Measures
   - Action: Introduce advanced multi-factor authentication and adaptive access controls.
   - Responsibility: Organizational
   - Timeline: Implementation within 6 months, ongoing evaluation and adjustments as needed.

4. Refined Incident Response Protocols
   - Action: Review and update incident response plan; conduct staff simulations.
   - Responsibility: Organizational
   - Timeline: Plan update within 3 months; biannual drills and training thereafter.

5. Proactive Regulatory Compliance Updates
   - Action: Establish a dedicated team for regulatory monitoring and policy integration.
   - Responsibility: Compliance Officer and perhaps a newly formed Regulatory Compliance Team
   - Timeline: Team formation within 1 month; ongoing regulatory monitoring and quarterly policy reviews.

6. Continuous Employee Training and Awareness Programs
   - Action: Launch a comprehensive cybersecurity education program.
   - Responsibility: Organizational
   - Timeline: Initial rollout within 1 year, with annual updates and annual certifications.

Monitoring and Evaluation

- Each phase of the implementation will be closely monitored and overseen by senior management.
- Regular progress reports can be requested to evaluate the effectiveness of the implemented measures and make adjustments as necessary.

IX. Compliance Considerations

Purpose of Compliance Considerations

This section provides a comprehensive analysis of how the identified risks and proposed mitigation strategies align with regulatory requirements, particularly HIPAA and PIPEDA. The focus is on ensuring that ScribeBerry's risk management approach is effective in addressing security concerns and also in maintaining compliance with legal standards.

Analysis of Risk Alignment with Regulatory Requirements

1. Data Encryption and Protection Compliance: The enhanced data encryption protocols recommended align with HIPAA's requirements for safeguarding ePHI. This measure supports compliance with the Security Rule's standards for transmission security and data at rest.

2. Third-Party Vendor Management and HIPAA Compliance: Strengthening third-party vendor management, including updated BAAs, ensures adherence to HIPAA's Business Associate requirements, providing a robust framework for data sharing and processing. PIPEDA is also addressed through a PIA through Scribeberry as well as through Microsoft's cloud services

3. Access Control Measures and HIPAA Standards: The implementation of advanced access control measures addresses the HIPAA Security Rule's requirements for administrative, physical, and technical safeguards.

4. Incident Response Planning and Breach Notification Compliance: Refining incident response protocols supports compliance with HIPAA's Breach Notification Rule, ensuring timely and effective responses to potential data breaches.

5. Regulatory Compliance Team and Ongoing HIPAA Alignment: Establishing a dedicated regulatory compliance team helps in continuously aligning ScribeBerry's practices with evolving HIPAA regulations and other relevant laws.

<u>Documentation of Compliance-Related Considerations</u>

- Policy and Procedure Documentation: Ensuring that all policies and procedures updated or created in response to the SRA are thoroughly documented and accessible for review.
- Training Records: Maintaining detailed records of all compliance training sessions, particularly those related to HIPAA, to demonstrate the organization's commitment to compliance education.
- BAAs and Vendor Agreements: Keeping updated records of all Business Associate Agreements and vendor contracts, including any modifications made post-SRA.
- Compliance Monitoring Reports: Regular generation of compliance monitoring reports

<u>Conclusion</u>

The alignment of ScribeBerry's risk mitigation strategies with regulatory requirements is a critical component of the organization's overall security and compliance strategy.

X. Training and Awareness

<u>Recommendations for Employee Training and Awareness Programs</u>

1. Comprehensive Cybersecurity Training: Implement an annual mandatory training program covering cybersecurity best practices, HIPAA/PIPEDA compliance, and handling of ePHI.

2. Regular Security Updates: Monthly briefings on the latest security threats and trends to keep staff informed and vigilant.

3. Simulated Security Drills: security drills simulating different threat scenarios to assess and improve the response capabilities of staff.

Plan for Regular Updates and Reinforcement of Security Practices

- Ongoing Learning Platform: Consider utilizing an e-learning platform for continuous education and updates on security practices.
- Feedback Mechanism: Refine the system for employees to report potential security concerns and receive timely feedback.

XI. Monitoring and Review

Strategy for Ongoing Monitoring of Risks and Effectiveness of Implemented Controls

- Continuous Risk Assessment Tools: Use automated tools for real-time monitoring of system vulnerabilities and threat detection.
- Performance Metrics: Develop metrics to measure the effectiveness of implemented security controls.

Schedule for Regular Review and Update of the SRA

- Annual SRA Review: Conduct a comprehensive review of the SRA annually to ensure it remains relevant and effective.
- Ad-Hoc Reviews: Perform ad-hoc reviews in response to significant changes in the threat landscape or operational environment.

XII. Conclusions

Summary of the SRA Process and Key Outcomes

- The SRA process provided a thorough evaluation of ScribeBerry's security posture, identifying key risks and areas for improvement.
- The implementation of recommended strategies while not required, but can be expected to significantly enhance ScribeBerry's security framework. Scribeberry is privacy compliant in its current format

Overall Assessment of ScribeBerry's Risk Environment and Security Posture

- ScribeBerry possesses a strong security posture with effective measures in place to protect ePHI.

- Continued vigilance and adaptation to emerging threats are necessary to maintain and improve this posture.

XIII. Appendices

Relevant Documentation:
Anthropic BAA
Azure Canada Privacy Laws
Azure Foundational PIA
Microsoft Data Processing
HIPAA Questionnaire - Dashboard Summary
Azure Compliance Offerings
Azure BAA
Privacy Policy Scribeberry
Scribeberry Notice of Privacy Policies
Comprehensive Scribeberry Guide (PIA)
Scribeberry PIA Amendment
Scribeberry Contingency Plan
Scribeberry HIPAA Sanctions Plan
HIPAA Compliance Program for Scribeberry
Terms and Conditions for Scribeberry

Final Words

As we conclude this Security Risk Assessment for ScribeBerry, it is evident that the organization maintains a robust and proactive approach towards data security and regulatory compliance. The assessment has highlighted areas of strength as well as opportunities for further enhancement. Implementing the recommended strategies can augment ScribeBerry’s security posture against evolving cyber threats and ensure continued adherence to industry best practices and regulatory standards.

Ingrid Ruys
Privacy Auditor
Date: 14 Jan 2024