Sangoma Technologies Corporation
HIPAA Security Rule Assessment

Prepared By: Amy Baker
Date: May 3, 2023

Table of Contents

Sensitive Information Warning

This document contains confidential information and sensitive information about the security posture of Sangoma Technologies Corporation and its wholly owned subsidiaries, DBA Sangoma Technologies Corporation, henceforth Sangoma Technologies.

This document should be classified at Sangoma Technologies Corporation highest proprietary information classification level.

Only those individuals that have a valid "**need to know**" should be allowed access to this document.

About VikingCloud

Headquartered in Chicago, Illinois, VikingCloud, Inc. (henceforth “VikingCloud”) is a highly respected, trusted compliance and leading security provider. The VikingCloud compliance and security services are designed to meet the unique needs of small to mid-sized healthcare entities and the providers that serve them. The company’s flexible solutions and services, easy-to-use online tools, and personalized support significantly simplify compliance and security for Sangoma Technologies Corporation.

The VikingCloud security team members hold many advanced industry certifications (e.g., CISSP, CISA, CISM) that uniquely position them to serve entities compliance and security needs.

Entities that carry out health care activities and functions, as well as the business associates that are required to comply with the HIPAA Rules may utilize the VikingCloud services listed below.

VikingCloud Healthcare Services

+ Advanced Managed Security Services & Security Consulting
+ HIPAA Gap Analysis
+ HIPAA Remediation Assistance
+ HIPAA Security Rule Analysis
+ Security Awareness Training
+ IT Risk Assessment
+ Application and Network Layer Penetration Testing
+ Web Application Security Testing
+ Internal Vulnerability Scanning
+ External Vulnerability Scanning
+ Advanced Endpoint Protection
+ Social Engineering
+ Log Management and Monitoring

Executive Summary

HIPAA Engagement Overview

Sangoma Technologies Corporation (Sangoma Technologies) contracted with VikingCloud to perform a HIPAA Risk Assessment of the systems and facilities that store, process, and transmit Electronic Protected Health Information (ePHI). The HIPAA Risk Assessment process solely focuses on the security of ePHI data, whether Sangoma Technologies has effectively implemented information security policies and processes, and if there are adequate security measures to comply with the requirements to protect ePHI. Additionally, the Risk Assessment reviews whether Sangoma Technologies is utilizing industry best-practices, which includes recommendations for remediation of any non-compliant items (policies, processes, procedures, system configurations or vulnerabilities). This is *only* a risk assessment and does *not* include professional services for remediation efforts.

Completing the HIPAA compliance assessment constitutes the initial step for an organization to follow HIPAA regulations. The recommendations in this report provide Sangoma Technologies compliance group with a framework to develop the necessary policies, procedures, and security measures that will permit Sangoma Technologies to be compliant with HIPAA regulations. Once it is determined where Sangoma Technologies needs to improve, the risk analysis standard is usually met by completing an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity.

As with any assessment, this project provides a snapshot of Sangoma Technologies at a given point in time. Changes in technology, process, or organization may alter the IT environment and affect portions of this assessment.

The findings and recommendations in this report should heighten Sangoma Technologies awareness of their overall information security environment. VikingCloud's recommendations are based upon a detailed understanding of the team's current business needs. The effective implementation of the recommended security controls will aid in the prevention of unauthorized, accidental, or deliberate disruption, disclosure, modification, and use of Sangoma Technologies assets. The implementation of any recommendations contained herein is strictly voluntary and solely at Sangoma Technologies' discretion.

Business Overview

Sangoma Technologies provides telecommunications and internet routing services to its health customers. Sangoma Technologies does not store, process, but does transmit “Electronic Protected Health Information” (ePHI) for their customers. Sangoma Technologies provides the communications interface between complying merchants and service providers and their health institutions or other intermediaries as an Infrastructure as a Service (IaaS) service provider. Sangoma Technologies seeks to establish the compliance of its routing and transmission infrastructure only. The employees of Sangoma Technologies do not interact with health information in any aspect of management of these environments. Sangoma Technologies has a role of network provider, which means that it has no responsibility for ePHI that its customers could potentially traverse its network. Its access to network devices could impact the security of an ePHI environment if its customers are using the network for ePHI transmissions. As a result, Sangoma Technologies is potentially responsible for security of ePHI as a network transport provider.

Sangoma Technologies Corporation has the following office location(s):
Corporate Headquarters #1:
Sangoma Technologies Inc.
100 Renfrew Drive, Suite 100
Markham, ON, CA L3R 9R6

Corporate Headquarters #2:
Sangoma US Inc.
301 N Cattlemen Road, Suite 300
Sarasota, FL, USA, 34232

HIPAA Security Rule

To improve the efficiency and effectiveness of the healthcare system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted. The HIPAA Act included Administrative Simplification provisions that required U.S. Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and

code sets, unique health identifiers, and security. The Security Rule was published by HHS in February of 2003 and had a final compliance deadline of April 2005.

The HIPAA Security Rule specifically focuses on the provisions for protecting ePHI through the implementation of the Administrative, Physical, and Technical Safeguards. In general, the standards, requirements, and implementation specifications of HIPAA apply to all organizations defined by HIPAA as a Covered Entity, Hybrid Entity, Business Associate, or Subcontractor.

At a summary level, Sangoma Technologies identifies as a Business Associate and is required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule; and,
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures
- Documentation Requirements

The federal regulations are published in the Code of Federal Regulations (CFR) - 45 C.F.R. Part 160, Part 162, and Part 164.

HITECH ACT

Under the HITECH Act, the legal liability associated with non-compliance is increased. Furthermore, proactive, and reactive enforcement by the Office for Civil Rights (OCR) is increased through the issuance of fines, penalties, and compliance audits. The HIPAA Omnibus Rule of

2013 extends the compliance requirements to downstream vendors (“Subcontractors”) who create, receive, maintain, or transmit ePHI on behalf of Covered Entities or Business Associates. The IT security-related requirements defined by the HITECH Act and the Omnibus Rule include:

- Timeliness of Notification
- Methods of Notice
- Content of Notification
- Breach Notification Procedures

HIPAA Security Rule - Required vs Addressable.

While the Administrative, Physical, and Technical Safeguards identified under HIPAA are mandatory, their implementation may differ based on the type of requirement. Under the HIPAA Security Rule, Standards and Implementation Specifications are classified as either “Required” or “Addressable”. It is important to note that neither of these classifications should be interpreted as “optional”. An explanation of each is provided below:

- **Required (R)** – Implementation specifications identified as “Required” must be fully implemented by the covered organization. Furthermore, all HIPAA Security Rule requirements identified as “Standards” are classified as “Required”.
- **Addressable (A)** – The concept of an “Addressable” implementation specification was developed to provide covered organizations flexibility with respect to how the requirement could be satisfied. To meet the requirements of an addressable specification, a covered organization must: (a) implement the addressable implementation specification as defined; (b) implement one or more alternative security measures to accomplish the same purpose; or (c) not implement either an addressable implementation specification or an alternative. Where the organization chooses an alternative control or determines that a reasonable and appropriate alternative is not available, the organization must fully document their decision and reasoning. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

Environmental Analysis

Sangoma Technologies Corporation Contact Information

This HIPAA Security Rule assessment was performed predominantly through the following Sangoma Technologies Corporation point of contacts:

Name	Title	Email	Phone
Eric Krichbaum	Information Security Officer	ekrichbaum@sangoma.com	+1 (415)-287-1246

Information Gathering

The VikingCloud assessor performed the HIPAA assessment via remote Microsoft Teams screensharing and data collection tools. The VikingCloud assessor took all necessary steps to ensure the integrity of the assessment was not negatively impacted by ensuring that all people, processes, and technologies examined were the same as if the HIPAA assessor were onsite. The methods utilized for observing implementations and collecting evidence provided the same level of assurance as for an onsite assessment.

This HIPAA assessment was conducted remotely via Microsoft Teams with Sangoma Technologies staff March 23, 2023 – May 1, 2023. Sangoma Technologies engaged security, infrastructure, developers, administrative, and operations personnel, and third-party service providers as required, to answer questions and provide supporting artifacts.

Documentation Reviewed

The Sangoma Technologies policies and procedures, and supporting evidence provided throughout the course of the engagement were reviewed during the assessment and prior to the issuance of this report. VikingCloud's secure online portal, Asgard, was used as a document repository for this assessment.

Assessment Methodology

The VikingCloud methodology for performing HIPAA assessments is based on established and repeatable assessment frameworks compiled from the Office of Civil Rights (OCR) Audit Protocol, and the National Institute of Standards and Technology (NIST). Specifically, NIST 800-66 serves as the de facto standard for directing organizations on the typical activities that should be considered when pursuing HIPAA compliance as part of an overarching information security program. The "Introductory Resource Guide for Implementing the HIPAA Security Rule", as well as numerous other NIST special publications, have been supported and referenced by the OCR as viable interpretations and guidance for achieving HIPAA compliance.

While the NIST special publications are largely aimed at federal agencies, the HITRUST Common Security Framework (CSF) was developed specifically for the healthcare industry through

collaboration with healthcare, business, technology, and information security professionals. The framework was developed to assist healthcare organizations, including Covered Entities and Business Associates, in identifying the obstacles and problematic areas within the confines of protecting patient information and streamlining effective security controls.

Specific to Sangoma Technologies, VikingCloud primarily leveraged the OCR Audit Protocol, in addition to the NIST 800-66, to perform a comprehensive HIPAA Security Rule Assessment.

Key Activities

Below are the key activities performed by VikingCloud for Sangoma Technologies 2023 HIPAA Security Rule assessment:

- Performed an environment characterization to understand the uses and flows of ePHI throughout the organization.
- Reviewed policies and procedures to identify compliance gaps.
- Reviewed the design of controls in place to satisfy the IT security-related requirements of HIPAA, HITECH, and the Omnibus Rule.
- Performed detailed control analysis and testing for the purpose of understanding the level of operating effectiveness.
- Provided detailed assessment results outlining the organization's HIPAA compliance posture, as well as areas for remediation.

Electronic Protected Health Information Data Flows: (Network Overview)

The network topology for Sangoma Technologies is a Juniper switched configuration with redundant storage for failover capability and no single point of failure. The core network connections are MPLS private circuits with each network node configured with Cisco routers. Firewall connections are protected using high-availability Fortinet FortiGate firewalls.

These Fortinet FortiGate firewalls, Juniper switches and Cisco routers are used to provide a fully segmented environment for Sangoma Technologies customers. Syslog centralized logging is used and Logwatch is used to log any potential incident of unauthorized access and alert appropriate personnel. Change management to these firewalls and routers is tracked using FieldPoint Advanced Service Management.

Segmentation is implemented using router ACL (Access Control Lists) and firewall rules sets under control of Sangoma Technologies to create a strict separation between customer networks and Sangoma Technologies administrative network employee access.

Segmentation is provided by Cisco 7606-S, Cisco 7609-S, Cisco ASR, and Cisco 7606 routers. Traffic is limited by FortiNet FortiGate 1000-D and 1500-D firewalls to only defined IP ranges in these networks. All devices are managed using Sangoma Technologies approved and deployed hardened images. These images are based off SANS and Cisco best-practices guidance. Traffic is monitored by OSSEC host-based IDS running on the Fedora Linux hosts and alerts are generated by Logwatch for any traffic that is outside defined parameters. Authentication is provided by TACACS+ managed by Sangoma Technologies for their devices, which are accessed using OpenSSH for a secure remote connection.

A Guest wireless network is provided at the corporate office using a dedicated VLAN segment. Remote access through a VPN (Virtual Private Network) requires two-factor authentication (MFA) and is managed by an ACL for authorized users.

User accounts are managed with Microsoft Active Directory, group permissions are required for any access to the ePHI data based on job role.

Summarized Findings

Detailed findings will be found in the HIPAA Security Rule - Detailed Findings section of this report. Below is a high-level summary of the HIPAA Security Rule compliance status as demonstrated by Sangoma Technologies:

The objective of this engagement was to review, analyze, and document the Sangoma Technologies application, services, and environment, as well as its compliance efforts specific to HIPAA/HITECH. Based upon a gap analysis exercise, examination of the in-scope ePHI environments, detailed control testing, and Sangoma Technologies interviews, the VikingCloud assessor has determined that Sangoma Technologies has successfully demonstrated adherence and compliance with the HIPAA Security Rule compliance program.

HIPAA Security Rule – Detailed Findings

Sangoma Technologies does not differentiate between incidental ePHI and other data received through its services, and all controls in place for §164.306 through §164.316 which apply to all Sangoma Technologies data within the environment, without preference or recognition of the presence of ePHI (except where otherwise noted).

The following sections outline Sangoma Technologies overall adherence to each HIPAA Standard based on interviews with Sangoma Technologies personnel, as well as by observation of systems and processes used in the ePHI environment.

HIPAA Breach Notification Rule – Detailed Findings

The HIPAA Breach Notification Rule does not apply to Sangoma Technologies. Sangoma Technologies does not have knowledge of any ePHI stored within its environment. All identification and notification of breach by covered entities identifies as a Business Associate.

Sangoma Technologies does not provide healthcare services directly to individuals and is not classified as a HIPAA Covered Entity. Adherence to this rule for data deemed to contain ePHI, therefore, is the responsibility of Sangoma Technologies who may be Covered Entities or Business Associates insofar as any such data are concerned.

To aid in compliance to these rules, the following section outlines Sangoma Technologies overall adherence to HIPAA Standard for Breach Notification for any breach of Sangoma Technologies data. The conclusions below are based on interviews with Sangoma Technologies, as well as by observation of systems and processes used in the ePHI environment.

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.306 – Security Standards: General Rules					
§164.306(a) – General Requirements	Does the covered entity or business associate: 1. Ensure confidentiality, integrity, and availability of ePHI? 2. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI? 3. Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required by the Privacy Rule? 4. Ensure compliance with the Security Rule by its workforce?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.306(a) – General Requirements	Has the entity determined which security measures it implements? The covered entity or business associate should take into account the following factors. 1. Its size, complexity, and capabilities 2. Its technical infrastructure, hardware, and software security capabilities. 3. The costs of security measures 4. The probability and criticality of potential risks to ePHI.	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308 – Administrative Safeguards					
§164.308(a) – Security Management Process	Does the entity prevent, detect, contain, and correct security violations?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(1)(ii)(A) – Security Management Process – Risk Analysis	Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(1)(ii)(B) – Security Management Process – Risk Management	Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.308(a)(1)(ii)(C) – Security Management Process – Sanction Policy	Does the entity apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(1)(ii)(D) – Security Management Process – Information System Activity Review	Does the entity regularly review records of information system activity?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(2) – Assigned Security Responsibility	Has the entity identified the security official responsible for the development and implementation of the policies and procedures required by this subpart?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(3)(i) – Workforce Security	Does the entity ensure all members of its workforce have appropriate access to ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(3)(ii)(A) – Workforce security – Authorization and/or Supervision	Does the entity authorize and/or supervise workforce member who work with ePHI or in locations where it might be accessed?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(3)(ii)(B) Workforce security – Workforce Clearance Procedure	Does the entity determine whether a workforce member's access to ePHI is appropriate?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(3)(ii)(C) Workforce security – Establish Termination Procedures	Does the entity terminate access to ePHI when employment or other arrangements with the workforce member ends?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.308(a)(4)(i) – Information Access Management	Does the entity authorize access to ePHI that supports the applicable requirements of the Privacy Rule?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(4)(ii)(A) – Information Access Management -- Isolating Healthcare Clearinghouse Functions	Does the clearinghouse protect ePHI from unauthorized access by the larger organization?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(4)(ii)(B) – Information Access Management – Access Authorization	Does the entity grant access to ePHI for workforce members?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(4)(ii)(C) – Information Access Management – Access Establishment and Modification	Does the entity authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(5)(i) – Security Awareness and Training	Does the entity provide security awareness and training to all new and existing members of its workforce?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(5)(ii)(A) – Security Awareness and Training – Security Reminders	Does the entity appropriately communicate security updates to all members of its workforce and, if appropriate, contractors periodically?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.308(a)(5)(ii)(B) – Security Awareness, Training, and Tools – Protection from Malicious Software	Does the entity have policies and procedures in place regarding a process to incorporate its procedures to guard against, detect, and report malicious software into its security awareness and training program?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(5)(ii)(C) – Security Awareness, Training, and Tools – Log-in Monitoring	Does the entity have policies and procedures in place to incorporate procedures for monitoring log-in attempts and reporting discrepancies into its security awareness and training program?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(5)(ii)(D) – Security Awareness, Training, and Tools – Password Management	Does the entity have policies and procedures in place to incorporate procedures for creating, changing, and safeguarding passwords into its security awareness and training program?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(6)(i) – Security Incident Procedures	Does the entity have policies and procedures in place to address security incidents?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(6)(ii) – Security Incident Procedures – Response and Reporting	Does the entity identify, respond to, report, and mitigate security incidents?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.308(a)(7)(i) – Contingency Plan	Does the entity have a contingency plan for responding to an emergency or other occurrences that damages systems that contain ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(7)(ii)(A) – Contingency Plan – Data Backup Plan	Does the entity create and maintain retrievable exact copies of ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(7)(ii)(B) Contingency Plan – Disaster Recovery Plan	Does the entity restore any lost data?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(7)(ii)(C) Contingency Plan – Emergency Mode Operation Plan	Does the entity enable the continuity of critical business processes for the protection of ePHI while operating in emergency mode?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(7)(ii)(D) Contingency Plan – Testing and Revision Procedure	Does the entity periodically test and revise its contingency plans?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(7)(ii)(A) Contingency Plan – Application and Data Criticality Analysis	Does the entity assess the relative criticality of specific application and data in support of other contingency plan components?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(a)(8) – Evaluation (R)	Does the entity perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.308(b)(1) – Business Associate Contracts and Other Arrangements (R)	Does the entity have policies and procedures in place to obtain satisfactory assurances from its business associates (or business associate subcontractors if entity is a business associate) and to review the satisfactory assurances to ensure the applicable requirements at § 164.314(a) are included in the business associate contract or other arrangement?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.308(b)(3) – Business Associate Contracts and Other Arrangements – Written Contract or Other Arrangement	Does the entity have policies and procedures in place to obtain satisfactory assurances from its business associates (or business associate subcontractors if entity is a business associate) and to review the satisfactory assurances to ensure the applicable requirements at § 164.314(a) is included in the written contract or other arrangement?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310 – Physical Safeguards					
§164.310(a)(1) – Facility Access Controls	Does the entity limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.310(a)(2)(i) – Facility Access Controls – Contingency Operations	Does the entity allow facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operation Plan in the event of an emergency?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(a)(2)(ii) – Facility Access Controls – Facility Security Plan	Does the entity safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(a)(2)(iii) – Facility Access Controls – Access Control and Validation Procedures	Does the entity control a person's access to facilities based on their role or function including visitor control and control of access to software programs for testing and revision?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(a)(2)(iv) – Facility Access Controls – Maintain Maintenance Records	Does the entity document repair and modifications to the physical components of a facility which are related to security?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(b) – Workstation Use	Does the entity specify the proper functions to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(c) Workstation Security	Does the entity workstations that access electronic protected health information restricted to authorized users?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.310(d)(1) – Device and Media Controls	Does the entity govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within facility?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(d)(2)(i) – Device and Media Controls – Disposal	Does the entity address the disposal of ePHI data, hardware, or electronic media on which it is stored?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(d)(2)(ii) – Device and Media Controls – Media Re-use	Does the entity remove ePHI before reusing electronic media and who is responsible for the overseeing those processes?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(d)(2)(iii) – Device and Media Controls – Accountability	Does the entity record the movements of hardware and electronic media and any person responsible therefore?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.310(d)(2)(iv) – Device and Media Controls – Data Backup and Storage Procedures	Does the entity create retrievable, exact copy of ePHI when needed, before movement of equipment?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312 – Technical Safeguards					
§164.312(a)(1) – Access Control	Does the entity only allow access to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) to electronic information systems that maintain ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.312(a)(2)(i) – Access Control – Unique User Identification	Does the entity assign unique user IDs to track user identity?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(a)(2)(ii) – Access Control – Emergency Access Procedure	Does the entity provide access to ePHI during an emergency?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(a)(2)(iii) – Access Control – Automatic Logoff	Does the entity automatically terminate all electronic sessions after a predetermined time of inactivity?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(a)(2)(iv) – Access Control – Encryption and Decryption	Does the entity encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(b) – Audit Controls	Does the entity have hardware, software and/or procedural mechanism to record and examine activity in information systems that contain or use ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(c)(1) – Integrity	Does the entity protect ePHI form improper alteration or destruction?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(c)(2) – Integrity – Mechanism to Authenticate ePHI	Does the entity have electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(d) – Person or Entity Authentication	Does the entity verify that a person or entity seeking access to ePHI is the individual claimed?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.312(e)(1) – Transmission	Does the entity have security controls to guard against unauthorized access to ePHI transmitted over electronic communications networks?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(e)(2)(i) – Transmission Security – Integrity Controls	Does the entity have policies and procedures in place to implement security measures to ensure that electronically transmitted ePHI cannot be improperly modified without detection until disposed of?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.312(e)(2)(ii) – Transmission Security – Encryption	Does the entity have encryption mechanism to encrypt ePHI whenever deemed?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314 – Organizational Requirements					
§164.314(a) – Business associate contracts	Does the entity have policies and procedures in place requiring that its business associate contracts, or other arrangements require that subcontractors that create, receive, maintain, or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.314(a)(2)(i)(A) – Business associate Contracts	Does the entity have policies and procedures in place requiring that its business associate contracts, or other arrangements require that subcontractors that create, receive, maintain, or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314(a)(2)(i)(B) – Business associate Contracts	Does the entity have policies and procedures in place requiring that its business associate contracts, or other arrangements require that subcontractors that create, receive, maintain, or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.314(a)(2)(i)(C) – Business associate Contracts	Does the entity have policies and procedures in place requiring that its business associate contracts, or other arrangements require that subcontractors that create, receive, maintain, or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314(a)(2)(ii) – Other arrangements	Does the entity have policies and procedures in place requiring that its business associate contracts, or other arrangements require that subcontractors that create, receive, maintain, or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.314(a)(2)(iii) – Business associate contracts with subcontractors	Does the entity have policies and procedures in place requiring that its business associate contracts, or other arrangements require that subcontractors that create, receive, maintain, or transmit ePHI on behalf of its business associates agree to comply with the applicable parts of Subpart C of 45 CFR Part 164 by entering into a business associate contract or other arrangement that complies with 45 CFR § 164.314(a)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314(b)(1) – Requirements for group health plans	Specific exceptions to this requirement are provided when the only ePHI disclosed to a plan sponsor is disclosed pursuant to permitted disclosures under the HIPAA Privacy Rule, specifically § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508. The standard includes the following required implementation specifications:	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314(b)(2)(i) – Group health plans implementation and specification	Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.314(b)(2)(ii) – Group health plans implementation and specification	Ensure that the adequate separation required by § 164.504(f)(2)(iii) [of the Privacy Rule] is supported by reasonable and appropriate security measures;	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314(b)(2)(iii) – Group health plans implementation and specification	Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information;	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.314(b)(2)(iv) – Group health plans implementation and specification	Report to the group health plan any security incident of which it becomes aware.	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.316 – Policies and Procedures					
§164.316(a) – Policies and Procedures	Does the entity have policies and procedures in place requiring the said entity to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv)?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

HIPAA Security Standards	HIPAA Audit Inquiry	In Place	Not In Place	N/A	Viking Cloud Findings & Comments
§164.316(b)(1) – Standard Documentation	Does the entity maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.316(b)(2)(i) – Documentation – Time Limit (Required)	Does the entity retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.316(b)(2)(ii) – Documentation – Availability	Does the entity make documentation available to those persons responsible for implementing the procedures to which the documentation pertains?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant
§164.316(b)(2)(iii) – Documentation – Updates (Required)	Does the entity review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI?	☒	☐	☐	No Gaps. Sangoma Technologies Corporation is Compliant

Appendix A - Definitions

Below are a few key terms used or referenced in the report above. Guidance for the definitions listed below was collected using NIST 800-66.

Confidentiality – is “the property that data or information is not made available or disclosed to unauthorized persons or processes.”

Integrity – is “the property that data or information have not been altered or destroyed in an unauthorized manner.”

Availability – is “the property that data or information is accessible and useable upon demand by an authorized person.”

Individually Identifiable Information – Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information – Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.

Electronic Protected Health Information (ePHI) – Information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information (see “Protected Health Information”).

Covered Entity – Covered entity means: (1) A health plan. (2) A healthcare clearinghouse. (3) A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. (4) Medicare A-2 Prescription Drug Card Sponsors.

Healthcare Clearinghouse – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Business Associate – (1) Except as provided in paragraph (2) of this definition, "business associate" means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized healthcare arrangement (as defined at 45 C.F.R. Sec. 164.501) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized healthcare arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized healthcare arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized healthcare arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in

such organized healthcare arrangement. (3) A covered entity may be a business associate of another covered entity

Hybrid Entity – A single legal entity: (1) That is a covered entity; (2) Whose business activities include both covered and noncovered functions; and (3) That designates healthcare components in accordance with paragraph § 164.105(a)(2)(iii)(C).

Standard – A rule, condition, or requirement: (1) Describing the following information for products, systems, services, or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of individually identifiable health information.

Appendix B – Required and Addressable

The following table outlines each HIPAA Security Rule requirement for the Addressable or Required specification.

Audit Type	Section	Key Activity	Required/Addressable
Security	§164.306(a)	General Requirements	R
Security	§164.308(a)	Security Management Process	R
Security	§164.308(a)(1)(ii)(A)	Security Management Process -- Risk Analysis	R
Security	§164.308(a)(1)(ii)(B)	Security Management Process -- Risk Management	R

Security	§164.308(a)(1)(ii)(C)	Security Management Process – Sanction Policy	R
Security	§164.308(a)(1)(ii)(D)	Security Management Process -- Information System Activity Review	R
Security	§164.308(a)(2)	Assigned Security Responsibility	R
Security	§164.308(a)(3)(i)	Workforce Security	R
Security	§164.308(a)(3)(ii)(A)	Workforce security -- Authorization and/or Supervision	A
Security	§164.308(a)(3)(ii)(B)	Workforce security -- Workforce Clearance Procedure	A
Security	§164.308(a)(3)(ii)(C)	Workforce security -- Establish Termination Procedures	A
Security	§164.308(a)(4)(i)	Information Access Management	R
Security	§164.308(a)(4)(ii)(A)	Information Access Management -- Isolating Healthcare Clearinghouse Functions	R
Security	§164.308(a)(4)(ii)(B)	Information Access Management -- Access Authorization	A
Security	§164.308(a)(4)(ii)(C)	Information Access Management -- Access Establishment and Modification	A
Security	§164.308(a)(5)(i)	Security Awareness and Training	R
Security	§164.308(a)(5)(ii)(A)	Security Awareness and Training -- Security Reminders	A
Security	§164.308(a)(5)(ii)(B)	Security Awareness, Training, and Tools -- Protection from Malicious Software	A
Security	§164.308(a)(5)(ii)(C)	Security Awareness, Training, and Tools -- Log-in Monitoring	A
Security	§164.308(a)(5)(ii)(D)	Security Awareness, Training, and Tools -- Password Management	A
Security	§164.308(a)(6)(i)	Security Incident Procedures	R

Security	§164.308(a)(6)(ii)	Security Incident Procedures -- Response and Reporting	R
Security	§164.308(a)(7)(i)	Contingency Plan	R
Security	§164.308(a)(7)(ii)(A)	Contingency Plan – Data Backup Plan	R
Security	§164.308(a)(7)(ii)(B)	Contingency Plan –Disaster Recovery Plan	R
Security	§164.308(a)(7)(ii)(C)	Contingency Plan -- Emergency Mode Operation Plan	R
Security	§164.308(a)(7)(ii)(D)	Contingency Plan -- Testing and Revision Procedure	A
Security	§164.308(a)(7)(ii)(A)	Contingency Plan --Application and Data Criticality Analysis	A
Security	§164.308(a)(8)	Evaluation	R
Security	§164.308(b)(1)	Business Associate Contracts and Other Arrangements	R
Security	§164.308(b)(3)	Business Associate Contracts and Other Arrangements -- Written Contract or Other Arrangement	R
Security	§164.310(a)(1)	Facility Access Controls	R
Security	§164.310(a)(2)(i)	Facility Access Controls -- Contingency Operations	A
Security	§164.310(a)(2)(ii)	Facility Access Controls -- Facility Security Plan	A
Security	§164.310(a)(2)(iii)	Facility Access Controls -- Access Control and Validation Procedures	A
Security	§164.310(a)(2)(iv)	Facility Access Controls -- Maintain Maintenance Records	A
Security	§164.310(b)	Workstation Use	R
Security	§164.310(c)	Workstation Security	R
Security	§164.310(d)(1)	Device and Media Controls	R
Security	§164.310(d)(2)(i)	Device and Media Controls -- Disposal	R

Security	§164.310(d)(2)(ii)	Device and Media Controls -- Media Re-use	R
Security	§164.310(d)(2)(iii)	Device and Media Controls -- Accountability	A
Security	§164.310(d)(2)(iv)	Device and Media Controls -- Data Backup and Storage Procedures	A
Security	§164.312(a)(1)	Access Control	R
Security	§164.312(a)(2)(i)	Access Control -- Unique User Identification	R
Security	§164.312(a)(2)(ii)	Access Control -- Emergency Access Procedure	R
Security	§164.312(a)(2)(iii)	Access Control -- Automatic Logoff	A
Security	§164.312(a)(2)(iv)	Access Control -- Encryption and Decryption	A
Security	§164.312(b)	Audit Controls	R
Security	§164.312(c)(1)	Integrity	R
Security	§164.312(c)(2)	Integrity -- Mechanism to Authenticate ePHI	A
Security	§164.312(d)	Person or Entity Authentication	R
Security	§164.312(e)(1)	Transmission	R
Security	§164.312(e)(2)(i)	Transmission Security -- Integrity Controls	A
Security	§164.312(e)(2)(ii)	Transmission Security --Encryption	A
Security	164.314(a)(1)	Business Associate Contracts or Other Arrangements	R
Security	164.314(a)(2)(i)(A)	Business associate contracts	R
Security	164.314(a)(2)(i)(B)	Business associate contracts.	R
Security	164.314(a)(2)(i)(C)	Business associate contracts.	R
Security	164.314(a)(2)(ii)	Other Arrangements	R

Security	164.314(a)(2)(iii)	Business associate contracts with subcontractors	R
Security	164.314(b)(1)	Requirements for Group Health Plans	R
Security	164.314(b)(2)(i)	Group Health Plan Implementation Specification	R
Security	164.314(b)(2)(ii)	Group Health Plan Implementation Specification	R
Security	164.314(b)(2)(iii)	Group Health Plan Implementation Specification	R
Security	164.314(b)(2)(iv)	Group Health Plan Implementation Specification	R
Security	§164.316(a)	Policies and Procedures	R
Security	§164.316(b)(1)	Documentation	R
Security	§164.316(b)(2)(i)	Documentation – Time Limit	R
Security	§164.316(b)(2)(ii)	Documentation- Availability	R
Security	§164.316(b)(2)(iii)	Documentation – Updates	R