HIPAA Security Rule Compliance Assessment

Assessment period: September 1, 2021 to December 17, 2021

Submission date: January 26, 2022

Bitdefender

Prepared for:

Mihaita Justin Stancu
mstancu@bitdefender.com

Prepared by:

Chris Nelms, CISA, CCSK, Security+
Security Consultant
Technology Services
chris.nelms@coalfire.com

Disclosure statement:

This document contains sensitive information about the computer security environment, practices, and current vulnerabilities and weaknesses of the security infrastructure of ("Bitdefender"), as well as proprietary tools and methodologies owned by Coalfire Systems, Inc. or its subsidiaries ("Coalfire"). This document is intended for use by the management of Bitdefender only and is subject to the terms, conditions, requirements, and restrictions set forth in those agreements that govern the services provided to Bitdefender by Coalfire. Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

Management's representation:

The Management of Bitdefender has affirmed that all information provided to Coalfire over the course of this engagement, which serves as the basis for the scope and conclusions of this report, is, to the best of their knowledge after due investigation and inquiry, complete, accurate, and reliable.

Table of Contents

Introduction

Assessment Objective

As part of its Health Insurance Portability and Accountability Act (HIPAA) compliance program, Bitdefender engaged Coalfire Systems, Inc. (“Coalfire”) to perform an assessment of the controls in place to satisfy the requirements of the HIPAA Security Rule, as well as the requirements of the HIPAA Breach Notification Rule as formalized by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Rule of 2013. The specific objectives included:

Characterization of the electronic protected health information (ePHI) environment to understand and document the creation, receipt, maintenance, and transmission of ePHI.

Evaluation of the security posture of the ePHI environment in accordance with the requirements of the HIPAA Security Rule and the HIPAA Breach Notification Rule.

Identification of gaps related to the administrative, technical, and physical safeguard requirements.

Issuance of detailed recommendations to assist the organization in developing a corrective action plan.

Table 3-1: Compliance Summary provides a complete list of the HIPAA Security Rule and HIPAA Breach Notification Rule requirements evaluated.

HIPAA Security Rule and HIPAA Breach Notification Rule

The HIPAA Security Rule specifically focuses on the safeguarding of ePHI through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a covered entity or a business associate. These organizations are 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 unauthorized uses or disclosures of protected health information (PHI).

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 and Documentation Requirements

While the administrative, physical, and technical requirements 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 – 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 – 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 its 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.

The HIPAA Breach Notification Rule, 45 CFR §164.404 - 414, requires HIPAA covered entities and business associates to provide notification following a breach of unsecured PHI. The major sections of the rule include:

Notification in the Case of Breach

Notification to the Media

Notification to the Secretary

Notification by a Business Associate

Law Enforcement Delay

Business Overview

BitDefender Holding B.V. (Dutch Holding), Bitdefender SRL (Romanian subsidiary), Bitdefender Inc. (US subsidiary), Bitdefender Canada Inc. (Canadian subsidiary), Bitdefender GmbH (German subsidiary), Bitdefender Italia S.R.L. (Italian subsidiary), Bitdefender España SLU (Spanish subsidiary), Bitdefender S.A.S (French subsidiary), Bitdefender ApS (Danish subsidiary), Bitdefender Ltd. (UK subsidiary), Bitdefender Netherlands B.V. (Dutch subsidiary), Bitdefender IPR Management Limited (Cypriot subsidiary), Bitdefender FZ-LLC (UAE subsidiary), Bitdefender Australia Pty Ltd. (Australian subsidiary), collectively “Bitdefender” is a global cybersecurity company that protects millions of systems in over 170 different countries.

The Bitdefender product was launched in 2001 in Romania. Bitdefender's corporate headquarters is in Bucharest, Romania. Bitdefender maintains office presence in North America (Santa Clara, CA, USA; San Antonio, TX, USA; Fort Lauderdale, FL, USA; Toronto, ON, Canada; Vancouver, BC, Canada); Europe, the Middle East, and Africa (EMEA) (the United Kingdom, France, Germany, Spain, Denmark, Cyprus, Italy, the Netherlands, the United Arab Emirates); Asia Pacific (APAC) (Australia: Melbourne).

Business-to-Business (B2B)

GravityZone

GravityZone is an enterprise security solution with a unified management console available from the cloud hosted by Bitdefender, or as a virtual appliance installed on-premises by a customer. GravityZone provides a single point for deploying, enforcing, and managing security policies for any number and any type of endpoints in any location.

GravityZone provides multiple layers of security for endpoints:

GravityZone Business Security: Antivirus (AV) for small businesses

GravityZone Advanced Business Security: Provides protection for physical and virtual desktops, servers, and mobile devices; security and antispam for Exchange mailboxes; and antivirus for Infrastructure – all managed from a single console.

GravityZone Elite Security: Prevention, hardening, risk, and incident analytics

GravityZone Ultra Security: Extended detection and response

GravityZone Full Disk Encryption

GravityZone Patch Management

GravityZone Security for Storage

GravityZone Email Security: Cloud-based email security

GravityZone Ultra Managed Detection and Response: Security-operations-center-driven, security-focused outcomes

GravityZone is also available for Managed Service Providers (MSPs):

Cloud Security for MSP: Advanced MSP security suite

Security for Amazon Web Service (AWS): Optimized protection for AWS

Managed Detection and Response Services (MDR)
Managed Detection and Response (MDR) provides outsourced cybersecurity operations providing 24/7/365 coverage for customers. MDR services combine cybersecurity for endpoints with network and security analytics, underpinned by threat intelligence to perform the following:

Event monitoring: MDR monitors alerts, responds to detections, and provides a summarized analysis via real-time reporting.

Threat hunting: MDR uses tactical and strategic threat intelligence paired with Bitdefender expertise to plan and execute threat hunting missions in the customer's protected environments. During these missions, MDR examines the customer's environment for evidence of adversarial behavior.

Pre-approved actions: MDR has a set of documented actions that can be executed in response to findings in the protected environment. The customer indicates whether actions are pre-approved for execution without consultation. When an action is undertaken in the environment, the operation will execute the agreed-upon action and document that work in the appropriate case.

Reviewing and taking action based on alerts: MDR actively review alerts from customer environments and proactively reviews telemetry searching for evidence of compromise. When identified and if pre-approved, MDR takes specific actions on behalf of the customer to mitigate the business impact.

Business-to-Business-to-Consumer (B2B2C) Solutions

Bitdefender Central Web
Bitdefender Central is the platform where partners' end users access online features and services and remotely perform security and protection tasks on devices. Bitdefender Central is available as a web portal that allows for the management of security solutions for the business-to-business-to-consumer (B2B2C) endpoint security line of products and the internet of things (IoT) security line of products.

Bitdefender Partner Integrations (B2B2C)

Rebranding/Customization Services (Original Equipment Manufacturer [OEM])
Bitdefender has several white-label security solutions:

Rebranding services (white-label or co-branded) for the Bitdefender endpoint solutions

Customization of:

Endpoint Security Solutions for Windows, macOS, Android, Linux, and iOS

Central Web

Login

Connect services: subscription integrations and notifications

IoT Security Platform
The Bitdefender IoT Security Platform's self-improving design supports the rapid adoption of internet-connected devices on new or existing infrastructures. It protects entire networking ecosystems against cyberattack, malware, and spying attempts. The Bitdefender IoT Security Platform's flexibility allows adding security features, even on lower-performance devices where heavy local processing impacts end user quality of service due to hardware constraints.

The main module of the IoT Security Platform is the at-home services protection on the router, which includes device detection, vulnerability assessment, web protection, distributed denial of service detection and protection, and exploit prevention.

Management Subscription Platform
Bitdefender uses the B2B2C management subscription platform to set up distribution chains for the Bitdefender products (white label or not) through various partners. The management subscription platform presents its functionalities in two ways:

A web-based management console

An application programming interface (API) that allows for the same level of management available through the web console

Connect Back-end Services
All Bitdefender B2B2C products utilize the Connect back-end services, which includes the following: common APIs, login APIs, subscriptions APIs, endpoint security APIs (core), specific APIs for specific products (Data Privacy, Parental, Box, and Virtual Private Network [VPN]), databases, and cloud-to-cloud integration services.

The system description in this section of the report details the products identified above (excluding on-premises services), which, for purposes of this report, are collectively referred to as the Bitdefender System. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Scope, Timing, and Methodology

Assessment Scope

The primary focus of this compliance assessment is the ePHI created, received, maintained, or transmitted by the in-scope applications and the facilities that maintain the servers and that house these applications, systems, and databases. Coalfire assessed facilities that involve the creation, access, and management of ePHI data. Bitdefender, through formal policy, workforce training, and physical and logical controls, attempts to minimize the risks associated with creating, receiving, maintaining, and transmitting ePHI as part of its product service offerings.

ePHI Environment Characterization

Bitdefender utilizes AWS, Google Cloud Provider (GCP), and on-premise hosting to provide the resources to host the Bitdefender applications. Bitdefender leverages the experience and resources of AWS, GCP, and on-premise infrastructure to scale quickly and securely as necessary to meet current and future demand. However, Bitdefender is responsible for designing and configuring the Bitdefender applications' architecture within AWS, GCP, and on-premise to ensure that security and confidentiality requirements are met.

Network Diagram

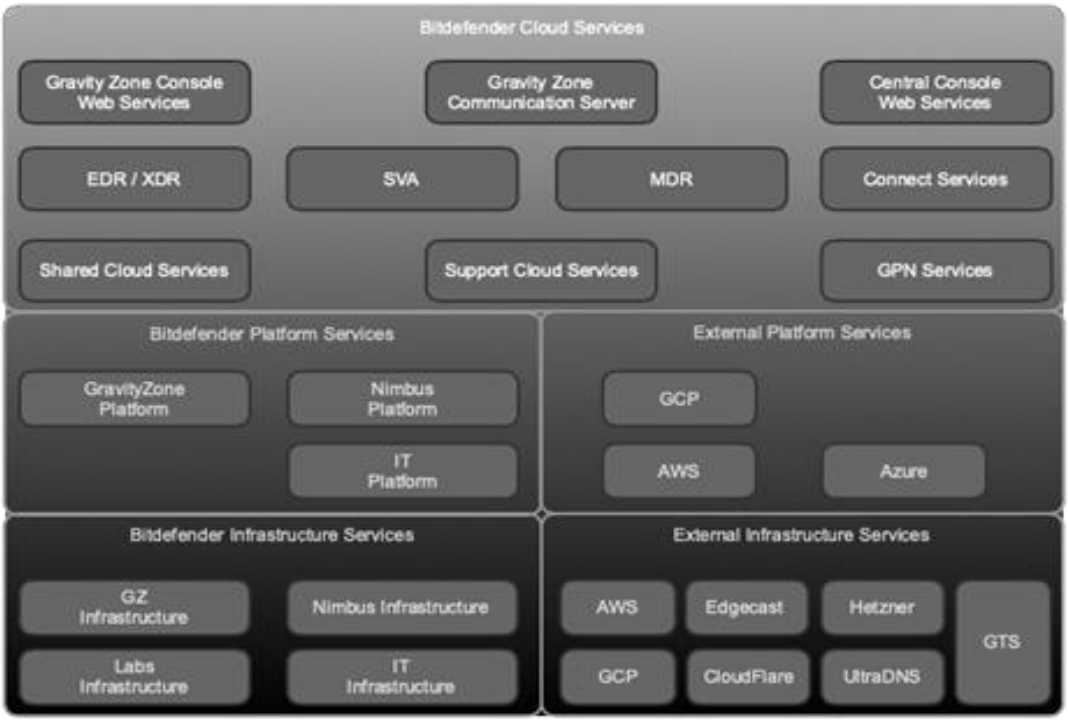

Figure 1: Network Diagram

Assessment Timing and Activities

The assessment formally commenced on September 1, 2021, during the Project Charter meeting. All relevant discovery, data collection, analysis, client interviews, and reporting took place between September 15, 2021, and December 17, 2021. Analysis and report preparation activities continued until the date of this report. Coalfire's assessment activities included the following:

Participated in a formal Project Charter meeting and provided an overview of the assessment process to key project participants.

Prepared and circulated request for information documents associated with the in-scope environments, infrastructure, and policies and procedures.

Reviewed all supplied documentation and control evidence, noting specific controls and potential gaps.

Interviewed key personnel, including those individuals specifically responsible for the design and implementation of security-related information technology (IT) controls.

Communicated potential gaps as identified so remediation efforts could be completed prior to the issuance of this report.

Reviewed evidence to support the operating effectiveness of control activities asserted to be in place.

Assessment Methodology

The Coalfire methodology for performing HIPAA assessments is based on established and repeatable assessment frameworks compiled from the National Institute of Standards and Technology (NIST) Special Publications (SPs) and the Office for Civil Rights (OCR) Audit Protocols. Specifically, NIST SP 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. Additionally, Coalfire gives consideration to NIST SP 800-53 to provide a greater level of review where outside risk remains from NIST SP 800-66 and the OCR Audit Protocols. NIST SP 800-53 provides security and privacy controls for federal information systems and organizations. NIST SPs have been supported and referenced by the OCR as viable interpretations and guidance for achieving HIPAA compliance.

For Bitdefender, Coalfire utilized NIST guidance and the most recent OCR Audit Protocols to perform a comprehensive HIPAA Compliance Assessment. As such, Coalfire:

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 HIPAA Security Rule and the HIPAA Breach Notification 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 maturity, as well as recommendations for remediation of gaps.

Personnel Interviewed

Coalfire interviewed the following personnel over the course of the engagement:

ID #	Name	Title
1	Mihai Stancu	Chief Information Security Officer (CISO)
2	Aurel Nae	Head of Information Security
3	Cristian Susco	Fraud Prevention and Investigations Director
4	Oana Giu	Legal Advisor
5	Danuta Bunea	Project Manager

Table 0-1: Personnel Interviewed

Documentation Reviewed

All documentation and evidence provided throughout the course of the engagement were reviewed during the assessment and prior to the issuance of this report. CoalfireOne, Coalfire's secure project portal, was used as a document repository. A full list of the evidence collected and reviewed is available in Appendix A – Documentation Reviewed.

Executive Summary

Conclusion

The objective of this engagement was to review, analyze, and document Bitdefender environment and its compliance efforts specific to the HIPAA Security Rule and the HIPAA Breach Notification Rule. Bitdefender's compliance intentions are established through the design and implementation of administrative, technical, and physical controls throughout the infrastructure and supporting processes. Based on documentation review, inquiry, and observation of control effectiveness, Coalfire noted the status of the HIPAA safeguards and requirements as displayed by the HIPAA Compliance Scorecard below. This opinion is based upon Bitdefender's written and verbal assertions and Coalfire's observations during the assessment period.

HIPAA Compliance Scorecard				
Safeguards and Requirements	**Total**	**No Exceptions**	**Exceptions**	**Compliance %**
Security Rule				
Administrative Safeguards	28	28	0	100.0%
Physical Safeguards	12	12	0	100.0%
Technical Safeguards	11	11	0	100.0%
Organizational Safeguards	3	3	0	100.0%
Policies and Procedures and Documentation Requirements (1 response(s) empty)	4	4	0	100.0%
Breach Notification Rule				
Breach Notification Rule	5	5	0	100.0%

Table 0-1: Compliance Summary

Summary results

The tables below provide a high-level overview of compliance for the assessed environment. Each of the implementation specifications was assigned a compliance status to assist Bitdefender in prioritizing remediation efforts. Full compliance for a given requirement was assessed based on three attributes. The first was to confirm that policies and procedures have been formally documented to meet the requirement. The second was to assess through interviews if appropriate controls are known and disseminated throughout the organization. The third was to determine whether the design of the controls are reasonable and appropriate for the size and complexity of the organization. If any of the three attributes were not present, the compliance status was identified as having an exception. Standards and implementation specifications that did not apply to Bitdefender were identified as not applicable (N/A).

● No Exception ✖ Exception

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Administrative Safeguards	
§164.308(a)(1)(i) Security Management Process (R) Standard	●
§164.308(a)(1)(ii)(A) Risk Analysis (R) Implementation specification	●
§164.308(a)(1)(ii)(B) Risk Management (R) Implementation specification	●
§164.308(a)(1)(ii)(C) Sanction Policy (R) Implementation specification	●
§164.308(a)(1)(ii)(D) Information System Activity Review (R) Implementation specification	●
§164.308(a)(2) Assigned Security Responsibility (R) Standard	●
§164.308(a)(3)(i) Workforce Security (R) Standard	●
§164.308(a)(3)(ii)(A) Authorization and/or Supervision (A) Implementation specification	●
§164.308(a)(3)(ii)(B) Workforce Clearance Procedure (A) Implementation specification	●
§164.308(a)(3)(ii)(C) Termination Procedures (A) Implementation specification	●
§164.308(a)(4)(i) Information Access Management (R) Standard	●
§164.308(a)(4)(ii)(B) Access Authorization (A) Implementation specification	●
§164.308(a)(4)(ii)(C) Access Establishment and Modification (A) Implementation specification	●
§164.308(a)(5)(i) Security Awareness and Training (R) Standard	●
§164.308(a)(5)(ii)(A) Security Reminders (A) Implementation specification	●
§164.308(a)(5)(ii)(B) Protection from Malicious Software (A) Implementation specification	●
§164.308(a)(5)(ii)(C) Log-in Monitoring (A) Implementation specification	●
§164.308(a)(5)(ii)(D) Password Management (A) Implementation specification	●
§164.308(a)(6)(i) Security Incident Procedures (R) Standard	●
§164.308(a)(6)(ii) Response and Reporting (R) Implementation specification	●
§164.308(a)(7)(i) Contingency Plan (R) Standard	●
§164.308(a)(7)(ii)(A) Data Backup Plan (R) Implementation specification	●
§164.308(a)(7)(ii)(B) Disaster Recovery Plan (R) Implementation specification	●
§164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (R) Implementation specification	N/A
§164.308(a)(7)(ii)(D) Testing and Revision Procedure (A) Implementation specification	●
§164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis (A) Implementation specification	●
§164.308(a)(8) Evaluation (R) Standard	●

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
§164.308(b)(2) Business Associate Contracts and Other Arrangements (R) (Business Associate)	●
§164.308(b)(3) Written Contract or Other Arrangement (R) Implementation specification	●

Table 0-2: Administrative Safeguards Summary – §164.308

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Physical Safeguards	
§164.310(a)(1) Facility Access Controls (R) Standard	●
§164.310(a)(2)(i) Contingency Operations (A) Implementation specification	●
§164.310(a)(2)(ii) Facility Security Plan (A) Implementation specification	●
§164.310(a)(2)(iii) Access Control and Validation Procedures (A) Implementation specification	●
§164.310(a)(2)(iv) Maintenance Records (A) Implementation specification	●
§164.310(b) Workstation Use (R) Standard	●
§164.310(c) Workstation Security (R) Standard	●
§164.310(d)(1) Device and Media Controls (R) Standard	●
§164.310(d)(2)(i) Disposal (R) Implementation specification	●
§164.310(d)(2)(ii) Media Re-use (R) Implementation specification	●
§164.310(d)(2)(iii) Accountability (A) Implementation specification	●
§164.310(d)(2)(iv) Data Backup and Storage (A) Implementation specification	●

Table 0-3: Physical Safeguards Summary – §164.310

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Technical Safeguards	
§164.312(a)(1) Access Control (R) Standard	●
§164.312(a)(2)(i) Unique User Identification (R) Implementation specification	●
§164.312(a)(2)(ii) Emergency Access Procedure (R) Implementation specification	N/A
§164.312(a)(2)(iii) Automatic Logoff (A) Implementation specification	●
§164.312(a)(2)(iv) Encryption and Decryption (A) Implementation specification	●
§164.312(b) Audit Controls (R) Standard	●
§164.312(c)(1) Integrity (R) Standard	●

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
§164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information (A) Implementation specification	●
§164.312(d) Person or Entity Authentication (R) Standard	●
§164.312(e)(1) Transmission Security (R) Standard	●
§164.312(e)(2)(i) Integrity Controls (A) Implementation specification	●
§164.312(e)(2)(ii) Encryption (A) Implementation specification	●

Table 0-4: Technical Safeguards Summary – §164.312

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Organizational Requirements	
§164.314(a)(1) Business Associate Contracts or Other Arrangements (R) Standard	●
§164.314(a)(2)(i) Business Associate Contracts (R) Implementation specification	●
§164.314(a)(2)(iii) Business Associate Contracts with Subcontractors (R) Implementation specification	●

Table 0-5: Organizational Requirements Summary – §164.314

Standards and Implementation Specifications (R) = Required, (A) = Addressable	Compliance Status
Policies and Procedures and Documentation Requirements	
§164.316(a) Policies and Procedures (R) Standard	●
§164.316(b)(1) Documentation (R) Standard	●
§164.316(b)(2)(i) Time Limit (R) Implementation specification	●
§164.316(b)(2)(ii) Availability (R) Implementation specification	●
§164.316(b)(2)(iii) Updates (R) Implementation specification	●

Table 0-6: Policies and Procedures and Documentation Requirements Summary – §164.316

Standards and Implementation Specifications	Compliance Status
§164.410(a) Notification by a Business Associate Standard	●
§164.410(b) Timeliness of Notification Implementation specification	●
§164.410(c) Content of Notification Implementation specification	●
§164.412 Law Enforcement Delay	●

Standards and Implementation Specifications	Compliance Status
§164.414(b) Administrative Requirements and Burden of Proof	●

Table 0-7: Breach Notification Rule Summary – §164.404–164.414

Observations and Recommendations

Administrative Safeguards – §164.308

Administrative Safeguards - §164.308	
Security Management Process – 164.308(a)(1)	
Security Management Process (R) – 164.308(a)(1)(i)	**Status**
Implement policies and procedures to prevent, detect, contain, and correct security violations.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf DOC-002 – IS-51-ISM010 Information Security Program Policy.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures were in place to implement countermeasures or safeguards to prevent, detect, contain, and correct security violations. Coalfire inquired of management and validated that documentation related to security violations has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures have been implemented to prevent, detect, contain, and correct security violations. **Gaps Noted:** None	
Recommendations	
None	
Risk Analysis (R) – 164.308(a)(1)(ii)(A)	**Status**
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity or business associate.	●

Administrative Safeguards - §164.308	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-003 – IS-43-IS100 IT Risk Management Policy.pdf DOC-004 – IS - 42 - ISM Risks management register.xlsx DOC-005 – IS - 42 - RiskReport- Sept 2021.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to risk analysis were in place and required a periodic assessment to be performed on the risks and vulnerabilities to the in-scope environment. Coalfire inquired of management and validated that documentation related to risk analysis has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that a risk analysis for the in-scope environment was performed within the review period and included: • A defined scope identifying all systems that create, transmit, maintain, or transmit ePHI. • An assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI. • The details of identified threats and vulnerabilities. • An assessment of the current security measures. • Impact and likelihood analysis. • Risk rating. **Gaps Noted:** None	
Recommendations	
None	
Risk Management (R) – 164.308(a)(1)(ii)(B)	**Status**
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-003 – IS-43-IS100 IT Risk Management Policy.pdf DOC-004 – IS - 42 - ISM Risks management register.xlsx DOC-005 – IS - 42 - RiskReport- Sept 2021.pdf	

Administrative Safeguards - §164.308
Observations: Coalfire reviewed documentation and confirmed that policies and procedures related to risk management were in place and demonstrated: • The process was sufficient to reduce risks to an acceptable level. • The process was ongoing and communicated throughout the organization. • Mitigation efforts were in place to lower residual risks. Coalfire inquired of management and validated that documentation related to risk management has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that: • Risk mitigation strategies were documented, prioritized, and contained associated action plans. • Implemented security measures appropriately addressed the threats and vulnerabilities identified in the risk analysis according to the risk rating. • Security measures were sufficient to mitigate or remediate the identified risks to an acceptable level. **Gaps Noted:** None
Recommendations
None

Sanction Policy (R) – 164.308(a)(1)(ii)(C)	Status
Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	●

Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-006 – HR-21- Internal Regulation - Employee's Handbook [ENG].pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to sanctions were in place to communicate the disciplinary actions that may result when a workforce member violates the organization's policies or security measures involving ePHI. Coalfire inquired of management and validated that documentation related to sanctions has been reviewed, disseminated, and implemented for the in-scope environment.

Administrative Safeguards - §164.308	
Coalfire inquired of management and confirmed that no security violations resulting in disciplinary actions occurred within the review period. **Gaps Noted:** None	
Recommendations	
None	
Information System Activity Review (R) – 164.308(a)(1)(ii)(D)	**Status**
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png DOC-009 – IR-19028.doc DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to information security activity review were in place and addressed the periodic review of audit logs, access reports, log-in monitoring reports, and security incident tracking reports for all systems that handle or impact ePHI. Coalfire inquired of management and validated that documentation related to information system activity review has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that in-scope information systems generated activity records and activity reviews were performed by qualified individuals according to the organization's required frequency. **Gaps Noted:** None	
Recommendations	
None	

Administrative Safeguards - §164.308	
Assigned Security Responsibility – 164.308(a)(2)	
Assigned Security Responsibility (R) – 164.308(a)(2)	**Status**
Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to the assignment of a security official were in place and identified the responsibilities of the role. Coalfire inquired of management and validated that documentation related to the establishment and duties of the security official has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed the documentation and confirmed that an individual (or group of individuals) was designated as the security official, their duties were clearly defined, their identity was communicated to the workforce, and the security official was responsible for compliance with the HIPAA Security Rule and for the implementation of security policies and procedures. **Gaps Noted:** None	
Recommendations	
None	
Workforce Security – 164.308(a)(3)	
Workforce Security (R) – 164.308(a)(3)(i)	**Status**
Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information	●

Administrative Safeguards - §164.308	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to workforce security were in place and ensured that: • Workforce members were granted the minimum necessary access to systems or applications containing ePHI according to their job role and responsibilities. • The various levels of access (e.g., access matrix, roles) to information systems were appropriately approved and communicated. • Management periodically reviewed workforce members' access to information systems and applications that contain ePHI to validate the access continues to be appropriate. Coalfire inquired of management and validated that documentation related to workforce security has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that: • Access granted to workforce members was provisioned according to the levels required for their job descriptions and duties and was approved by the appropriate management. • Management conducted access reviews on a scheduled, periodic basis to re-certify that workforce members continued to have the appropriate access. **Gaps Noted:** None	
Recommendations	
None	
Authorization and/or Supervision (A) – 164.308(a)(3)(ii)(A)	**Status**
Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	●

Administrative Safeguards - §164.308	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to the appropriate authorization and/or supervision of workforce members who work with ePHI, or with information systems or in locations where ePHI may be stored or accessed, were in place and included: • Identification of the management level individuals or roles who have the authority to approve access. • Processes for submitting and granting access. • Verification of the authorization and/or supervisory approvals and of the workforce members' levels of access ePHI. Coalfire inquired of management and validated that documentation related to access authorization and supervision of workforce members has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that workforce members who were authorized for access to ePHI, or to systems or locations where ePHI might be accessed, were properly authorized in accordance with the organization's related policies and procedures. **Gaps Noted:** None	
Recommendations	
None	
Workforce Clearance Procedure (A) – 164.308(a)(3)(ii)(B)	**Status**
Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-013 – HR-23-report Cosmin Alexandru Florea.pdf DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf	

Administrative Safeguards - §164.308	
DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to workforce clearance were in place and included conducting background checks. Coalfire inquired of management and validated that documentation related to workforce clearance has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that background checks were performed as part of the pre-employment process and were re-validated as appropriate. **Gaps Noted:** None	
Recommendations	
None	
Termination Procedures (A) – 164.308(a)(3)(ii)(C)	**Status**
Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-014 – 141.ISD-Leavingform-171221-1533-52.pdf DOC-015 – [#CERES-24370] Remove GravityZone account - jsimon@bitdefender.com.pdf DOC-016 – term_check.PNG DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf DOC-018 – Expiration date automation.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to access termination (when employment terminates or job assignment changes) were in place and supported: • Recovery of company-owned devices (e.g., laptops, USB devices, smart phones). • Deactivation of access to information systems for voluntary and involuntary terminations. • Termination of access by third-parties (e.g., contractors, vendors), where applicable.	

Administrative Safeguards - §164.308
• Timeframes to terminate access according to risk. Coalfire inquired of management and validated that documentation related to access termination has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that procedures were implemented for terminating workforce member and third-party access in a timely manner when employment arrangements terminate or job duties change. **Gaps Noted:** None
Recommendations
None

Information Access Management – 164.308(a)(4)	
Information Access Management (R) – 164.308(a)(4)(i)	**Status**
Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf DOC-015 – [#CERES-24370] Remove GravityZone account - jsimon@bitdefender.com.pdf DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to access restriction were in place to restrict ePHI access to only those persons and entities with a need for access and complied with the minimum necessary requirement. Coalfire inquired of management and validated that documentation related to information access restriction has been reviewed, disseminated, and implemented for the in-scope environment.	

Administrative Safeguards - §164.308	
Coalfire reviewed evidence of the technical implementation of role-based access and of workforce members' initial access and modification requests and confirmed that the minimum necessary requirement and safeguards that limit unnecessary or inappropriate access to and disclosure of PHI were implemented. **Gaps Noted:** None	
Recommendations	
None	
Access Authorization (A) – 164.308(a)(4)(ii)(B)	**Status**
Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to logical access were in place for granting access, including the authority and process to grant access, and included: • Roles required to approve requests to create information system accounts. • Procedures to create, enable, modify, disable, and remove information system accounts. Coalfire inquired of management and validated that documentation related to granting logical access has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures were implemented for granting access to ePHI, including determining appropriate levels of workforce members' access to systems containing, transmitting, or processing ePHI. **Gaps Noted:** None	

Administrative Safeguards - §164.308	
Recommendations	
None	
Access Establishment and Modification (A) – 164.308(a)(4)(ii)(C)	**Status**
Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to user access were in place to determine if access was appropriately documented, reviewed, or modified for users accessing workstations, transactions, programs, or processes. Coalfire inquired of management and validated that documentation related to access establishment and modification has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that: Workforce members' access to information systems was reviewed and recertified in a timely manner by the appropriate personnel. Modifications to individuals' access to information systems were made according to documented policies and procedures and approved by management. **Gaps Noted:** None	
Recommendations	
None	
Security Awareness and Training – 164.308(a)(5)	
Security Awareness and Training (R) – 164.308(a)(5)(i)	**Status**
Implement a security awareness and training program for all members of its workforce (including management).	●

Administrative Safeguards - §164.308	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf DOC-019 – B2B2C - 50 - ISM311 Records Retention Schedule.pdf DOC-020 – IS - 30 - training_current_users_2021.xlsx DOC-021 – IS - 31 - training_new_users_sample_2021.xlsx DOC-022 – IS - 33 - Screenshot 2021-10-22 at 13-21-47 Online Course Learning Bitdefender.png **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to security awareness and training were in place to ensure Bitdefender: • Provides workforce members security awareness and training upon hire and periodically thereafter. • Identifies workforce members (including managers, senior executives, and as appropriate, Business Associates, and contractors) who will be provided with the security awareness and training. • Provides workforce members with security awareness and training when there is a change in the organization's information systems. • Retains training logs for a minimum of six (6) years. • Provides training content that emphasizes the importance of information security topics, as well as acceptable use and disclosure of sensitive information. Coalfire inquired of management and validated that documentation related to security awareness and training has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures for a security awareness and training program were implemented for all members of the workforce. **Gaps Noted:** None	
Recommendations	
None	
Security Reminders (A) – 164.308(a)(5)(ii)(A)	**Status**
Periodic security updates.	●

Administrative Safeguards - §164.308	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf DOC-020 – IS - 30 - training_current_users_2021.xlsx DOC-021 – IS - 31 - training_new_users_sample_2021.xlsx DOC-022 – IS - 33 - Screenshot 2021-10-22 at 13-21-47 Online Course Learning Bitdefender.png DOC-023 – IS - 34 - Newsletter subscriptions.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures were in place to communicate periodic security reminders to workforce members. Coalfire inquired of management and validated that documentation related to periodic security reminders has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that periodic security reminders (e.g., emails, posters, newsletters, phishing campaigns) were communicated to workforce members. **Gaps Noted:** None	
Recommendations	
None	
Protection from Malicious Software (A) – 164.308(a)(5)(ii)(B)	**Status**
Procedures for guarding against, detecting, and reporting malicious software.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-022 – IS - 33 - Screenshot 2021-10-22 at 13-21-47 Online Course Learning Bitdefender.png DOC-020 – IS - 30 - training_current_users_2021.xlsx DOC-021 – IS - 31 - training_new_users_sample_2021.xlsx DOC-024 – IT - 88 - Screenshot of antimalware configuration.docx DOC-025 – ITG-NetworkandSystemHardeningstandardsprocedures-181021-0859-22.pdf DOC-026 – IT - 82 - Evidence of the most recent security patches applied to a sample of servers.docx	

Administrative Safeguards - §164.308
Observations: Coalfire reviewed documentation and confirmed that policies and procedures were in place for patch management and for protecting against malicious software, and the security awareness and training program included content on malicious software. Coalfire inquired of management and validated that documentation related to protection against malicious software has been reviewed, disseminated, and implemented for the in-scope environment and that the organization provided antivirus and patching process training to appropriate workforce members. Coalfire reviewed evidence and confirmed that content on malicious software was included in the security awareness and training program provided to all workforce members, and appropriate workforce members received training for their roles in guarding against, detecting, and reporting malicious software. **Gaps Noted:** None
Recommendations
None

Log-in Monitoring (A) – 164.308(a)(5)(ii)(C)	Status
Procedures for monitoring log-in attempts and reporting discrepancies.	●

Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-020 – IS - 30 - training_current_users_2021.xlsx DOC-021 – IS - 31 - training_new_users_sample_2021.xlsx DOC-027 – alert.PNG DOC-028 – AWS monitoring.png DOC-029 – GCP monitoring.png **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures were in place for log-in monitoring, and the security awareness and training program included specific training for workforce members responsible for monitoring log-in attempts and reporting discrepancies. Coalfire inquired of management and validated that documentation related to log-in monitoring has been reviewed, disseminated, and implemented for the in-scope environment and workforce members responsible for monitoring log-in attempts have received training for their role.

Administrative Safeguards - §164.308	
Coalfire reviewed evidence and confirmed that appropriate workforce members were trained on the procedures for monitoring log-in attempts and reporting discrepancies. **Gaps Noted:** None	
Recommendations	
None	
Password Management (A) – 164.308(a)(5)(ii)(D)	**Status**
Procedures for creating, changing, and safeguarding passwords.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-020 – IS - 30 - training_current_users_2021.xlsx DOC-021 – IS - 31 - training_new_users_sample_2021.xlsx DOC-030 – IT - 76 - System generated or screenshots of password and lockout configuration.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to password management were in place and addressed: • Workforce training for creating, changing, and safeguarding passwords. • Actions to take in case of a password compromise. • Best practice (or more stringent) password configuration requirements. • Confirming the workforce member's identity (e.g., security question) prior to performing a password reset. • Use of one-time passwords for new accounts or password resets. Coalfire inquired of management and validated that documentation related to password management has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that all workforce members were trained on secure password management and evidence of password technical controls demonstrating that policies and procedures have been implemented. **Gaps Noted:** None	

Administrative Safeguards - §164.308	
Recommendations	
None	
Security Incident Procedures – 164.308(a)(6)	
Security Incident Procedures (R) – 164.308(a)(6)(i)	**Status**
Implement policies and procedures to address security incidents.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-031 – IS-53-IS050 Security Incident Response Policy.pdf
DOC-032 – IS-53-IS051 Security Incident Response Plan.pdf

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to security incidents were in place and addressed:

- Identification of the specific events considered to be security incidents.
- Identification of workforce members' roles and responsibilities regarding security incidents.
- Management involvement regarding security incidents.
- Dissemination of the incident response policies and procedures to the appropriate workforce members.
- Coordination of security incidents with third parties.
- Steps to be taken in response to a security incident.
- The frequency for the review and update of the security incident response policy/policies and procedure(s).

Coalfire inquired of management and validated that documentation addressing security incidents has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that the incident response plan was appropriate for addressing security incidents and the plan was updated and reviewed according to the organization's required update frequency.

Gaps Noted:
None

Recommendations
None

Administrative Safeguards - §164.308	
Response and Reporting (R) – 164.308(a)(6)(ii)	**Status**
Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	●

Control Observations/Gaps Noted

Documents/Evidence Reviewed:
DOC-031 – IS-53-IS050 Security Incident Response Policy.pdf
DOC-009 – IR-19028.doc
DOC-032 – IS-53-IS051 Security Incident Response Plan.pdf
DOC-033 – IS -95 - Incident Response Exercise Report 07.06.2021.pdf

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to incident response and reporting were in place and included requirements for:

- The testing of the security incident response plan.
- Providing training to workforce members who are assigned to incident response roles.

Coalfire inquired of management and validated that documentation related to security incident response and reporting has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that the organization:

- Identified and responded to suspected or known security incidents.
- Mitigated the harmful effects of security incidents.
- Appropriately documented security incidents and their outcomes.
- Performed a test of the incident response plan.
- Provided training to workforce members assigned to incident response roles.

Gaps Noted:
None

Recommendations

None

Administrative Safeguards - §164.308	
Contingency Plan – 164.308(a)(7)	
Contingency Plan (R) – 164.308(a)(7)(i)	**Status**
Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	●

Control Observations/Gaps Noted

Documents/Evidence Reviewed:
DOC-034 – IS-101-ISM200 Business Continuity Policy.pdf
DOC-035 – IS-101-ISM400 Bitdefender Business Continuity Plan.pdf
DOC-036 – IS - 103 - Business Continuity and Disaster Recovery Exercise Report 17 Sept 2021.pdf

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to contingency planning were in place, supported a formal contingency plan for responding to an emergency or other occurrences that damage systems that contain ePHI, and contained:

- Identification of responsibilities in the contingency process.
- Dissemination of the contingency planning policies to the appropriate workforce members.
- Management involvement in contingency planning.
- Coordination of contingency planning process with business associates and vendors.
- Identification of the steps for executing the contingency plan.
- Frequency for the review and update of the contingency planning policies and procedures.
- Testing of the contingency plan.

Coalfire inquired of management and validated that documentation related to contingency planning has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed the contingency plan and confirmed that the plan was periodically reviewed and updated and contained reasonable and appropriate processes for responding to an emergency or other occurrence that damages systems that contain ePHI.

Gaps Noted:
None

Recommendations

None

Administrative Safeguards - §164.308	
Data Backup Plan (R) – 164.308(a)(7)(ii)(A)	**Status**
Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-037 – Nimbus – 48 - Nimbus - Backup and recovery procedures.pdf

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to data backup were in place and addressed:

- Backup schedules (e.g., frequency, type) for all locations where ePHI exists.
- Responsibilities for scheduling backups, restoring data, and responding to failed backup attempts.
- Requirements for encrypting backups.
- Storage location of backup media.

Coalfire inquired of management and validated that documentation related to data backup has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that procedures were implemented to create and maintain retrievable exact copies of ePHI and restoration tests were conducted, documented, and properly certified.

Gaps Noted:
None

Recommendations
None

Disaster Recovery Plan (R) – 164.308(a)(7)(ii)(B)	Status
Establish (and implement as needed) procedures to restore any loss of data.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-035 – IS-101-ISM400 Bitdefender Business Continuity Plan.pdf
DOC-037 – Nimbus – 48 - Nimbus - Backup and recovery procedures.pdf
DOC-036 – IS - 103 - Business Continuity and Disaster Recovery Exercise Report 17 Sept 2021.pdf

Administrative Safeguards - §164.308
Observations: Coalfire reviewed documentation and confirmed that policies and procedures related to disaster recovery (DR) were in place and addressed: • Responsibilities for restoring data. • The step-by-step process for restoring data. • Identification of occurring events (e.g., disruption, compromise, failure) requiring data restoration. • The timeframe for data restoration. • The frequency of data restoration tests for verification of media reliability and data integrity. • Review of the test results by appropriate management and documentation of any associated corrective actions. Coalfire inquired of management and validated that documentation related to data restoration has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that data restoration procedures were implemented, and data restoration tests were conducted, documented, and properly certified. **Gaps Noted:** None
Recommendations
None

Emergency Mode Operation Plan (R) – 164.308(a)(7)(ii)(C)	Status
Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	N/A

Control Observations/Gaps Noted
Documents/Evidence Reviewed: N/A **Observations:** N/A: Bitdefender holds no records that would impact patient care. **Gaps Noted:** None

Administrative Safeguards - §164.308	
Recommendations	
None	
Testing and Revision Procedure (A) – 164.308(a)(7)(ii)(D)	**Status**
Implement procedures for periodic testing and revision of contingency plans.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-034 – IS-101-ISM200 Business Continuity Policy.pdf
DOC-036 – IS - 103 - Business Continuity and Disaster Recovery Exercise Report 17 Sept 2021.pdf
DOC-037 – Nimbus – 48 - Nimbus - Backup and recovery procedures.pdf

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to periodic testing and revision of contingency plans were in place and addressed:

- Methods used to test the plans (e.g., component, system, table top exercises).
- Responsibilities for coordinating the testing.
- Testing frequency.
- The frequency for revising the contingency plans.
- Notification procedures.

Coalfire inquired of management and validated that documentation related to testing and revision has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that:

- The most recent test of the contingency plan was performed within the last twelve (12) months and results were appropriately documented.
- If necessary, corrective actions were taken as a result of the contingency plan test.
- The contingency plan has been approved, reviewed, and updated on a defined periodic basis.

Gaps Noted:
None

Recommendations
None

Administrative Safeguards - §164.308	
Applications and Data Criticality Analysis (A) – 164.308(a)(7)(ii)(E)	**Status**
Assess the relative criticality of specific applications and data in support of other contingency plan components.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-034 – IS-101-ISM200 Business Continuity Policy.pdf DOC-035 – IS-101-ISM400 Bitdefender Business Continuity Plan.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to applications and data criticality analysis were in place and addressed: • The frequency for reviewing and updating the business impact analysis. • Responsibilities for conducting the business impact analysis. • The systems and business processes to be included in the business impact analysis. Coalfire inquired of management and validated that documentation related to business impact analysis has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that the organization conducted the business impact analysis and assessed and categorized application criticality levels in order to determine recovery priorities for contingency plans. **Gaps Noted:** None	
Recommendations	
None	
Evaluation – 164.308(a)(8)	
Evaluation (R) – 164.308(a)(8)	**Status**
Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-040 – IS-49-ISM050 Security System Development Lifecycle Policy.pdf	

Administrative Safeguards - §164.308
DOC-041 – IS - 90 - Open port tasks from external scanning.html DOC-042 – Nimbus_assets_Mar_2021.html DOC-043 – VA-9367.pdf DOC-044 – Nimbus Infrastructure Penetration testing report September 2021.pdf DOC-045 – VA-10151.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to technical and non-technical evaluations were in place and addressed: • The types of technical (e.g., pen test, scans) and nontechnical (e.g., HIPAA assessments, risk assessments) evaluations. • Responsibilities for performing and approving the results of each evaluation. • The frequency for performing each evaluation. • Performing evaluations in response to environmental or operational changes or newly identified risks affecting the security of ePHI. Coalfire inquired of management and validated that documentation related to evaluations has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence of the periodic technical and non-technical evaluations performed by the organization and confirmed that policies and procedures were implemented. Additionally, the completion of this HIPAA Compliance Assessment assists the organization in meeting the non-technical evaluation requirement. **Gaps Noted:** None
Recommendations
None

Business Associate Contracts and Other Arrangements – 164.308(b)	
Business Associate Contracts and Other Arrangements (R) – 164.308(b)(2)	**Status**
A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-047 – Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf DOC-046 – Legal 1- BAA template.docx	

Administrative Safeguards - §164.308
Observations: Coalfire reviewed evidence and confirmed that the organization utilizes business associate agreements to obtain satisfactory assurances from business associates and subcontractors that have access to, or could impact, ePHI. Coalfire inquired of management and validated that documentation related to vendor contracting and risk management has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that the organization: • Executed sub-business associate agreements with the vendors and subcontractors that create, receive, maintain, or transmit ePHI on the organization's behalf. • The sub-business associate contracts contained the security requirements in place to address the confidentiality, integrity, and availability of ePHI. • Required all subcontractors to maintain business associate agreements equal to or greater than the business associate agreement with the origin covered entity. **Gaps Noted:** None
Recommendations
None

Written Contract or Other Arrangement (R) – 164.308(b)(3)	Status
Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	●

Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-047 – Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf DOC-046 – Legal 1- BAA template.docx **Observations:** Coalfire reviewed evidence and confirmed that the organization utilized business associate agreements to document the satisfactory assurances obtained from business associates and subcontractors that have access to, or could impact, ePHI. Coalfire inquired of management and validated that documentation related to vendor contracting and risk management has been reviewed, disseminated, and implemented for the in-scope environment.

Administrative Safeguards - §164.308
Coalfire reviewed evidence and confirmed that the organization executed business associate agreements with the entities which create, receive, maintain, or transmit ePHI on the organization's behalf, and the contracts contained the security requirements in place to address the confidentiality, integrity, and availability of ePHI. **Gaps Noted:** None
Recommendations
None

Table 0-1: Administrative Safeguards – §164.308

Physical Safeguards – §164.310

Physical Safeguards – §164.310	
Facility Access Controls – 164.310(a)	
Facility Access Controls (R) – 164.310(a)(1)	**Status**
Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf DOC-016 – term_check.PNG DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to facility physical access control and the use of facilities and equipment were in place to limit and restrict physical access to electronic information systems and data.	

Physical Safeguards – §164.310	
Coalfire inquired of management and validated that documentation related to facility access controls has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed documentation and confirmed that the third-party data center service provider implemented appropriate controls to limit physical access to electronic information systems and to the facilities in the data center, while ensuring that properly authorized access was allowed. **Gaps Noted:** None	
Recommendations	
None	
Contingency Operations (A) – 164.310(a)(2)(i)	**Status**
Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-035 – IS-101-ISM400 Bitdefender Business Continuity Plan.pdf DOC-036 – IS - 103 - Business Continuity and Disaster Recovery Exercise Report 17 Sept 2021.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to physical security were in place and addressed: • Procedures for granting access to facilities in support of disaster recovery and business resumption efforts. • A process for allowing facility access for the restoration of lost data under the contingency plans in the event of an emergency. • Establishment of alternate work locations. • Physical access to the third-party data center service provider is not required for the organization to restore lost data or recover systems during an emergency or disaster. Coalfire inquired of management and validated that documentation related to facility access for restoration activities has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed documentation and confirmed that the third-party data center service provider implemented appropriate controls to limit physical access to electronic information systems and to the facilities in the data center, while ensuring that properly authorized access was allowed.	

Physical Safeguards – §164.310	
Gaps Noted: None	
Recommendations	
None	
Facility Security Plan (A) – 164.310(a)(2)(ii)	**Status**
Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-007 – IS-47-IS140 Access Control Policy.pdf
DOC-087 – PS-9- IS300 Physical Security Policy.pdf
DOC-088 – PS-9-SEC010 - Physical Access Guide.pdf
DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png
DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png
DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf
DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf
DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf
DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to facility security were in place and addressed:

- Security measures to provide physical security protection for facilities and equipment.
- Responsibilities for managing the facility security plan.

Coalfire inquired of management and validated that documentation related to the facility security plan has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that policies and procedures were implemented to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Gaps Noted:
None

Physical Safeguards – §164.310	
Recommendations	
None	
Access Control and Validation Procedures (A) – 164.310(a)(2)(iii)	**Status**
Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-007 – IS-47-IS140 Access Control Policy.pdf
DOC-087 – PS-9- IS300 Physical Security Policy.pdf
DOC-088 – PS-9-SEC010 - Physical Access Guide.pdf
DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png
DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png
DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf
DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf
DOC-015 – [#CERES-24370] Remove GravityZone account - jsimon@bitdefender.com.pdf
DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf
DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to physical access control and validation were in place and addressed:

- Methods for controlling and validating access to the facility, including procedures for visitors, contractors, and employees.
- Responsibilities for reviewing and approving physical access requests.
- The frequency for reviewing the access rights of individuals with physical access to sensitive areas and facilities.

Coalfire inquired of management and validated that documentation related to physical access control and validation has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that policies and procedures were implemented to control and validate physical access to facilities.

Gaps Noted:
None

Physical Safeguards – §164.310	
Recommendations	
None	
Maintenance Records (A) – 164.310(a)(2)(iv)	**Status**
Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-087 – PS-9- IS300 Physical Security Policy.pdf DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png DOC-011 – B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf DOC-015 – [#CERES-24370] Remove GravityZone account - jsimon@bitdefender.com.pdf DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to facility maintenance were in place and addressed documenting the repairs and modifications to the physical components of the facility related to security. Coalfire inquired of management and validated that documentation related to maintenance records has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures were implemented to document repairs and modifications to the security-related physical components of the facility (e.g., hardware, walls, doors, locks). **Gaps Noted:** None	
Recommendations	
None	

Physical Safeguards – §164.310	
Workstation Use – 164.310(b)	
Workstation Use (R) – 164.310(b)	**Status**
Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-049 – HR-21- Bitdefender Code of Business Conduct.pdf DOC-006 – HR-21- Internal Regulation - Employee's Handbook [ENG].pdf DOC-050 – HR-22-Anexa la dosarul personal Florea Cosmin.pdf DOC-051 – Florea.pdf DOC-052 – HR-24-Florea Cosmin Alexandru-Anexa 3.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to device security were in place and addressed: • Safeguards to prevent or preclude unauthorized access to an unattended device and to prevent unauthorized persons from viewing sensitive information. • Procedures related to the proper use of workstations and devices. • Maintaining an inventory of devices and their classifications. Coalfire inquired of management and validated that documentation related to proper workstation and device use has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that procedures were implemented to maintain asset inventories and to classify and appropriately use and protect devices. **Gaps Noted:** None	
Recommendations	
None	

Physical Safeguards – §164.310	
Workstation Security – 164.310(c)	
Workstation Security (R) – 164.310(c)	**Status**
Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	●

Control Observations/Gaps Noted

Documents/Evidence Reviewed:
DOC-007 – IS-47-IS140 Access Control Policy.pdf
DOC-020 – IS - 30 - training_current_users_2021.xlsx
DOC-021 – IS - 31 - training_new_users_sample_2021.xlsx
DOC-024 – IT - 88 - Screenshot of antimalware configuration.docx
DOC-025 – ITG-NetworkandSystemHardeningstandardsprocedures-181021-0859-22.pdf
DOC-026 – IT - 82 - Evidence of the most recent security patches applied to a sample of servers.docx

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to workstation and device security were in place and addressed:

- Physical security requirements for devices (e.g., screen locks, encryption, data loss prevention/USB lock down).
- Antivirus protection.
- Patch management.
- Baseline configuration standards and build checklists.
- Restricting access to devices.
- Controls to protect data on mobile devices.

Coalfire inquired of management and validated that documentation related to workstation and device security has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that devices (workstations, servers, mobile devices) were installed with:

- Current operating systems and updates (patches).
- Antivirus/malicious software protection.
- Physical and logical access controls to limit access to the devices to only authorized users.

Gaps Noted:
None

Physical Safeguards – §164.310	
Recommendations	
None	
Device and Media Controls – 164.310(d)	
Device and Media Controls (R) – 164.310(d)(1)	**Status**
Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-035 – IS-101-ISM400 Bitdefender Business Continuity Plan.pdf DOC-089 – B2B-55-IS071 Vulnerabilities Assessment and Pentests Procedure.pdf DOC-090 – IS-51-ISM000 Policy.pdf DOC-053 – Nimbus – 80 - Nimbus - System inventory of all in scope assets - Inventory 15.10-15-28.csv DOC-054 – Synoptic - Datacenter media disposal.xlsx DOC-055 – 109. Evidence - C1.2 - Certificates of destruction for a sample of destroyed media [IT].docx DOC-056 – mdm_1.png DOC-057 – mdm_2.png **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to device and media control were in place and addressed the tracking and authorization processes for the receipt, removal, and movement of hardware and electronic media into, out of, and within the organization's facilities. Coalfire inquired of management and validated that documentation related to device and media control has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures were implemented to properly track, document, and authorize the movement of hardware and electronic media. **Gaps Noted:** None	
Recommendations	
None	

Physical Safeguards – §164.310	
Disposal (R) – 164.310(d)(2)(i)	**Status**
Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-058 – IS-50-IS020 Information and Media Disposal Policy.pdf DOC-053 – Nimbus – 80 - Nimbus - System inventory of all in scope assets - Inventory 15.10-15-28.csv DOC-054 – Synoptic - Datacenter media disposal.xlsx DOC-055 – 109. Evidence - C1.2 - Certificates of destruction for a sample of destroyed media [IT].docx DOC-059 – B2B2C - 110 - [#GDPRCLEAN-13280] Please process a GDPR deletion for user leejmike0@gmail.com.pdf DOC-060 – B2B2C - 110 - GDPRCLEAN-13280 screenshot.png **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to the disposal of ePHI data or the hardware or electronic media on which ePHI data is stored were in place and included: • The types of devices and media that store ePHI. • Identification of the sanitization and destruction methods utilized. • Management of the disposal process, including retention of disposal documentation. Coalfire inquired of management and validated that documentation related to disposal processes has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures were implemented to address the final disposition of ePHI and the sanitization and disposal of the hardware or media on which it was stored. **Gaps Noted:** None	
Recommendations	
None	
Media Re-use (R) – 164.310(d)(2)(ii)	**Status**
Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	●

Physical Safeguards – §164.310	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-058 – IS-50-IS020 Information and Media Disposal Policy.pdf DOC-019 – B2B2C - 50 - ISM311 Records Retention Schedule.pdf DOC-054 – Synoptic - Datacenter media disposal.xlsx DOC-055 – 109. Evidence - C1.2 - Certificates of destruction for a sample of destroyed media [IT].docx DOC-059 – B2B2C - 110 - [#GDPRCLEAN-13280] Please process a GDPR deletion for user leejmike0@gmail.com.pdf DOC-060 – B2B2C - 110 - GDPRCLEAN-13280 screenshot.png **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to media re-use were in place and addressed: • Identification of the methods utilized to remove ePHI from electronic media prior to external and internal re-use. • The process for verifying the removal of ePHI from electronic media. Coalfire inquired of management and validated that documentation related to media re-use has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that procedures were implemented for the removal of ePHI from electronic media before the media was made available for re-use. **Gaps Noted:** None	
Recommendations	
None	
Accountability (A) – 164.310(d)(2)(iii)	**Status**
Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf DOC-002 – IS-51-ISM010 Information Security Program Policy.pdf DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-053 – Nimbus – 80 - Nimbus - System inventory of all in scope assets - Inventory 15.10-15-28.csv	

Physical Safeguards – §164.310
Observations: Coalfire reviewed documentation and confirmed that policies and procedures related to media accountability were in place and addressed: • Certifying and maintaining records of electronic media and hardware movement. • Identification of the types of hardware and electronic media included in the accountability process. • The process for reconciling the device and media inventory. Coalfire inquired of management and validated that documentation related to media accountability has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that procedures were implemented to: • Maintain a system inventory list, including classification of devices according to sensitivity. • Track, record, and certify movement of media and hardware. **Gaps Noted:** None
Recommendations
None

Data Backup and Storage (A) – 164.310(d)(2)(iv)	Status
Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	●

Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-037 – Nimbus – 48 - Nimbus - Backup and recovery procedures.pdf DOC-039 – B2B-104-GZ_backup additional details.docx DOC-036 – IS - 103 - Business Continuity and Disaster Recovery Exercise Report 17 Sept 2021.pdf DOC-061 – IT - 104 - Screenshot of backup schedule configurations for infrastructure and databases.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to data backup were in place and required data backups to be made prior to the physical movement of systems containing ePHI. Coalfire reviewed documentation and confirmed that policies and procedures related to data backup were in place and required data backups to be made prior to the physical movement of systems containing ePHI.

Physical Safeguards – §164.310
Coalfire reviewed evidence and confirmed that a retrievable, exact copy of ePHI would be backed up and restored for any equipment which moved. During the review period, no equipment containing ePHI was relocated. **Gaps Noted:** None
Recommendations
None

Table 0-2: Physical Safeguards – §164.310

Technical Safeguards – §164.312

Technical Safeguards – §164.312	
Access Control – 164.312(a)	
Access Control (R) – 164.312(a)(1)	**Status**
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-008 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png DOC-010 – Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf DOC-015 – [#CERES-24370] Remove GravityZone account - jsimon@bitdefender.com.pdf DOC-017 – [#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures regarding access control were in place and included: • Identification of the capabilities of electronic information system access controls (i.e., read-only, modify, full access). • Identification of the type of access controls implemented for the electronic information systems. • The technical access controls and management of system and generic IDs and accounts.	

Technical Safeguards – §164.312	
• Processes and responsibilities for adding, modifying, and terminating user access. • The frequency for the review and verification of user and software program access to electronic information systems that maintain ePHI. Coalfire inquired of management and validated that documentation related to technical access controls has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that technical policies and procedures were implemented to allow access to electronic information systems containing ePHI to only those persons or software programs that were granted access rights. **Gaps Noted:** None	
Recommendations	
None	
Unique User Identification (R) – 164.312(a)(2)(i)	**Status**
Assign a unique name and/or number for identifying and tracking user identity.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-012 – B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to logical system access were in place and addressed the following: • All workforce members are assigned and must use a unique user ID account (e.g., user name). • Shared and generic accounts are prohibited or limited to special circumstances. • Unique user identification, including processes for establishing and assigning user IDs to track user identities. Coalfire inquired of management and validated that documentation related to unique user identification has been reviewed, disseminated, and implemented for the in-scope environment.	

Technical Safeguards – §164.312	
Coalfire reviewed evidence and confirmed that policies and procedures were implemented to assign unique identifies to users and to keep the use of generic and shared accounts to a minimum, and that a rationale for each exists. **Gaps Noted:** None	
Recommendations	
None	
Emergency Access Procedure (R) – 164.312(a)(2)(ii)	**Status**
Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	N/A
Control Observations/Gaps Noted	
Observations: N/A: Bitdefender does not hold any records that would impact patient care. **Gaps Noted:** None	
Recommendations	
None	
Automatic Logoff (A) – 164.312(a)(2)(iii)	**Status**
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-062 – IS - 136 - Bitdefender Screenlock Implementation.pdf	

Technical Safeguards – §164.312	
Observations: Coalfire reviewed documentation and confirmed that policies and procedures related to electronic session termination were in place and addressed automatic logoff or lockout of accounts based on a pre-determined time of inactivity. Coalfire inquired of management and validated that documentation related to automatic logoff has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that system settings and technical controls were implemented to terminated electronic sessions after a predetermined time of inactivity. **Gaps Noted:** None	
Recommendations	
None	
Encryption and Decryption (A) – 164.312(a)(2)(iv)	**Status**
Implement a mechanism to encrypt and decrypt electronic protected health information.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-063 – IS-137-IS111 Encryption and Key Management Standard.pdf DOC-064 – IS-137-ISM301 Information Classification Procedure.pdf DOC-065 – tls_flow_nimbus.PNG DOC-066 – tls_nimbus_nimbus.PNG DOC-067 – tls_push_nimbus.PNG DOC-068 – Nimbus – 58 - Nimbus - Encryption.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to encryption were in place and addressed: • Encryption types and encryption technology used for devices and systems known to store ePHI (FIPS 140-2 encryption). • Processes for managing encryption keys. • Restricted access for modifying or creating keys.	

Technical Safeguards – §164.312
Coalfire inquired of management and validated that documentation related to encryption and decryption has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures were implemented to enable encryption and decryption of data at rest. **Gaps Noted:** None
Recommendations
None

Audit Controls – 164.312(b)	
Audit Controls (R) – 164.312(b)	**Status**
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-019 – B2B2C - 50 - ISM311 Records Retention Schedule.pdf
DOC-069 – IS-55-IS170 Log Management and Monitoring Policy.pdf
DOC-027 – alert.PNG
DOC-028 – AWS monitoring.png
DOC-029 – GCP monitoring.png
DOC-070 – alert_config_panel.PNG

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to audit controls were in place and included:

- Identification of hardware, software and/or procedural mechanisms to record and examine activity in information systems that contain or impact ePHI.
- Identification of the systems and applications where auditing has been enforced.
- Identification of the specific activities (e.g., create, read, delete, success/failure, log-ins) that are logged.
- Responsibilities for and frequency of reviewing audit logs and log-ins.
- Identification of inappropriate or suspicious activity and log-in attempts and actions to take in response.
- The retention period for audit logs.

Technical Safeguards – §164.312
Coalfire inquired of management and validated that documentation related to audit controls has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that hardware, software, and procedural mechanisms were implemented that recorded and examined activity in information systems that contained or impacted ePHI. **Gaps Noted:** None
Recommendations
None

Integrity – 164.312(c)	
Integrity (R) – 164.312(c)(1)	**Status**
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-040 – IS-49-ISM050 Security System Development Lifecycle Policy.pdf DOC-063 – IS-137-IS111 Encryption and Key Management Standard.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx DOC-065 – tls_flow_nimbus.PNG DOC-066 – tls_nimbus_nimbus.PNG DOC-067 – tls_push_nimbus.PNG DOC-068 – Nimbus – 58 - Nimbus - Encryption.pdf DOC-071 – Nimbus – 35 - Nimbus - File Integrity monitoring - FIM system.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to the integrity of data at rest were in place and included: • Processes to protect ePHI from improper alteration or destruction. • Actions taken if improper alteration or destruction of ePHI is detected. Coalfire inquired of management and validated that documentation related to integrity of data at rest has been reviewed, disseminated, and implemented for the in-scope environment.	

Technical Safeguards – §164.312
Coalfire reviewed evidence and confirmed that policies and procedures were implemented to protect ePHI at rest from improper alteration or destruction. **Gaps Noted:** None
Recommendations
None

Mechanism to Authenticate Electronic Protected Health Information (A) – 164.312(c)(2)	Status
Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	●

Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-063 – IS-137-IS111 Encryption and Key Management Standard.pdf DOC-025 – ITG-NetworkandSystemHardeningstandardsprocedures-181021-0859-22.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx DOC-072 – MDR-59-Network-Segmentation-Diagram.png DOC-073 – B2B-84-RMMI-NSGReview.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to authentication of ePHI were in place and supported the implementation of mechanisms to corroborate that ePHI had not been altered or destroyed in an unauthorized manner. Coalfire inquired of management and validated that documentation related to authentication of ePHI has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that electronic mechanisms were implemented to corroborate that ePHI had not been altered or destroyed in an unauthorized manner. **Gaps Noted:** None
Recommendations
None

Technical Safeguards – §164.312	
Person or Entity Authentication – 164.312(d)	
Person or Entity Authentication (R) – 164.312(d)	**Status**
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	●
Control Observations/Gaps Noted	

Documents/Evidence Reviewed:
DOC-007 – IS-47-IS140 Access Control Policy.pdf
DOC-084 – B2B-60-GZ_GravityZone_Cloud_Network_Diagram.pdf
DOC-085 – Nimbus-GCP-AWS-Link.png
DOC-086 – Nimbus Logical.png
DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to entity authentication were in place to verify that a person or entity seeking access to ePHI is the one claimed, and included:

- Identification of the systems and applications requiring authentication.
- The authentication procedures for all systems and applications that access or impact ePHI.
- The authentication process for verifying the identity of a real person or an automated process or entity.

Coalfire inquired of management and validated that documentation related to entity authentication has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that policies and procedures were implemented to authenticate and verify the identities of persons and entities seeking access to ePHI or to systems that impact ePHI.

Gaps Noted:
None

Recommendations
None

Technical Safeguards – §164.312	
Transmission Security – 164.312(e)	
Transmission Security (R) – 164.312(e)(1)	**Status**
Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	●

Control Observations/Gaps Noted

Documents/Evidence Reviewed:
DOC-007 – IS-47-IS140 Access Control Policy.pdf
DOC-063 – IS-137-IS111 Encryption and Key Management Standard.pdf
DOC-064 – IS-137-ISM301 Information Classification Procedure.pdf
DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx
DOC-065 – tls_flow_nimbus.PNG
DOC-066 – tls_nimbus_nimbus.PNG
DOC-067 – tls_push_nimbus.PNG

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to transmission security were in place to implement controls to guard against unauthorized access to ePHI transmitted over electronic communication networks and included:

- Identification of the various methods, devices, and networks used to electronically transmit ePHI.
- Identification of specific technical security controls implemented.

Coalfire inquired of management and validated that documentation related to transmission security has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed evidence and confirmed that technical security measures were implemented to guard against unauthorized access to ePHI transmitted over electronic communications networks.

Gaps Noted:
None

Recommendations

None

Technical Safeguards – §164.312	
Integrity Controls (A) – 164.312(e)(2)(i)	**Status**
Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-019 – B2B2C - 50 - ISM311 Records Retention Schedule.pdf DOC-040 – IS-49-ISM050 Security System Development Lifecycle Policy.pdf DOC-063 – IS-137-IS111 Encryption and Key Management Standard.pdf DOC-025 – ITG-NetworkandSystemHardeningstandardsprocedures-181021-0859-22.pdf DOC-072 – MDR-59-Network-Segmentation-Diagram.png DOC-073 – B2B-84-RMMI-NSGReview.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to integrity of data in transmission were in place and addressed the security measures implemented to ensure that electronically transmitted ePHI has not been improperly modified without detection. Coalfire inquired of management and validated that documentation related to integrity of data in transmission has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that security measures were implemented to ensure that electronically transmitted ePHI was not improperly modified without detection. **Gaps Noted:** None	
Recommendations	
None	
Encryption (A) – 164.312(e)(2)(ii)	**Status**
Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-063 – IS-137-IS111 Encryption and Key Management Standard.pdf	

Technical Safeguards – §164.312
DOC-064 – IS-137-ISM301 Information Classification Procedure.pdf DOC-048 – IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx DOC-065 – tls_flow_nimbus.PNG DOC-066 – tls_nimbus_nimbus.PNG DOC-067 – tls_push_nimbus.PNG **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to encryption of data in transmission were in place and included: • The requirement for all ePHI in transit to be encrypted, and the types of encryption used to secure electronically transmitted ePHI (FIPS 140-2 encryption). • Key management processes. Coalfire inquired of management and validated that documentation related to encryption of data in transmission has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that a mechanism was implemented to encrypt ePHI in transmission when appropriate. **Gaps Noted:** None
Recommendations
None

Table 0-3: Technical Safeguards – §164.312

Organizational Requirements – §164.314

Organizational Requirements – §164.314	
Business Associate Contracts or Other Arrangements – 164.314(a)	
Business Associate Contracts or Other Arrangements (R) – 164.314(a)(1)	**Status**
Business associate contracts or other arrangements. The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.	●

Organizational Requirements – §164.314
Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-047 – Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf DOC-046 – Legal 1- BAA template.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to business associate contracts were in place and included the following requirements: • The organization uses a standard business associate contract with contractors or other entities to which it discloses ePHI. • The business associate agreement requires a business associate to ensure that any agent, including a subcontractor, agrees to the same restriction applied in the agreement. Coalfire inquired of management and validated that documentation related to business associate contracting has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that contract templates met the follow requirements as applicable: • Subcontractors that create, receive, maintain, or transmit ePHI on behalf of the organization agree to comply with the requirements in the contract or other arrangement. • Subcontractors must report any security incidents of which it becomes aware, including breaches of unsecured PHI to the organization. • The same requirements apply to the contract or other arrangements between a business associate and a subcontractor. **Gaps Noted:** None
Recommendations
None

Business Associate Contracts (R) – 164.314(a)(2)(i)	Status
The contract must provide that the business associate will-- (A) Comply with the applicable requirements of this subpart; (B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and	●

Organizational Requirements – §164.314	
(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410	

Control Observations/Gaps Noted

Documents/Evidence Reviewed:
DOC-047 – Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf
DOC-046 – Legal 1- BAA template.docx

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to business associate contracts were in place and included the following requirements:

- The organization uses a standard business associate contract with contractors or other entities to which it discloses ePHI.
- The business associate agreement requires a business associate to ensure that any agent, including a subcontractor, agrees to the same restriction applied in the agreement.

Coalfire inquired of management and validated that documentation related to business associate contracting has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire reviewed the organization's business associate contracts and confirmed that the contracts complied with the following requirements as applicable:

- The organization's business associates must implement appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate contract.
- The business associate must enter into compliant business associate contracts or other arrangement with its own subcontractors.
- The business associate must report, to the covered entity, any security incident of which it becomes aware, including breaches of unsecured PHI.

Gaps Noted:
None

Recommendations

None

Organizational Requirements – §164.314	
Business Associate Contracts with Subcontractors (R) – 164.314(a)(2)(iii)	**Status**
The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-074 – Legal-4-Procedure for approving Suppliers -non MCT agreements.pdf DOC-075 – Legal-4-Notes.docx DOC-076 – Legal-4-Procedure for approving MKT Suppliers standards agreements.pdf DOC-046 – Legal 1- BAA template.docx DOC-047 – Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to business associate contracting were in place and support applying appropriate requirements to the business associate and its subcontractors in the same manner as such requirements apply to the organization and its business associates. Coalfire inquired of management and validated that documentation related to the use of other arrangements for business associate contracting has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed the organization's business associate contracts and confirmed that the contracts complied with the following requirements as applicable: • The organization's business associates must implement appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate contract. • The business associate must enter into compliant business associate contracts or other arrangement with their own subcontractors. • The business associate must report, to the covered entity, any security incident of which it becomes aware, including breaches of unsecured PHI. **Gaps Noted:** None	
Recommendations	
None	

Table 0-4: Organizational Requirements – §164.314

Policies and Procedures and Documentation Requirements – §164.316

Policies and Procedures and Documentation Requirements – §164.316	
Policies and Procedures – 164.316(a)	
Policies and Procedures (R) – 164.316(a)	**Status**
Implement reasonable and appropriate policies and procedures 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). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to a policy management program were in place and addressed: • Responsibilities for policy and procedure maintenance. • The frequency for policy and procedure review. • Policy and procedure approvals. Coalfire inquired of management and validated that documentation related to the policy management program has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed documents as noted in the appendix A and confirmed that policies and procedures were in place to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule. **Gaps Noted:** None	
Recommendations	
None	

Policies and Procedures and Documentation Requirements – §164.316	
Documentation – 164.316(b)	
Documentation (R) – 164.316(b)(1)	**Status**
Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) 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.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-002 – IS-51-ISM010 Information Security Program Policy.pdf DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures for maintaining the written documentation required to comply with the HIPAA Security Rule were in place. Coalfire inquired of management and validated that documentation related to maintaining HIPAA Security Rule documentation has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that: • The organization maintained policies and procedures to comply with the HIPAA Security Rule in written or electronic form. • Actions, activities, or assessments required by the HIPAA Security Rule were retained as a written or electronic record. **Gaps Noted:** None	
Recommendations	
None	
Time Limit (R) – 164.316(b)(2)(i)	**Status**
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.	●

Policies and Procedures and Documentation Requirements – §164.316	
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-019 – B2B2C - 50 - ISM311 Records Retention Schedule.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to retention were in place and required policies and procedures to be retained for at least six (6) years from the date of creation or the last effective date. Coalfire inquired of management and validated that documentation related to policy and procedure retention has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire reviewed evidence and confirmed that policies and procedures had been retained since inception or for six (6) years from the date of creation or the date when last in effect. Coalfire reviewed documents as noted in the appendix A. **Gaps Noted:** None	
Recommendations	
None	
Availability (R) – 164.316(b)(2)(ii)	**Status**
Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-002 – IS-51-ISM010 Information Security Program Policy.pdf DOC-001 – IS-51-ISM020 Information Security Organization Policy.pdf DOC-077 – policy_location.docx **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures were in place to make documentation available to the workforce.	

Policies and Procedures and Documentation Requirements – §164.316	
Coalfire inquired of management and validated that documentation related to workforce access to policies and procedures has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire inspected evidence and confirmed that policies and procedures were made available to the personnel responsible for implementing the procedures. **Gaps Noted:** None	
Recommendations	
None	
Updates (R) – 164.316(b)(2)(iii)	**Status**
Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-002 – IS-51-ISM010 Information Security Program Policy.pdf DOC-003 – IS-43-IS100 IT Risk Management Policy.pdf DOC-007 – IS-47-IS140 Access Control Policy.pdf DOC-031 – IS-53-IS050 Security Incident Response Policy.pdf DOC-034 – IS-101-ISM200 Business Continuity Policy.pdf DOC-040 – IS-49-ISM050 Security System Development Lifecycle Policy.pdf DOC-058 – IS-50-IS020 Information and Media Disposal Policy.pdf DOC-069 – IS-55-IS170 Log Management and Monitoring Policy.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to policy management were in place and included requirements for a periodic review. Coalfire inquired of management and validated that documentation related to policy and procedure updates has been reviewed, disseminated, and implemented for the in-scope environment.	

Policies and Procedures and Documentation Requirements – §164.316
Coalfire reviewed the revision history for the policies and procedures provided for this assessment and confirmed that documentation was reviewed periodically and updated as needed. **Gaps Noted:** None
Recommendations
None

Table 0-5: Policies and Procedures Documentation Requirements – §164.316

Breach Notification Rule – §164.404 – 164.414

Breach Notification Rule – §164.404 – 164.414	
Notification by a Business Associate – 164.410	
Notification by a Business Associate – 164.410(a)	**Status**
(1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-078 – IS-7-ISM250 BC_DR Communication on Security Incidents.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to breach notification by a business associate were in place and addressed the reporting of breaches of unsecured PHI to the covered entity.	

Breach Notification Rule – §164.404 – 164.414
Coalfire inquired of management and validated that documentation related to the breach notification by a business associate has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire inquired of management and confirmed that no breaches occurred during the review period. **Gaps Noted:** None
Recommendations
None

Timeliness of Notification – 164.410(b)	Status
Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	●

Control Observations/Gaps Noted
Documents/Evidence Reviewed: DOC-078 – IS-7-ISM250 BC_DR Communication on Security Incidents.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to breach notification by a business associate were in place and addressed notifying the covered entity within 60 days of discovering the breach or security incident involving ePHI. Coalfire inquired of management and validated that documentation related to the timeliness of the breach notification by a business associate has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire inquired of management and confirmed that no breaches occurred during the review period. **Gaps Noted:** None
Recommendations
None

Breach Notification Rule – §164.404 – 164.414	
Content of Notification – 164.410(c)	**Status**
(1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	●

Control Observations/Gaps Noted

Documents/Evidence Reviewed:
DOC-078 – IS-7-ISM250 BC_DR Communication on Security Incidents.pdf
DOC-079 – Legal-8-Notes - breach notification.docx
DOC-080 – Legal-8-data breach notification_RO DPAuthority.pdf
DOC-081 – Legal-8-Example - Notice to Client GravityZone Console.pdf

Observations:
Coalfire reviewed documentation and confirmed that policies and procedures related to breach notification by a business associate were in place and addressed providing the covered entity with the identification of each individual whose unsecured PHI was compromised, as well as any other available information the covered entity is required to include in notification to the individual.

Coalfire inquired of management and validated that documentation related to the content of the breach notification by a business associate has been reviewed, disseminated, and implemented for the in-scope environment.

Coalfire inquired of management and confirmed that no breaches occurred during the review period.

Gaps Noted:
None

Recommendations

None

Breach Notification Rule – §164.404 – 164.414	
Law Enforcement Delay – 164.412	
Law Enforcement Delay – 164.412	**Status**
If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-078 – IS-7-ISM250 BC_DR Communication on Security Incidents.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures related to breach notification were in place and addressed delaying the notification of a breach in response to a law enforcement statement that a notice or posting would impede a criminal investigation or damage national security. Coalfire inquired of management and validated that documentation related to requests from law enforcement for delay in breach notification has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire inquired of management and confirmed that no breaches occurred during the review period. **Gaps Noted:** None	
Recommendations	
None	

Breach Notification Rule – §164.404 – 164.414	
Administrative Requirements and Burden of Proof – 164.414	
Administrative Requirements and Burden of Proof – 164.414(b)	**Status**
Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.	●
Control Observations/Gaps Noted	
Documents/Evidence Reviewed: DOC-019 – B2B2C - 50 - ISM311 Records Retention Schedule.pdf DOC-031 – IS-53-IS050 Security Incident Response Policy.pdf DOC-032 – IS-53-IS051 Security Incident Response Plan.pdf DOC-047 – Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf DOC-078 – IS-7-ISM250 BC_DR Communication on Security Incidents.pdf DOC-080 – Legal-8-data breach notification_RO DPAuthority.pdf DOC-081 – Legal-8-Example - Notice to Client GravityZone Console.pdf **Observations:** Coalfire reviewed documentation and confirmed that policies and procedures were in place to address: • Making breach notifications as required or demonstrating that the use or disclosure of the PHI did not constitute a breach of unsecured PHI. • Retention of all related documentation to the notification and the use or disclosure of the PHI to satisfy the burden of proof. Coalfire inquired of management and validated that documentation related to the burden of proof has been reviewed, disseminated, and implemented for the in-scope environment. Coalfire inquired of management and confirmed that no breaches occurred during the review period. **Gaps Noted:** None	
Recommendations	
None	

Table 0-6: Breach Notification Rule – §164.404 – 164.414

Documentation Reviewed

This section lists all documents and evidence reviewed as part of the assessment. Every item listed in the table below exists on the Coalfire portal. While not all documents listed are directly relevant to the assessment, all documents uploaded to, and available on, the Coalfire portal are included here for completeness.

Document ID	Document Filename
DOC-001	IS-51-ISM020 Information Security Organization Policy.pdf
DOC-002	IS-51-ISM010 Information Security Program Policy.pdf
DOC-003	IS-43-IS100 IT Risk Management Policy.pdf
DOC-004	IS - 42 - ISM Risks management register.xlsx
DOC-005	IS - 42 - RiskReport- Sept 2021.pdf
DOC-006	HR-21- Internal Regulation - Employee's Handbook [ENG].pdf
DOC-007	IS-47-IS140 Access Control Policy.pdf
DOC-008	Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q2.png
DOC-009	IR-19028.doc
DOC-010	Nimbus – 78 - OT - Access reviews for a sample of quarters - access review Q1.png
DOC-011	B2B2C - 77 - [#ITS-45491] INTRANET - Induction Form Submitted for Silviu Ionut Mertic 6_3_2021.pdf
DOC-012	B2B2C - 77 - [#ITS-46354] pdfs05 write access request - Silviu Mertic.pdf
DOC-013	HR-23-report Cosmin Alexandru Florea.pdf
DOC-014	141.ISD-Leavingform-171221-1533-52.pdf
DOC-015	[#CERES-24370] Remove GravityZone account - jsimon@bitdefender.com.pdf
DOC-016	term_check.PNG
DOC-017	[#ITS-45093] INTRANET - Leaving Form Submitted for Jose SIMON 5_14_2021.pdf
DOC-018	Expiration date automation.docx
DOC-019	B2B2C - 50 - ISM311 Records Retention Schedule.pdf
DOC-020	IS - 30 - training_current_users_2021.xlsx
DOC-021	IS - 31 - training_new_users_sample_2021.xlsx
DOC-022	IS - 33 - Screenshot 2021-10-22 at 13-21-47 Online Course Learning Bitdefender.png
DOC-023	IS - 34 - Newsletter subscriptions.pdf
DOC-024	IT - 88 - Screenshot of antimalware configuration.docx
DOC-025	ITG-NetworkandSystemHardeningstandardsprocedures-181021-0859-22.pdf
DOC-026	IT - 82 - Evidence of the most recent security patches applied to a sample of servers.docx
DOC-027	alert.PNG

Document ID	Document Filename
DOC-028	AWS monitoring.png
DOC-029	GCP monitoring.png
DOC-030	IT - 76 - System generated or screenshots of password and lockout configuration.docx
DOC-031	IS-53-IS050 Security Incident Response Policy.pdf
DOC-032	IS-53-IS051 Security Incident Response Plan.pdf
DOC-033	IS -95 - Incident Response Exercise Report 07.06.2021.pdf
DOC-034	IS-101-ISM200 Business Continuity Policy.pdf
DOC-035	IS-101-ISM400 Bitdefender Business Continuity Plan.pdf
DOC-036	IS - 103 - Business Continuity and Disaster Recovery Exercise Report 17 Sept 2021.pdf
DOC-037	Nimbus – 48 - Nimbus - Backup and recovery procedures.pdf
DOC-038	B2B-104-GZ- mongo_backup.sh
DOC-039	B2B-104-GZ_backup additional details.docx
DOC-040	IS-49-ISM050 Security System Development Lifecycle Policy.pdf
DOC-041	IS - 90 - Open port tasks from external scanning.html
DOC-042	Nimbus_assets_Mar_2021.html
DOC-043	VA-9367.pdf
DOC-044	Nimbus Infrastructure Penetration testing report September 2021.pdf
DOC-045	VA-10151.pdf
DOC-046	Legal 1- BAA template.docx
DOC-047	Legal-2 - 20210909 RO Business Associate Agreement Covenant Health Inc.pdf
DOC-048	IT - 85 - IT - Screenshot of a remote login to include evidence of multifactor authentication over a virtual private network connection.docx
DOC-049	HR-21- Bitdefender Code of Business Conduct.pdf
DOC-050	HR-22-Anexa la dosarul personal Florea Cosmin.pdf
DOC-051	Florea.pdf
DOC-052	HR-24-Florea Cosmin Alexandru-Anexa 3.pdf
DOC-053	Nimbus – 80 - Nimbus - System inventory of all in scope assets - Inventory 15.10-15-28.csv
DOC-054	Synoptic - Datacenter media disposal.xlsx
DOC-055	109. Evidence - C1.2 - Certificates of destruction for a sample of destroyed media [IT].docx
DOC-056	mdm_1.png
DOC-057	mdm_2.png
DOC-058	IS-50-IS020 Information and Media Disposal Policy.pdf

Document ID	Document Filename
DOC-059	B2B2C - 110 - [#GDPRCLEAN-13280] Please process a GDPR deletion for user leejmike0@gmail.com.pdf
DOC-060	B2B2C - 110 - GDPRCLEAN-13280 screenshot.png
DOC-061	IT - 104 - Screenshot of backup schedule configurations for infrastructure and databases.docx
DOC-062	IS - 136 - Bitdefender Screenlock Implementation.pdf
DOC-063	IS-137-IS111 Encryption and Key Management Standard.pdf
DOC-064	IS-137-ISM301 Information Classification Procedure.pdf
DOC-065	tls_flow_nimbus.PNG
DOC-066	tls_nimbus_nimbus.PNG
DOC-067	tls_push_nimbus.PNG
DOC-068	Nimbus – 58 - Nimbus - Encryption.pdf
DOC-069	IS-55-IS170 Log Management and Monitoring Policy.pdf
DOC-070	alert_config_panel.PNG
DOC-071	Nimbus – 35 - Nimbus - File Integrity monitoring - FIM system.pdf
DOC-072	MDR-59-Network-Segmentation-Diagram.png
DOC-073	B2B-84-RMMI-NSGReview.pdf
DOC-074	Legal-4-Procedure for approving Suppliers -non MCT agreements.pdf
DOC-075	Legal-4-Notes.docx
DOC-076	Legal-4-Procedure for approving MKT Suppliers standards agreements.pdf
DOC-077	policy_location.docx
DOC-078	IS-7-ISM250 BC_DR Communication on Security Incidents.pdf
DOC-079	Legal-8-Notes - breach notification.docx
DOC-080	Legal-8-data breach notification_RO DPAuthority.pdf
DOC-081	Legal-8-Example - Notice to Client GravityZone Console.pdf
DOC-084	B2B-60-GZ_GravityZone_Cloud_Network_Diagram.pdf
DOC-085	Nimbus-GCP-AWS-Link.png
DOC-086	Nimbus Logical.png
DOC-087	PS-9- IS300 Physical Security Policy.pdf
DOC-088	PS-9-SEC010 - Physical Access Guide.pdf
DOC-089	B2B-55-IS071 Vulnerabilities Assessment and Pentests Procedure.pdf
DOC-090	IS-51-ISM000 Policy.pdf

Environment Details

System Components and Technologies

Table B-2: Network Devices and Software identifies the network components and technologies reviewed as part of this assessment.

Network Devices/Software	
Firewalls	AWS GCP
Routers, switches, and load balancers	AWS GCP
Intrusion detection/prevention	Palo Alto

Table B-1: Network Devices and Software

Table B-3: Server Components identifies the server components and technologies reviewed as part of this assessment.

Servers	
Authentication servers	Azure Active Directory (AD) Active Directory Federation Services (ADFS)
Virtual private network (VPN) servers	Slipstreams (site-to-site VPN) FortiGate Cisco Adaptive Security Appliance VPN appliances
Web servers	GravityZone web console OEM Central Web Central Web Connect Web OEM Login
Application servers	Device42GravityZone
Database servers	Amazon Redis MongoDB GCP MySQL Amazon Relational Database Service (RDS) for MySQL
Configuration servers	AWS System Manager Ansible Puppet Windows System Center Configuration Manager (SCCM)

Table B-2: Server Components

Table B-4: Security Controls identifies the security components and technologies reviewed as part of this assessment.

Other Security Controls	
Authentication types	Single Sign On (SSO)
Data encryption at rest (e.g., laptops, smartphones, databases, servers)	AWS Encryption GCP Encryption MongoDB Encryption
Data encryption in transit (e.g., SFTP, SSL, HTTPS)	VPN TLS
Data loss prevention	N/A
Centralized log management (e.g., syslog, SIEM)	Splunk
File integrity monitoring	Zabbix ELK Stack
Internal/external wireless scanning	N/A
Change management	Jira Github Bitbucket
Data backup and disaster recovery	Veeam GCP Integrated Tools AWS Integrated Tools
User training and awareness	AbsorbLMS
Antivirus, spyware, malware, and endpoint protection	Bitdefender
Web filtering and content management	Palo Alto
Asset management	Nimbus Device42 AWS GCP
Remote access (e.g., VPN, Citrix, SSL)	VPN
Data transmission types	N/A
Network monitoring	Splunk
Mobile device management (MDM)	Microsoft Intune
Server/workstation operating systems	Windows
Patch/vulnerability management	AWS GCP Microsoft SCCM

Table B-3: Security Controls