# HIPAA Security Rule Policy & Standard

## Purpose

The purpose of this HIPAA “Security Rule” Policy is to provide a uniform method of complying with the HIPAA Security Rule, where Alight is acting as a business associate to covered entities and protecting PHI from accidental or deliberate disclosure, misuse, unauthorized access or unavailability. In accordance with the Security Rule, Alight has issued and will implement this Security Rule Policy in order to ensure the Confidentiality and Integrity of Protected Health Information “PHI”.

This Security Rule Policy is organized into three broad categories: administrative safeguards, physical safeguards and Technical Safeguards of the Security Rule adopted under HIPAA. This Security Rule Policy is designed to complement, supplement and be implemented in conjunction with Alight’s other policies and procedures. This Security Rule Policy is not, and should not be considered, a comprehensive replacement of such policies and procedures, but rather as an additional layer of protection for the security of PHI. See Section 4 for coverage matrix.

## Scope

The scope of this Policy is global, which includes all business units, all regions, and all entities of Hewitt Associates LLC (“Alight”) that handles Protected Health Information for US citizens. Alight refers to all wholly-owned subsidiaries of Hewitt Associates LLC, all subsidiaries in which Hewitt Associates LLC has a controlling interest, and all agents or authorized representatives of Hewitt Associates LLC or its subsidiaries.

## Applicable Audience

This Policy applies to all colleagues, contractors and vendors of Alight that come in contact with Protected Health Information. The term "colleague" refers to all full-time employees, part-time employees, temporary employees, and interns who provide services to Alight. The term “contractor” refers to any individual on another company’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.) who provides services to Alight. The term “vendor” refers to all other third parties with which Alight does business.

## Rationale

The Security Rule generally provides that certain entities that transmit protected health information electronically, or maintain such information in Electronic Media, must maintain reasonable and appropriate administrative, physical and Technical Safeguards in order to ensure the Integrity and Confidentiality of PHI. In addition, such entities must protect against any reasonably anticipated threats or hazards to the security or Integrity of the information and unauthorized use or disclosure of the Electronic Protected Health Information. This Security Rule Policy is intended to comply with the Security Rule, and any applicable state security rules and regulations as they relate to PHI.

## Compliance & Enforcement

Compliance with this Policy is mandatory.

Potential violations of this policy are subject to review and investigation by Alight and/or its agents. Violations of this policy may result in discipline, up to and including removal of assignment, end of contract for vendors, or termination. This is subject to the procedural requirements of the countries in which Alight operates. Alight reserves the right to refer for prosecution any violations of this policy. Violations of this policy may also result in fines from The U.S Department of Health and Human Services, and/or clients.

This Policy constitutes the current Policy with respect to its subject matter, and it supersedes and replaces all previous policies relating to its subject matter. Alight reserves the right to modify the Policy at its sole discretion at any time with the intent to update on an annual basis.

## Definitions

Unless a specific policy indicates otherwise, any defined term has the meaning ascribed to it in this Policy:

**“Administrative safeguards”** are administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of Alight’s Authorized Employees in relation to the protection of that information.

**“Authorized Employees”** means any authorized employees with access to PHI.

**“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, as amended by the health information Privacy provisions of the Health Information Technology for Economic and Clinical Health Act (“HITECH”) and the Genetic Information Nondiscrimination Act (“GINA”), as it may be further amended from time to time.

**“Physical Safeguards”** are physical measures, policies and procedures (e.g., locks and identification cards) to protect Alight’s electronic Information Systems and related buildings and equipment, from natural and environmental hazards and from unauthorized intrusion.

**“Protected Health Information”** shall mean information that is a subset of health information, including demographic information collected from an individual, and (a) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**“Security Officer”** means the means the individual identified in Section. 1. The Security Officer may delegate in writing certain of its responsibilities, as described in this Program, to other Authorized Employees. Obligations and responsibilities of the Security Officer may be performed by such Authorized Employee to the extent of the delegation.

**“Security Rule”** means the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 164, promulgated pursuant to HIPAA, as it may be amended from to time.

**“Security Rule Policy”** means the policies and procedures of Alight described herein.

**“Service Provider”** means any person to whom Alight delegates a function, activity, or service, other than in the capacity of a member of the workforce of Alight.

**“Technical Safeguards”** means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

### HIPAA Security Rule Policy & Standard Statements

### Alight’s Requirements for Global Security Services (GSS)

#### Roles & Responsibilities:

* + 1. Appoint a Security Officer responsible for development and implementation of the Policies and Procedures. The responsibility for the development, implementation and enforcement of these security policies and procedures rests with VP, Global Security Risk, Compliance and Assessments.
    2. Provide a uniform method of complying with the HIPAA Security Rule. Alight’s Global Security Services team has identified 36 security controls to meet this requirement referenced here:

<https://one.aon.net/sites/SRM/RCO/SitePages/IT%20Compliance.aspx>

* + 1. Assess potential risks and vulnerabilities to the PHI using a standard assessment process upon significant change or at least once per year. At a minimum, a description of the risk, its current level, and remediation requirements is documented. Alight assessment PHI as part of an overall risk management process.
    2. Conduct an assessment potential risks and vulnerabilities to the Confidentiality, Integrity and Availability of PHI upon significant change.
    3. Maintain a list of Information Systems currently in scope for HIPAA.
    4. Develop and maintain HIPAA Security Rule strategy and documentation.
    5. Work in collaboration with GPO to provide HIPAA Security Rule guidance to Alight business.
    6. Provide oversight for completion of HIPAA Security Rule self-assessment.
    7. Keep Alight executives and external parties informed of Alight’s HIPAA security rules status globally.

### Alight’s Requirements for Business Units handling PHI

* 1. Review and understand HIPAA and associated risk.
  2. Assign single point of contact (BU HIPAA lead) to interface with GSS and manage execution of HIPAA strategy.
  3. If a service provider is used, document roles and responsibilities of the service provider and HIPAA control ownership for Alight and service provider.
  4. Understand and conduct the compliance self-assessment requirements, including deficiency identification.
  5. Maintain ongoing compliance.
  6. Completing gap remediation identified in the self-assessment and associated costs.
  7. Notify GSS of any changes with potential to impact HIPAA scope such that an evaluation can be performed.
  8. Communicate any changes to systems in scope for HIPAA to Data Privacy and GSS through [GSS intake process](https://one.aon.net/sites/SRM/Lists/Request%20Security%20Services%20GlobalUS/AllItems.aspx#InplviewHashf0c8a375-98c2-4984-b6e4-d9fa3b642d35=)
  9. Ensure a Business Associate Agreement is in place with any service provider prior to the transfer of any PHI as stipulated under Alight’s HIPAA Privacy Policy (Section IV).

### Alight’s requirements for Service providers

* 1. PHI data should only be sent using secured transmissions and upon confirmation that an up to date Business Associate Agreement has been executed.
  2. Service providers handling health information on behalf of Alight or supporting infrastructure / application that is handling health data must be compliant with HIPAA applicable controls.
  3. HIPAA control ownership matrix must be completed to document who is responsible for executing the control and producing evidence.
  4. HIPAA schedule must be included in the contract for any services provide handling health information.

### Alight’s mapping of policy to HIPAA Security Rule Requirements

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HIPAA Security Standards | Organizational, Policies & Procedures Matrix | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
|  | | | |  | |  | | | |  | | |
| **ADMINISTRATIVE SAFEGUARDS** | | | | | | | | | | |
| **Standards** | | **Sections** | | | **Implementation Specifications** | | **Alight Policies & Standards** | | | |
| **Security Management Process** | | **164.308(a)(1)** | | | **Risk Analysis** | | 100.00 Global Information Security Policy | | | |
| 100.01 Data Security Classification Standard | | | |
| 202.00 Vulnerability & Compliance Management Policy | | | |
| 202.01 Vulnerability & Compliance Management Standard | | | |
| 203.00 Application Security Policy | | | |
| 203.01 Application Security Standard | | | |
| 401.01 Disaster Recovery Standard | | | |
| 700.00 Global Information Governance Policy | | | |
| HIPAA Security Rule Policy | | | |
| **Risk Management** | | 100.00 Global Information Security Policy | | | |
| 201.08 Internet Hosting & DMZ Standard | | | |
| 202.00 Vulnerability & Compliance Management Policy | | | |
| 202.01 Vulnerability & Compliance Standard | | | |
| 203.00 Application Security Policy | | | |
| 203.01 Application Security Standard | | | |
| HIPAA Security Rule Policy | | | |
| **Sanction Policy** | | Alight Code of Conduct | | | |
| 700.00 Global Information Governance Policy | | | |
| **Information System Activity Review** | | 201.00 Asset and Data Protection Policy | | | |
| 201.05 Platform Configuration Standard | | | |
| 201.10 Logging & Monitoring Standard | | | |
| 201.11 Network Security Infrastructure Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| **Assigned Security Responsibility** | | **164.308(a)(2)** | | | **HIPAA Security Officer** | | HIPAA Security Rule Policy | | | |
| **Workforce Security** | | **164.308(a)(3)** | | | **Authorization and/or Supervision** | | 201.01 Access Control & Authorization Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| 300.01 Physical Access Control Standard | | | |
| **Workforce Clearance Procedure** | | 201.01 Access Control & Authorization Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| **Termination Procedures** | | 201.01 Access Control & Authorization Standard | | | |
| 204.00 Mobile Device Security Policy | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| 300.08 Physical Security Audits & Compliance Standard | | | |
| 700.00 Global Information Governance Policy | | | |
| **Information Access Management** | | **164.308(a)(4)** | | | **Isolating Health Care Clearinghouse Functions** | | Not Applicable to Alight | | | |
| **Access Authorization** | | 201.00 Asset and Data Protection Policy | | | |
| 201.01 Access Control & Authorization Standard | | | |
| 201.03 Encryption Standard | | | |
| 201.05 Platform Configuration Standard | | | |
| 201.09 Remote Access Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| 300.00 Physical Security Policy | | | |
| **Access Establishment & Modification** | | 201.01 Access Control & Authorization Standard | | | |
| **Security Awareness Training** | | **164.308(a)(5)** | | | **Security Reminders** | | 209.00 Security Awareness Policy | | | |
| 209.01 Security Awareness Standard | | | |
| **Protection from Malicious Software** | | 209.01 Security Awareness Standard | | | |
| **Log-in Monitoring** | |
| **Password Management** | |
| **Security Incident Procedures** | | **164.308(a)(6)** | | | **Response and Reporting** | | 201.02 Password & Authentication Standard | | | |
| 208.00 Incident Response Policy | | | |
| 208.01 Incident Response Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| 402.00 Situation Response Policy | | | |
| 402.01 Situation Response Standard | | | |
| **Contingency Plan** | | **164.308(a)(7)** | | | **Data Backup Plan** | | 201.05 Platform Configuration Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| 300.03 Emergency Response Standard | | | |
| 401.00 Disaster Recovery Policy | | | |
| 401.01 Disaster Recovery Standard | | | |
| **Disaster Recovery Plan** | | 208.01 Incident Response Standard | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| 400.01 Business Continuity Management Standard | | | |
| 401.00 Disaster Recovery Policy | | | |
| 401.01 Disaster Recovery Standard | | | |
| **Emergency Mode Operation Plan** | | 300.07 Duty of Care Standard | | | |
| 400.00 Business Continuity Management Policy | | | |
| 400.01 Business Continuity Management Standard | | | |
| 700.00 Global Information Governance Policy | | | |
| Minimum Baseline Security Standards (MBSS) | | | |
| Alight Code of Conduct | | | |
| **Testing and Revision Procedures** | | 400.00 Business Continuity Management Policy | | | |
| 400.01 Business Continuity Management Standard | | | |
| 401.00 Disaster Recovery Policy | | | |
| 401.01 Disaster Recovery Standard | | | |
| **Application and Data Criticality Analysis** | | 100.01 Data Security Classification Standard | | | |
| 400.00 Business Continuity Management Policy | | | |
| 400.01 Business Continuity Management Standard | | | |
| 401.00 Disaster Recovery Policy | | | |
| 401.01 Disaster Recovery Standard | | | |
| **Evaluation** | | **164.308(a)(8)** | | |  | | 100.00 Global Information Security Policy | | | |
| 202.01 Vulnerability & Compliance Management Standard | | | |
| 400.00 Business Continuity Management Policy | | | |
| 401.00 Disaster Recovery Policy | | | |
| 402.00 Situation Response Policy | | | |
| HIPAA Security Rule Policy | | | |
| **Business Associate Contracts & Other Arrangements** | | **164.308(b)(1)** | | | **Written Contracts and Other Arrangements** | | 201.08 Internet Hosting & DMZ Standard | | | |
| 202.00 Vulnerability & Compliance Management Policy | | | |
| 203.00 Application Security Policy | | | |
| 600.00 Supplier Security Governance Policy | | | |
| 300.06 Security Guard Operations Standard | | | |
| 700.00 Global Information Governance Policy | | | |
| HIPAA Privacy Policy (Page #76) | | | |
| **PHYSICAL SAFEGUARDS** | | | | | | | | | | |
| **Standards** | | **Sections** | | | **Implementation Specifications** | | | **Alight Policies & Standards** | | |
| **Facility Access Controls** | | **164.310(a)(1)** | | | **Contingency Operations** | | | 300.00 Physical Security Policy | | |
| 300.01 Physical Access Control Standard | | |
| 300.02 Physical Security Systems and Space Design Standards | | |
| 300.03 Emergency Response Standard | | |
| **Facility Security Plan** | | | Minimum Baseline Security Standards (MBSS) | | |
| 201.05 Platform Configuration Standard | | |
| 300.00 Physical Security Policy | | |
| 300.02 Physical Security Systems and Space Design Standards | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| 300.05 Physical Security Equipment Maintenance Standard | | |
| 300.06 Security Guard Operations Standard | | |
| 300.08 Physical Security Audits & Compliance Standard | | |
| **Access Control and Validation Procedures** | | | 201.01 Access Control & Authorization Standard | | |
| 300.00 Physical Security Policy | | |
| 300.01 Physical Access Control Standard | | |
| 300.02 Physical Security Systems and Space Design Standards | | |
| 300.08 Physical Security Audits & Compliance Standard | | |
| **Maintenance Records** | | | 300.02 Physical Security Systems and Space Design Standards | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| 300.05 Physical Security Equipment Maintenance Standard | | |
| **Workstation use** | | **164.310(b)** | | |  | | | 201.05 Platform Configuration Standard | | |
| 300.00 Physical Security Policy | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| **Workstation Security** | | **164.310(c)** | | |  | | | 201.05 Platform Configuration Standard | | |
| 204.00 Mobile Device Security Policy | | |
| 600.00 Supplier Security Governance Policy | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| **Device & Media Controls** | | **164.310(d)(1)** | | | **Disposal** | | | 100.01 Data Security Classification Standard | | |
| 100.02 Data Destruction Standard | | |
| 204.00 Mobile Device Security Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| 700.00 Global Information Governance Policy | | |
| **Media Re-Use** | | | 100.02 Data Destruction Standard | | |
| 201.05 Platform Configuration Standard | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| **Accountability** | | | 100.01 Data Security Classification Standard | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| 700.00 Global Information Governance Policy | | |
| **Data Backup & Storage** | | | 201.05 Platform Configuration Standard | | |
| 204.00 Mobile Device Security Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
|  | |  | | |  | | |  | | |
| **TECHNICAL SAFEGUARDS** | | | | | | | | | | |
| **Standards** | | **Sections** | | | **Implementation Specifications** | | | **Alight Policies & Standards** | | |
| **Access Control** | | **164.312(a)(1)** | | | **Unique User Identification** | | | 201.01 Access Control & Authorization Standard | | |
| 201.02 Password & Authentication Standard | | |
| 201.08 Internet Hosting & DMZ Standard | | |
| Minimum Baseline Security Standards (MBSS) | | |
| **Emergency Access Procedure** | | | 201.01 Access Control & Authorization Standard | | |
| Minimum Baseline Security Standards (MBSS) | | |
| **Automatic Logoff** | | | 201.02 Password & Authentication Standard | | |
| 201.05 Platform Configuration Standard | | |
| 201.12 Wireless Network Security Standard | | |
| 204.00 Mobile Device Security Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
| **Encryption and Decryption** | | | 100.01 Data Security Classification Standard | | |
| 201.00 Asset and Data Protection Policy | | |
| 201.02 Password & Authentication Standard | | |
| 201.03 Encryption Standard | | |
| 201.05 Platform Configuration Standard | | |
| 204.00 Mobile Device Security Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
| **Audit Control** | | **164.312(b)** | | |  | | | 100.00 Global Information Security Policy | | |
| 201.05 Platform Configuration Standard | | |
| 201.10 Logging & Monitoring Standard | | |
| 201.12 Wireless Network Security Standard | | |
| 208.00 Incident Response Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
| 700.00 Global Information Governance Policy | | |
| **Integrity** | | **164.312(c )(1)** | | | **Mechanism to Authenticate Protected Health Information** | | | 100.01 Data Security Classification Standard | | |
| 201.00 Asset and Data Protection Policy | | |
| 201.01 Access Control & Authorization Standard | | |
| 201.05 Platform Configuration Standard | | |
| 201.10 Logging & Monitoring Standard | | |
| 204.00 Mobile Device Security Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
| 700.00 Global Information Governance Policy | | |
| **Person or Entity Authentication** | | **164.312(d)** | | |  | | | 201.00 Asset and Data Protection Policy | | |
| 201.01 Access Control & Authorization Standard | | |
| 201.02 Password & Authentication Standard | | |
| 201.05 Platform Configuration Standard | | |
| 201.07 Outbound Internet Access Standard | | |
| 201.09 Remote Access Standard | | |
| 201.11 Network Security Infrastructure Standard | | |
| 204.00 Mobile Device Security Policy | | |
| Minimum Baseline Security Standards (MBSS) | | |
| **Transmission Security** | | **164.312(e )(1)** | | | **Integrity Controls** | | | 100.01 Data Security Classification Standard | | |
| 201.03 Encryption Standard | | |
| 201.05 Platform Configuration Standard | | |
| 300.04 Clear Desk / Clear Screen Standard | | |
| **Encryption** | | | 100.01 Data Security Classification Standard | | |
| 201.00 Asset and Data Protection Policy | | |
| 201.03 Encryption Standard | | |
| 201.05 Platform Configuration Standard | | |
| 201.09 Remote Access Standard | | |
| 201.11 Network Security Infrastructure Standard | | |
| 201.12 Wireless Network Security Standard | | |
| Minimum Baseline Security Standards (MBSS) | | |
|  | |  | | |  | | |  | | |
| **ORGANIZATIONAL REQUIREMENTS** | | | | | | | | | | |
| **Standards** | | **Sections** | | | **Implementation Specifications** | | | **Alight Policies & Standards** | | |
| **Business associate contracts or other arrangements** | | **164.314(a)(1)** | | | **Business Associate Contracts** | | | Alight’s HIPAA Security Rule Policy | | |
| Alight’s HIPAA Privacy Policy (Section IV) | | |
|
|
|
|
|
|
|
| **Requirement for Group Health Plans** | | **164.314(b)(1)** | | | **Implementation Specifications** | | | Not Applicable to Alight | | |
|  | | |
|
|
|  | |  | |  | | | | | |  | | | | |

## Reporting a Data Breach

All data security / privacy incidents including potential compromise of card holder data should be reported to the Alight Global Emergency Operations Center at +1-866-730-1442 (Americas) or +443-569-8235 (International) or via email to [global.eoc.mailbox@aon.com](mailto:global.eoc.mailbox@aon.com).

## Applicable Standards

* Are listed in Section 4.0 Alight’s mapping of policy to HIPAA Security Rule Requirements

## References and Mandates

* HIPAA Security Standards <https://sp.aonavenue.aon.net/myaon/aonasc/en-us/law/Compliance/Pages/Site%20Pages/Global-Privacy-Office-Home.aspx>
* Alight’s HIPAA Privacy Policy

## Legal Conflicts

Alight’s Global Security Services Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight’s Global Security Services Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard of Alight shall take precedence over the more general provisions contained in Global Security Services Policies and Standards.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact the Global Data Privacy Team for further guidance.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 2.1 |
| Owner | Alight Global Security Services | Risk Controls and Assessments |
| Author(s) | Alight Global Security Services | Risk Controls and Assessments |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | September 1, 2015 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2015 September | Original | Drafted first HIPAA Security Rule Policy |
| 2.0 | 2016 August | 2016 Policy Review | Minor revisions. Changed from SRM/IRSS to GSS. Changed mapping document to reflect changes to policy |
| 2.1 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |