Point32Health

C&IS 006: CYBER AND INFORMATION SECURITY - INFORMATION ASSET MANAGEMENT STANDARD

VERSION 1.0

I. INTRODUCTION

1. AUTHORITY

responsible for the development, maintenance, and communication of the Cyber & Information Security Policy and Standard Framework.

The Enterprise Security, Privacy, and Resilience Committee is responsible for approving the Cyber & Information Security Policy and Standard Framework and any material changes to this Standard.

This Standard applies to the following subsidiaries of Point32Health, Inc.: Harvard Pilgrim Health Care, Inc., Harvard Pilgrim Health Care of New England, Inc., HPHC Insurance Company, Inc., Harvard Pilgrim Group Health Plan, Tufts Associated Health Maintenance Organization, Inc., Tufts Health Public Plans, Inc., Tufts Insurance Company, CarePartners of Connecticut, Inc., Point32Health Services, Inc. group health plans, Tufts Benefit Administrators, Inc., and Total Health Plan, Inc., their employees, contractors, and temporary workers (“colleagues”).

Point32Health may modify the Cyber & Information Security Standards at any time at its sole discretion and without prior notice, subject to the approval of the CISO.

Certain subsidiaries, offices or divisions may be subject to additional or more restrictive legal or regulatory requirements, depending on the law of the jurisdiction in which they operate.

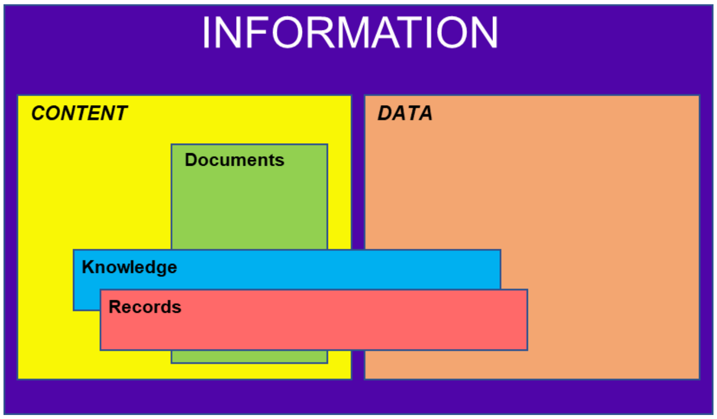
2. PURPOSE

The purpose of this Standard is to provide a documented, consistent methodology for defining the assigned level of confidentiality, or Information Classification, associated with a given Information Asset owned or managed by Point32Health. Knowing the Information Classification of an Information Asset will assist colleagues with adequately managing and protecting Point32Health Information Assets in accordance with the level of risk / sensitivity associated with the information.

3. SCOPE

The identification, classification, and associated protection of Information Assets, owned, stored, managed, or used by Point32Health representatives—regardless of media type, e.g., electronic, printed.

For purposes of this Standard and the broader Cyber & Information Security Policy Framework, ***Information*** is defined as the overarching term used to represent data (structured or unstructured), content, documents, reports, and knowledge – whether electronic, printed/physical, or verbal. The illustration below represents the definition and associated relationship information subtypes.



4. ROLES AND RESPONSIBILITIES

Specific roles and responsibilities have been created to ensure that Information Assets are managed properly throughout the organization. The role descriptions below represent the steps by which an Information Asset is classified and managed by each of the primary Information Asset roles.

a. **Cyber & Information Security** – Subject matter experts reporting into the Cyber & Information Security division of the IT Department. Provides support and consultancy to affected managers and stakeholders regarding requirements and implementation plans, develops supporting In-Practice guidance, and education.

b. **Information Asset Owner** - All Information Assets will have a designated Information Asset Owner. An Information Asset Owner is a Point32Health employee that has the ultimate accountability to establish and maintain a secure control environment to ensure confidentiality, integrity, and availability of the Information Asset for which they own.

Typically, the Information Asset Owner is the most senior manager of the business area(s) that defines the need and requirements for creation of the Information Asset (SVP). As necessary, the Information Asset Owner may delegate some of their responsibilities to an appropriate employee, e.g., Information Asset Custodian.

Other responsibilities of the Information Asset Owner include:

i. assigning the Information Classification to Information Assets they own.
ii. approving and validating levels of access to individuals or job functions, in accordance with the needs of the colleagues' job requirements;[1]
iii. periodically reviewing access to validate that permissions are still appropriate;[2]

[1] *Responsibilities may be delegated to Information Custodians; accountability may not be delegated.*

[2] *Point32Health's managed IT infrastructure (network, operating systems, etc.) control environments, and associated risks will be directly owned and managed by Point32Health's IT organization.*

iv. ensuring that Information Asset Custodians and Information Users are aware of the assigned Information Classification and expectations to handle and protect the Information Asset in accordance with the assigned classification; [2]

v. understanding security control deficiencies and associated risks related to the continued management and protection of the Information Asset(s) owned; collaborate with Information Asset Custodians and other individuals to correct known control deficiencies in a timely manner.

vi. identifying needs for the protection and monitoring of Information Assets; collaborate with IT and other business partners to determine appropriate method to implement additional security controls to address these needs; and

vii. correcting, mitigating, or accepting risks associated with a given Information Asset security control deficiency.[2]

c. **Information Asset Custodians –** An Information Asset Custodian is a Point32Health colleague that is responsible for the implementation and oversight of necessary safeguards to protect the Information Asset, as defined by the Information Asset Owner (by assigning its Information Classification). Information Asset Custodians may be a business application owner or owner an application, file share, Microsoft SharePoint site, Microsoft Teams site, etc.

i. IT Managers with responsibility for application and access management are doing so at the direction and delegation of the corresponding Information Asset Custodian.

ii. All third-party relationship owners are considered the Information Asset Custodian for all Point32Health information or systems/applications accessible by the third-party vendor/service provider.

iii. There may be more than one Information Asset Custodian of an Information Asset. External parties, including trusted partners, contingent resources, and outsourced providers are not authorized to be a Point32Health Information Asset Custodian.

iv. Responsibilities of Information Asset Custodians include:

- ensuring that access is strictly limited to the roles, individuals, and permissions required for the colleague(s) to effectively complete their job responsibilities; and
- notifying Information Asset Owners of security control deficiencies and associated recommendations. Information Asset Custodians must collaborate with Information Asset Owners to address identified security control deficiencies, in accordance with the Information Asset Owner's expectations

d. **Point32Health Managers** – All employees with a job title referencing the term "manager" or having one or more colleagues reporting directly and/or indirectly to them. Point32Health Managers are responsible for awareness of the Information Security Standards and ensuring that applicable requirements defined within these Standards are adhered to within their areas of responsibility.

If unable to comply with the published Standards, the responsible Point32Health Manager must notify Cyber & Information Security of any variance per the published Risk Assessment Standard.

e. **Information User** ("Colleagues") – Any Point32Health colleague, contractor, contingent worker, or temporary resource, with access to information assets or any person who uses Point32Health information assets to perform their job responsibilities. Responsibilities of information users include:

i. Ensuring that access, management, and use of information meets or exceeds the requirements defined by the Information Asset Classification assigned by the Information Asset Owner.

ii. Protecting the accessibility and disclosure of information, both consciously or inadvertently, by locking devices when not actively in use and not displaying or disclosing information to any individual not approved for access based on job requirements. Notifying management immediately if:

- access to Restricted or Highly Restricted Information Assets is available outside of the scope of their role and responsibilities, or
- information has been lost or stolen—regardless of device or media type (laptop, personal device, removable media, printed materials, etc.).

iii. Always securing laptops, desktop computers, mobile devices, portable storage media, and printed materials containing Point32Health information.

iv. Properly safeguarding all account login credentials for which you are authorized; never share personal login credentials.

v. Notifying the IT Customer Support Center (IT Help Desk) immediately if there is any reason to believe that they have fallen victim to any type of social engineering attack (e.g., email phishing, text-based "smishing", phone call, etc.), *especially* an attack that may have resulted in downloading software, theft of any login credentials, credit card information or bank account information, purchasing of goods (e.g., gift cards), unauthorized access to computers, or any other suspicious activity.

II. STANDARD

This Standard provides requirements related to the identification, management, handling, use, and protection of Information Assets in accordance with Point32Health's Cyber & Information Security Policy.

INFORMATION CLASSIFICATION

a. An Information Asset is information that is owned or managed by Point32Health. It includes any type of information that, if lost, stolen, modified, misused, or deleted, destroyed, or made unavailable could impact Point32Health's reputation, cause financial impact, reduce the organization's ability to meet regulatory, legal, or contractual obligations, or affect Point32Health's ability to deliver products and services.

b. Each Information Asset must indicate its level of confidentiality (effectively the level of impact to Point32Health if the Information Asset is disclosed to unauthorized parties).and associated diligence required to protect it.

Information Asset classification is essential to:

i. ensure Information Assets are known and managed in accordance with their level of confidentiality, and

ii. assist Information Custodians and Information Users to identify and manage information in accordance with the Information Asset Classification assigned by the Information Asset Owner.

c. Point32Health must use the following Information Asset Classification labels:

i. **Public** – No meaningful negative impact to Point32Health if disclosed, internally or externally. Information in this category is generally intended for public consumption and has been approved for such use. Information Assets in this category may be shared with internal or external parties for approved Point32Health business purposes.

ii. **General Business** – May result in moderate negative impact to Point32Health if disclosed to unauthorized parties. Includes general business information about Point32Health's organizational structure, practices, processes, and policies. May be shared with internal colleagues and trusted external parties (contractual protections are firmly in place) when required to achieve Point32Health's business objectives.

iii. **Restricted** – May result in material negative impact to Point32Health if disclosed to unauthorized parties. Information in this category includes sensitive business information, including information that must be protected to meet legal, contractual, regulatory obligations, e.g., personal information, protected health information. Access is limited to employees and specifically authorized external parties that require it to achieve specific job responsibilities or contractual obligations with Point32Health.

iv. **Highly Restricted** – Unauthorized disclosure of information in this category may result in severe negative impact to the Point32Health organization. Access is strictly limited to named individuals only. Information in this category should never be shared with others unless authorized, in writing, by the Information Asset Owner – whether internal or external.

v. **Confidential** – This term is used for legal and regulatory compliance needs only. For purposes of this document, the classification of “Confidential” represents all information that is owned or managed by or on behalf of the Point32Health organization. This term or classification should not be used to classify or label information of any type, unless directed to do so by a representative of the Point32Health Legal or Compliance departments.

Note: If the Information Asset Classification of a given Information Asset is not known, is not clearly in the public domain, and is not clearly determined by referring to the examples within this document, it must be assumed to be “Restricted” until such time that the classification can be provided by an employee that is knowledgeable about the specific Information Asset’s classification.

The following guide should be used as a reference for the definition, examples, labeling, storage, distribution, transmission, and disposal of Information Assets – regardless of media types.

Information Classification	**Public**	**General Business**	**Restricted**	**Highly Restricted**
Definition	No meaningful negative impact to Point32Health if disclosed, internally or externally. Information in this category is generally intended for public consumption and has been approved for such use. Information Assets in this category may be shared with internal or external parties for approved Point32Health business purposes.	May result in moderate negative impact to Point32Health if disclosed to unauthorized parties. Includes general business information about Point32Health's organizational structure, practices, processes, and policies. Maybe be shared with internal colleagues and trusted external parties (contractual protections are firmly in place) when required to achieve Point32Health's business objectives.	May result in material negative impact to Point32Health if disclosed to unauthorized parties. Information in this category includes sensitive business information, including information that must be protected to meet legal, contractual, regulatory obligations, e.g., PI (Personal Information), PHI (Protected Health Information). Access is limited to employees and specifically authorized external parties that require it to achieve specific job responsibilities or contractual obligations with Point32Health.	Unauthorized disclosure of information in this category may result in severe negative impact to the Point32Health organization. Access is strictly limited to named individuals only. Information in this category should never be shared with others unless authorized, in writing, by the Information Asset Owner – whether internal or external.
Examples	• Annual Report (published) • Public websites • Regulatory filings (published) • Marketing materials • News releases	• Policies, processes, and procedures • Code of Conduct • Employee benefits • Organizational charts • Internal contact information • Internal memos, communications • Contract and other templates	• Personal information, protected health information (PI/PHI) • Customer lists, contact information • Financials, e.g., budget, projects, financial planning • Pricing, underwriting, claims information • IT architecture, designs, and system configurations • Legal contracts, matters of litigation • Risks, issues, and vulnerability information • System/security event logs, alerts, escalations • Incident related information • Detailed procedures • Strategic plans, e.g., products, dept, business	• Individually assigned credentials, passwords • Private keys, certificates • Board of Directors presentation documents, meeting notes, minutes • Executive succession planning • Annual Report (un-published) • Merger & Acquisition information

Information Asset Protection and Handling Requirements

Note: Information Assets intended for public audiences are not required to be protected or labeled in its final version. While these materials are being drafted and not yet approved for public distribution, they should be assigned an alternate Information Asset Classification.

Handling and Protection Requirements	**Highly Restricted**	**Restricted**	**General Use**
Use document footers or other methods to effectively label information with its Information Asset Classification	X	X	X
Do not print on shared printers outside of a Point32Health or home office, e.g., hotel, library, airport	X	X	X
Protect printed materials with lock and key when not *actively* in use - includes at Point32Health and home office	X	X	
Shred or place printed materials in designated shred bins at a Point32Health facility	X	X	X
Restrict access within approved repositories to authorized roles/job titles that require it to meet job requirements	X	X	X
Restrict access within approved repositories to specifically named and authorized individuals	X		
Do not share or discuss with colleagues that do not have a legitimate business need and have not been authorized	X	X	X
Use MS Teams, SharePoint, or OneDrive "share" options to collaborate with colleagues instead of emailing copies	X	X	
Avoid retaining local ("convenience") copies in email, folders, and printed materials when task/project has completed	X	X	X
Must be encrypted while structured data is stored - internally or externally, e.g., databases, data warehouses	X	X	
Must be encrypted while stored in any format - internally or externally, e.g., file shares, OneDrive, MS Teams	X		
Encrypt when writing information to portable storage media (e.g., USB thumb drives, portable hard disks, CD/DVD)	X	X	
Do not share or discuss information with external parties unless approved by Procurement, Privacy, and Security	X	X	X
Do not store or transmit to external locations, unless approved by Procurement, Privacy, and Security	X	X	
Must be encrypted while transmitted to external parties or locations (only after being approved, authorized)	X	X	
Must be encrypted while transmitted within the internally managed Point32Health computing environment	X	X	
Do not discuss in areas where unauthorized parties may overhear - within a Point32Health office	X	X	
Do not discuss where unauthorized parties may overhear - outside of a Point32Health office	X	X	X
Must be permanently destroyed via electronic or physical means (e.g., paper shredder) when no longer required	X	X	

- Information Users may only store Point32Health Information Assets on approved equipment (e.g., Point32Health managed laptops/desktops, servers, etc.), unless authorized by the Information Owner or approved through the Cyber & Information Security Risk Assessment process and by Privacy.
- Information Assets identified as an official record within the organization’s Records Retention schedule must be protected against unauthorized modification or destruction. Not all repositories are authorized to host official company Records – engage with Cyber & Information Security for more details.
- The specific security requirements for protecting an Information Asset are determined by the assigned Information Classification.

III. EXCEPTION MANAGEMENT

Inability to meet the requirements set forth in this Information Security Standard poses a potential risk to the Point32Health organization. As such, any variance must be shared with Cyber & Information Security. Cyber & Information Security will assess the risk and recommend an appropriate course of action (e.g., eliminate, correct, mitigate, or accept the identified risk).

IV. CONTACT INFORMATION

For all inquiries / questions regarding the Cyber & Information Security Policy and Standards, contact: CyberInformationSecurity@point32health.org.

V. REFERENCE DOCUMENTS

VI. REVISION HISTORY

Version	Effective Date	Changed By	Change Description
1.0	April 1, 2024	Cyber & Information Security; Legal, Compliance, Privacy, and other SMEs and stakeholders	Initial publication

All material changes reflected in the latest version of this Standard will become effective 90 calendar days after publication of the Standard. During the 90-day period, impacted technical and business stakeholders must complete a gap analysis and provide a recommended target to the CISO for applying material security changes to the existing environment, where applicable.