Point32Health

CYBER & INFORMATION SECURITY POLICY

Version 1.0

Purpose

Point32Health's Information Assets (and underlying technology infrastructure systems, applications, and services), whether under our direct control or managed by a third-party service provider on behalf of Point32Health must be protected against unauthorized information disclosure, misuse, modification, compromise, corruption, destruction, and disruption of core business services. The purpose of this Cyber & Information Security Policy is to establish a single, company-wide, framework for appropriately securing Point32Health's Information Assets.

Information Assets take on many forms, ranging from data stored in a database, electronic medical records, financial reports, legal contracts, email messages, customer lists, employee information, and internal company policies, just to cite a few diverse examples. Regardless of how information is created, communicated, used, and stored, it is the responsibility of Point32Health to protect it. Further, use of these assets must adhere with applicable statutory, regulatory, and contractual obligations.

The protection of these assets is essential to managing our risk at business-unit and company-wide levels. Point32Health also recognizes its role in the stewardship of Information Assets entrusted to us by our customers and business partners. Therefore, appropriate steps must be taken to protect all Information Assets regardless of whether they belong to Point32Health, any of its subsidiaries or affiliated companies, its customers, partners, vendors, consultants, subcontractors, contingent workers, or employees.

Cyber and information security is assured when the requirements for confidentiality, integrity, and availability for each asset are fulfilled. These requirements include:

- Safeguarding of non-public, information from unauthorized disclosure and restricting user access to information based on business needs and minimal necessary standards.
- Ensuring accuracy and consistency in data and protecting it from unauthorized access, destruction, or modification.
- Managing information access and maintaining an appropriate control environment
- Ensuring availability of and access to information, systems, applications, and services based upon business need

An Information Asset must be protected to an extent and for a period relative to its value and the degree of adverse impact that could result from its unauthorized disclosure, modification, misuse, destruction, or unavailability.

Maintenance of this policy and oversight to its implementation has been assigned to the Point32Health Enterprise Security, Privacy, and Resilience Committee. Comments may be directed to CyberInformationSecurity@point32health.org.

Governance

Ownership

All Information Assets will have a designated Information Owner. An Information 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(s) they own. Typically, the Information (Asset) Owner is the most senior manager of the business area(s) and is responsible for defining the need and requirements for creation of the Information Asset. As necessary, the Information Owner may delegate some of these responsibilities to an appropriate Point32Health employee.

Information Custodian

An Information Custodian is a Point32Health employee that is responsible for the implementation and oversight of necessary safeguards to protect an Information Asset, as defined by the Information Owner.

The Custodian must define the rights and entitlements of Information Assets under their responsibility. The assigned rights and entitlements must be limited to those that are specifically required for the individual or those in predefined roles to complete their job responsibilities ("principle of least privilege").

Information Custodians may be a third-party service provider relationship owner, business application owner, product owner, Microsoft SharePoint site owner, file share owner, etc. Point32Health technology owners (e.g., IT department, HRIS) responsible for the architecture, design, implementation, maintenance, and continued support of technology infrastructure, systems, applications, databases, and utilities are also considered Information Custodians and are required to maintain a technology control environment to adequately protect Information Assets hosted, used, stored, transmitted, accessed, analyzed, or destroyed from unauthorized use, modification, destruction, or access disruption.

Information User

An employee, contractor, consultant, or contingent worker ("colleagues") with access to Information Assets; a person who uses Point32Health Information Assets to perform their job functions.

Classification

All Information Assets must be classified based upon its sensitivity within one of the following four categories: Public, General Business, Restricted, and Highly Restricted.

Information Assets whose classification is not known, labeled, or not obviously in the public domain must not be freely circulated or otherwise left unprotected. Information Assets are assumed to be classified as "Restricted" until such time that the classification can confidently be assigned via review of guidance materials available on the Point32Health intranet or has been confirmed by the Information Owner, or an authorized delegate.

Public information has no meaningful adverse 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.

General Business information may result in moderate adverse 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 appropriate internal colleagues and trusted external parties (when contractual protections are firmly in place) when required to achieve Point32Health's business objectives.

Restricted information may result in material adverse 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, and regulatory obligations, e.g., personal information, protected health information. Access is limited to employees with a need-to-know or have access to this information in the performance of their job duties and specifically authorized external parties that require it to achieve specific job responsibilities or contractual obligations with Point32Health.

Highly Restricted information may result in severe adverse impact to Point32Health if disclosed to unauthorized parties. Access is strictly limited to named individuals only. Information in this category should never be shared with others (whether internal or external) unless authorized, in writing, by the Information Asset Owner.

Confidential information is the term 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.

Cyber & Information Security Standards exist to provide clear objectives and requirements for using, sharing, transmitting, storing, and disposing of Point32Health Information Assets.

The Information Owner assigns the classification of Information Assets and is accountable for the associated security risks.

Managing Entitlements

All users must be individually authenticated prior to accessing any Point32Health Information Asset or supporting technology.

Point32Health colleagues will be granted access to the parts of the system, processes, and products necessary for them to fulfill designated responsibilities. This means that some business processes may require separate duties and segregations of roles and responsibilities to ensure an effective control environment.

Role-based entitlements are used to align access permissions with pre-defined roles in support of Point32Health's business processes. The roles, and their associated responsibilities, are consistently defined, documented, and maintained. External access to Information Assets by members, customers, providers, and other business partners must be derived from the business relationship, with entitlements aligned to the activities and responsibilities needed to complete the business process.

Responsibility

Responsibility for the protection of Information Assets rests with all Point32Health colleagues at every level. Managers are responsible for ensuring awareness of and adherence to this policy and all supporting standards.

The need to ensure confidentiality, integrity, and availability of Point32Health Information Assets imposes certain responsibilities upon the users of the resources. All colleagues are required to comply with Point32Health's Cyber & Information Security Policy, standards, guidelines, and procedures. Users must access Information Assets responsibly and in accordance with Point32Health Privacy Policies and accept their obligation to maintain confidentiality and not disclose company information to unauthorized parties.

Each colleague has a responsibility to prevent unauthorized access to Information Assets, including unintended access by people outside of the organization such as relatives, friends, customers, business partners, vendors, and visitors. Colleagues are responsible for the following:

- Protecting the Information Assets being accessed by complying with applicable security controls, standards, and procedures.
- Notifying their manager or supervisor immediately if they can access information outside of the scope of their role and responsibilities.
- Protecting laptops, mobile devices, portable media, documents, and printed materials that may contain non-public Point32Health information at all times.
- Ensuring that information is stored, accessed, and shared only via secure, authorized means.

Security Education and Awareness

Security education must be provided for all Information Owners, Information Custodians, and Information Users to ensure that they are aware and understand their responsibilities concerning the use, management, and protection of information. The degree of education and awareness must be aligned with the risk associated with the colleague's role within the control environment.

Third-party Security

Standards, procedures, and controls must be in place to assure that third-party contracts and security capabilities provide for the protection of Point32Health's Information and Technology Assets.

Access

Prior to accessing Point32Health Information Assets and supporting technology, all internal and authorized external users must be positively and uniquely identified and authenticated. Processes must be developed, documented, and followed for requesting, reviewing, approving, and maintaining user access to Point32Health's Information Assets, including adjustments in access due to changes in a role. Access must be periodically reviewed to ensure alignment to current role and entitlements.

The Point32Health access control infrastructure includes both physical and technical controls. Supporting security standards and physical safeguards must be implemented to protect the operating facilities, corporate network, servers, workstations, applications, and servers owned and operated by Point32Health.

All Point32Health networks, regardless of private or public connectivity, must be protected from unauthorized use or access. An approved remote access solution must be the only remote connection method into the corporate network. Any device or application connecting to the corporate network must meet established standards.

Acceptable Use

Authorized Use

Users are authorized to use Point32Health Information Assets that correspond to their role, responsibilities, and entitlements. Further, the use of Information Assets must respect employee, member, customer, and business confidentiality, including vendor contractual restrictions; colleague privacy; and all legal restrictions including copyright and trademark.

Introduction of unauthorized information, software, and hardware to Point32Health's environment is forbidden. Users must obtain approval from Point32Health's IT department prior to installation of any applications or devices on Point32Health's technology environment.

Communication Services

Appropriate care must be taken when accessing, using, storing, sharing, and transmitting Information Assets. The communication services, networks, and other infrastructure components must be used appropriately to ensure those assets are protected. Colleagues must exercise caution when transferring or storing all non-public information outside of the Point32Health environment; in these cases, users are limited to using only those solutions and protocols specifically approved by Point32Health's IT department.

Point32Health makes certain electronic communication services available to its colleagues to enhance their ability to do their job. Colleagues will have access to email, instant messaging tools, social media, telephone, collaboration and productivity tools, computer software and other software, and the Internet.

Point32Health provides such systems to enable colleagues to conduct necessary business functions. Good judgement, good taste, common sense, policy compliance, and respect for Point32Health and those with whom Point32Health does business, must always guide usage. Professional workplace standards apply. Access may not be used to solicit or advance other personal or commercial interests.

Colleagues are not permitted to access, create, transmit, store, or receive any offensive, discriminatory, or disruptive messages. These include any messages containing sexual implications, profanity, racial slurs, gender-specific comments or any other comment that offensively address anyone's age, creed, gender, sexual orientation, religious beliefs, race, color, ancestry, ethnic origin, place of origin, citizenship, language, marital, civil, social, or family status or condition, past criminal convictions, records of offences, pregnancy or disability, or any other ground protected under human rights legislation.

Communication services are reserved for business use and all information transmitted through them is company property. While incidental personal use is allowed, it is expected that the colleague's work will

not be impacted by such use. All messages, communications, and files composed, transmitted, stored, or received on these systems are and remain the property of Point32Health. Internet access will be managed through Point32health's corporate security infrastructure.

Policy Violations and Investigations

All colleagues are responsible for notifying incident@point32health.org of any suspicious activity, security breaches, or violations of this policy, including cyber and information security failures, and incidents. Colleagues may also anonymously report by contacting the Compliance, Fraud, Waste & Abuse, and Cybersecurity Hotline at 1-877-548-6712 or via the web at: https://point32health.ethicspoint.com.

If an abuse of this policy is confirmed, managers, working with Human Resources, have the authority to take disciplinary action, up to and including termination of employment.

Once a security incident is identified, steps will be taken to limit further impact to Information Assets or supporting technology and assist with the identification of violators. Depending upon the type and severity of the incident, law enforcement may also be engaged.

Documentation, including audit logs, analysis, reports, and meeting notes must be produced, and kept by Cyber & Information Security to assist in future investigations. Records of adverse security events must be maintained to provide sufficient information to support comprehensive audits of the effectiveness of and compliance with security measures. Records must be reviewed periodically.

Computer and Communication Systems

If computer or communication systems are involved in a suspected incident, an initial response may be to review access for failure and unusual use. Further, various statutes and regulations allow employers to monitor colleagues' electronic communications to detect unauthorized access and misuse without prior notice. The company reserves and intends to exercise this right to review, audit, intercept, access, and disclose any message created, received, or sent over Point32Health's communication systems for any purpose. Intrusion detection and prevention systems may be used to perform real-time monitoring of sensitive Information Assets and detect attempted unauthorized access. Monitoring procedures must be documented in accordance with company procedures to ensure adherence.

Supporting Documentation

Supporting and approved Cyber & Information Standards are incorporated by reference herein and represent Point32Health's Cyber & Information Security Policy.

Revision History

Version	Approved Date	Published Date	Changed By	Change Description
1.0		April 1, 2024	Cyber & Information Security, various internal SME stakeholders	Initial publication