Cylerity Corporation

Information Security Policy

Document Owner	Kenneth Penkowski Chief Product Officer, Cylerity Corporation kenneth.penkowski@cylerity.com (888) 803-3886 x888
Last Revision Date	7 January, 2022
Approval Date	7 January, 2022
Effective Date	7 January, 2022

Contents

Introduction

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Cylerity Corporation, hereinafter, referred to as Cylerity. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Cylerity with policies and guidelines concerning the acceptable use of Cylerity technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Cylerity employees or temporary workers at all locations and by contractors working with the Cylerity as subcontractors.

Scope

This policy document defines common security requirements for all Cylerity personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of Cylerity, entities in the private sector, in cases where Cylerity has a legal, contractual or fiduciary duty to protect said resources while in Cylerity's custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Cylerity network system which is comprised of various hardware, software, communication equipment and other devices designed to assist Cylerity in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Cylerity domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Cylerity at its office locations or at remote locales.

Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

- **CEO –** The Chief Executive Officer is responsible for the overall privacy and security Cylerity's of the company.
- **CIO** – The Chief Information Officer
- **CPO –** The Chief Privacy Officer is responsible for HIPAA privacy compliance issues.
- **CST** – Confidentiality and Security Team
- **Encryption** – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
- **External Media –**flash drives, USB keys, thumb drives.
- **Firewall –** a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
- **FTP** – File Transfer Protocol
- **HIPAA** - Health Insurance Portability and Accountability Act
- **IT** - Information Technology
- **LAN** – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
- **NTFS –** New Technology File Systems – NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.
- **SOW - Statement of Work -** An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.
- **User** - Any person authorized to access an information resource.
- **Privileged Users –** system administrators and others specifically identified and authorized by Cylerity management.
- **Users with edit/update capabilities –** individuals who are permitted, based on job assignment, to add, delete, or change records in a database.
- **Users with inquiry (read only) capabilities –** individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.
- **VLAN –** Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

- VPN – Virtual Private Network – Provides a secure passage through the public Internet.
- WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.
- Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

Privacy Officer

Cylerity has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of the Cylerity privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for the Cylerity is:

Kenneth Penkowski
Chief Product Officer, Cylerity Corporation
kenneth.penkowski@cylerity.com
(888) 803-3886 x888

Confidentiality / Security Team (CST)

The Cylerity has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Cylerity and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Quality Council in a new calendar year. This committee will consist of the positions within the Cylerity most responsible for the overall security policy planning of the organization- the CEO, PO, CMO, ISO, and the CIO (where applicable). The current members of the CST are:

- Ryan Wheeler, Chief Executive Officer
- Kenneth Penkowski, Chief Product Officer

The CST will meet quarterly to discuss security issues and to review concerns that arose during the quarter. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within the Cylerity and act as the first line of defense in enhancing the security posture of the Cylerity.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

The Privacy Officer (PO) or other assigned personnel is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by the Cylerity. This log will also be reviewed during the quarterly meetings.

Employee Responsibilities

Employee Requirements

The first line of defense in data security is the individual Cylerity employees. Cylerity employees are responsible for the security of all data which may come to them in whatever format. The Cylerity is responsible for maintaining ongoing training programs to inform all users of these requirements.

- Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Cylerity policy states that all computers will have the automatic screen lock function set to automatically activate upon 30 minutes of inactivity. Employees are not allowed to take any action which would override this setting.
- Home Use of Cylerity Corporate Assets - Only computer hardware and software owned by and installed by Cylerity is permitted to be connected to or installed on Cylerity equipment. Only software that has been approved for corporate use by the Cylerity may be installed on Cylerity equipment. Personal computers supplied by Cylerity are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Cylerity for home use.
- Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Cylerity are the property of the Cylerity unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Cylerity employees at their own expense.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.

- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
- Exception: Authorized information system support personnel, or others authorized by the Cylerity Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Cylerity has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Cylerity computers must be approved by Cylerity.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by Cylerity is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of Cylerity is strictly prohibited.

Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, Cylerity encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Cylerity owned equipment are considered the property of the Cylerity – not the property of individual users. Consequently, this policy applies to all Cylerity employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, Slack, Dropbox, voice mail, instant messaging, Internet, personal computers, and servers.

Cylerity provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
b) Illegal activities – Use of Cylerity information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
c) Commercial use – Use of Cylerity information resources for personal or commercial profit is strictly prohibited.
d) Political Activities – All political activities are strictly prohibited on Cylerity premises. Cylerity encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Cylerity assets or resources.
e) Harassment – The Cylerity strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, Cylerity prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is NOT the policy of the Cylerity to monitor the content of any electronic communication, Cylerity is responsible for servicing and protecting the Cylerity's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Cylerity reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Cylerity policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

Internet Access

Internet access is provided for Cylerity users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by Cylerity should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Reporting Software Malfunctions

Users should inform the appropriate Cylerity personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, Cylerity computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.

- Inform the appropriate personnel or Cylerity ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

Report Security Incidents

It is the responsibility of each Cylerity employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Cylerity CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Cylerity CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Cylerity Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by Cylerity and hold all data

in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Cylerity policy and will result in personnel action, and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on Cylerity computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Cylerity purchased software on home or on non-Cylerity computers or equipment.

Cylerity proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of Cylerity without written consent of the respective supervisor or department head. It is crucial to Cylerity to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Cylerity data to a non-Cylerity Computer System, the supervisor or department head should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

Internet Considerations

Special precautions are required to block Internet (public) access to Cylerity information resources not intended for public access, and to protect confidential Cylerity information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Cylerity Privacy Officer or appropriate personnel authorized by the Cylerity shall be obtained before:

- An Internet, or other external network connection, is established;
- Cylerity information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the Cylerity. The network can be used to market services related to Cylerity, however use of the network for personal profit or gain is prohibited.

- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Cylerity Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Installation of authentication and encryption certificates on the e-mail system

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

Use of WinZip encrypted and zipped e-mail

This software allows Cylerity personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Cylerity staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

De-identification / Re-identification of Personal Health Information (PHI)

As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged.

De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.

PHI includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state

- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

Identification and Authentication

User Logon IDs

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are audited at least twice yearly[13] and all inactive logon IDs are revoked. The Cylerity Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3)[14] unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Cylerity systems or networks must have a completed and signed Network Access Form (Appendix C). This form must be signed by the supervisor or department head of each user requesting access.

Passwords

User Account Passwords

User IDs and passwords are required in order to gain access to all Cylerity networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

- Password Length – Passwords are required to be a minimum of eight characters, but Cylerity recommends novel and memorable phrases up to 64 characters[15].
- Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

- Change Frequency – Passwords must be changed every 120 days[16]. Compromised passwords shall be changed immediately.
- Reuse - The previous twelve[17] passwords cannot be reused.
- Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.
- Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

Confidentiality Agreement

Users of Cylerity information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix D). The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the Cylerity information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Cylerity information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Request Form (Appendix C). This form can only be initiated by the appropriate department head, and must be signed by the department head and the Security Officer or appropriate personnel.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the information system, only upon the signature of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

User Login Entitlement Reviews

If an employee changes positions at the Cylerity, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by indicating on the Network Access Request Form (Appendix C) both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the Form so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

No less than annually, the IT Manager shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate HIPAA compliance and protect patient data.

Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department by indicating "Remove Access" on the

employee's Network Access Request Form (Appendix C) and submitting the Form to the IT Department. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the IT Department of employee's last scheduled work day so that their user account(s) can be configured to expire. The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as Cylerity equipment and property is returned to the Cylerity prior to the employee leaving the Cylerity on their final day of employment.

No less than quarterly, the IT Manager or their designee shall provide a list of active user accounts for both network and application access to department heads for review. Department heads shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by the Cylerity, the department head will immediately notify the IT Department of the employee's termination status and submit the updated Network Access Request Form (Appendix C).

Malicious Code

Antivirus Software Installation

Antivirus software is installed on all Cylerity personal computers.

- Configuration - The antivirus software currently implemented by the Cylerity is Norton Antivirus[18].
- Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.
- Monitoring/Reporting –Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

New Software Distribution

Only software created by Cylerity application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix C. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Cylerity computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage Cylerity hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Cylerity computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Cylerity personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Cylerity computer or network.

Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not "bootable".

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Cylerity are the property of the Cylerity unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Cylerity ownership at the time of employment. Nothing contained herein applies to software purchased by Cylerity employees at their own expense.

Encryption

Definition

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

Encryption Key

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, Cylerity shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. Cylerity employs several methods of secure data transmission.

S/MIME (secure/Multipurpose internet mail extensions)

A widely accepted protocol for sending digitally signed and encrypted messages. S/MIME in Exchange Online provides the following services for email messages:

- Encryption: Protects the content of email messages.
- Digital signatures: Verifies the identity of the sender of an email message.

File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

Transport Layer Security (TLS)

Cylerity uses TLS 1.2 or higher for data in transit.

Advanced Encryption Standard (AES)-256

Cylerity uses AES-256 for data at rest.

Telecommuting

SARS-CoV-2 has changed how the world goes to work. For the health of Cylerity employees and our contractors, we have embraced telecommuting for the foreseeable future.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and data security. Workers accessing Cylerity's cloud-based infrastructure present additional environments that must be protected against spreading Trojans, viruses, or other malware.

General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- Need to Know: Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- Password Use: The use of a strong password, changed at least every 120 days[21], is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- Training: Personnel who telecommute must complete the same annual privacy training as all other employees.
- Contract Specific: There may be additional requirements specific to the individual contracts to which an employee is assigned.

Required Equipment

Employees approved for telecommuting must understand that the Cylerity will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

Cylerity Provided:

- Cylerity supplied workstation.
- A cable lock to secure the workstation to a fixed object.
- If using VPN, a Cylerity issued hardware firewall is required.
- If printing, a Cylerity supplied printer.

Employee Provided:

- Broadband internet connection,
- Paper shredder,
- Secure office environment isolated from visitors and family,
- A lockable file cabinet or safe to secure documents when away from the home office.

Hardware Security Protections

Virus Protection

Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Cylerity personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use

Established procedures must be rigidly followed when accessing Cylerity information of any type. The Cylerity requires the use of VPN software and a firewall device.

Security Locks

Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens

No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 30[23] minutes of inactivity.

Data Security Protection

Data Backup

Backup procedures have been established that encrypt the data being moved to encrypted cloud storage in Microsoft Azure. Use only that procedure – do not create one on your own. If there is not a backup procedure established, or if you have external media that is not encrypted, contact the appropriate Cylerity personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to the Cylerity

Transferring of data to Cylerity requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Cylerity.

External System Access

If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail

Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Cylerity Networks

Extreme care must be taken when connecting Cylerity equipment to a home or hotel network. Although the Cylerity actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Cylerity has no ability to monitor or control the security procedures on non-Cylerity networks.

Protect Data in Your Possession

View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers

Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location

Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Cylerity

All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement.

Shredding

All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Cylerity work environment, MUST have direct access to a shredder.

Disposal of Electronic Media

All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The Privacy Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

Specific Protocols and Devices

Wireless Usage Standards and Policy

This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Cylerity laptops and mobile devices.

Approval Procedure

In order to be granted the ability to utilize the wireless network interface on your Cylerity laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the Privacy Officer or appropriate personnel of the Cylerity. The Network Access Request Form (found in Appendix A) is used to make such a request. Once this form is completed and approved you will be contacted by appropriate Cylerity personnel to setup your laptop and schedule training.

Software Requirements

The following is a list of minimum software requirements for any Cylerity laptop that is granted the privilege to use wireless access:

- Windows 11 for x64-based Systems
- macOS Monterey 12.2 for MacBook Pro users
- Norton Antivirus software
- Full Disk Encryption
- Microsoft Edge Version 98.0.1108.43 (64-bit) or Greater
- Mozilla Firefox Version 97.0
- Google Chrome
    - Windows: Version 98.0.4758.81
    - macOS: Version 98.0.4758.81
    - Linux: Version 98.0.4758.81
    - Andriod: Version 98.0.4758.87

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.

Training Requirements

Once you have gained approval for wireless access on your Cylerity computer, you will be required to attend a usage and security training session to be provided by the Privacy Officer or appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted, and in most cases will include several individuals at once.

Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Cylerity in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Cylerity networks. Every workstation or server that has been used by either Cylerity employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Cylerity data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a Cylerity employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Cylerity networks. Transportable media received from an external source could potentially pose a threat to Cylerity networks. ***Sensitive data*** includes all human resource data, financial data, Cylerity proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No sensitive data should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Cylerity data or sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Cylerity.
- Non-Cylerity workstations and laptops may not have the same security protection standards required by the Cylerity, and accordingly virus patterns could potentially be transferred from the non-Cylerity device to the media and then back to the Cylerity workstation.
  Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.
- Data may be exchanged between Cylerity workstations/networks and workstations used within the Cylerity. The very nature of data exchange requires that under certain situations data be exchanged in this manner.
  Examples of necessary data exchange include data provided to auditors via USB key during the course of the audit.
- Before initial use and before any sensitive data may be transferred to transportable media, the media must be sent to the Privacy Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy sensitive data only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves the Cylerity, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

Cylerity utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Cylerity laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

Disposal of External Media / Hardware

Disposal of External Media

External media (USB drives) should be disposed of in a method that ensures that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Disposition of Excess Equipment

As the older Cylerity computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

Change Management

Statement of Policy

To ensure that Cylerity is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain electronic protected health information ("ePHI"). Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated Cylerity employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

Audit Controls

Statement of Policy

To ensure that Cylerity implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information ("ePHI"). Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

The Cylerity is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Cylerity will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure

1. See policy entitled Information System Activity Review for the administrative safeguards for auditing system activities.
2. The Information Technology Services shall enable event auditing on all computers that process, transmit, and/or store ePHI for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of patient data being accessed for each attempted access. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.

The Cylerity shall utilize appropriate network-based and host-based intrusion detection systems. The Information Technology Services shall be responsible for installing, maintaining, and updating such systems.

Information System Activity Review

Statement of Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Cylerity shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Procedure

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Cylerity's information systems that contain or use ePHI.
2. The Information Technology Services shall be responsible for conducting reviews of Cylerity's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
4. Such reviews shall be conducted annually. Audits also shall be conducted if Cylerity has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:
    a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
    b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
    c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format referred to in Section 2 of this policy and procedure.

1. The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Cylerity's administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).

Data Integrity

Statement of Policy

Cylerity shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect Cylerity's ePHI from improper alteration or destruction.

Procedure

To the fullest extent possible, Cylerity shall utilize applications with built-in intelligence that automatically checks for human errors.

Cylerity shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.

To prevent transmission errors as data passes from one computer to another, Cylerity will use encryption, as determined to be appropriate, to preserve the integrity of data.

Cylerity will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.

To prevent programming or software bugs, Cylerity will test its information systems for accuracy and functionality before it starts to use them. Cylerity will update its systems when IT vendors release fixes to address known bugs or problems.

1. Cylerity will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
2. To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

Contingency Plan

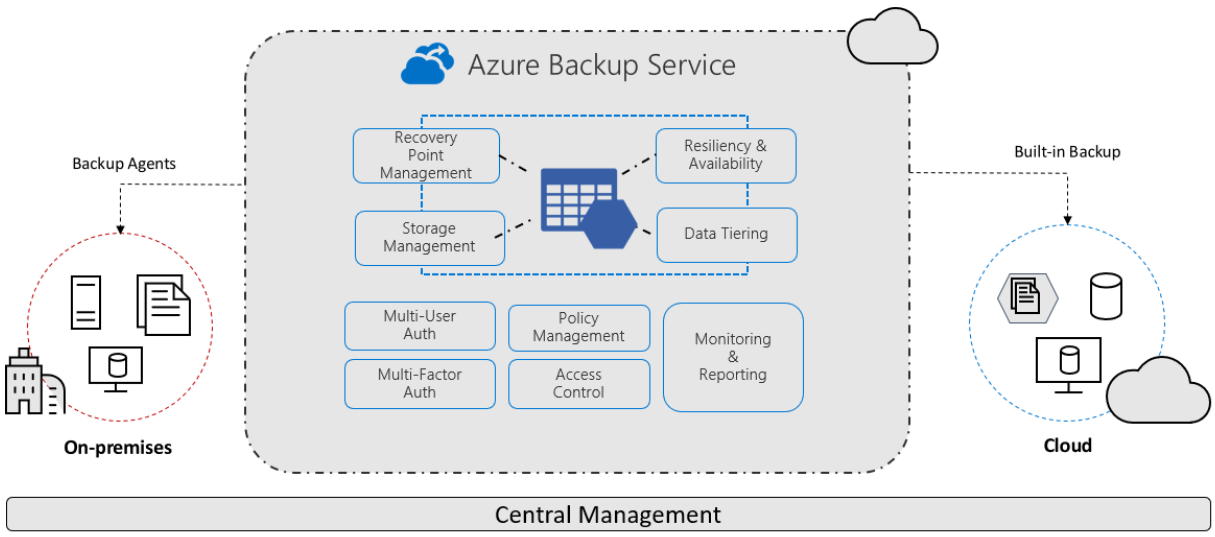
Statement of Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI.

Cylerity is committed to maintaining formal records for responding to an emergency or other occurrence that damages systems containing ePHI. Cylerity shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure

1. Data Backup Plan
    a. Cylerity, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies in Microsoft Azure.



    b. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

c. The Security Officer shall test backup procedures on an annual basis to ensure that exact copies can be retrieved and made available. Such testing shall be documented by the Security Officer. To the extent such testing indicates need for improvement in backup procedures, the Security Officer shall identify and implement such improvements in a timely manner.

2. Disaster Recovery and Emergency Mode Operations Plan
   a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:
      i. Restoring or recovering any loss and/or systems necessary to make data available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
      ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.
   b. The disaster recovery and emergency mode operation plan shall include the following:
      i. Current copies of the information systems inventory and network configuration developed and updated as part of Cylerity's risk analysis.
      ii. Current copy of the written backup procedures developed and updated pursuant to this policy.
      iii. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions.
      iv. Identification of an emergency response team. Members of such team shall be responsible for the following:
         1. Determining the impact of a disaster and/or system unavailability on Cylerity's operations.
         2. In the event of a disaster, securing the site and providing ongoing physical security.
         3. Retrieving lost data.
         4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.
         5. Taking such steps necessary to restore operations.

v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:
    1. Members of the immediate response team,
    2. Information systems vendors, and
    3. All current workforce members.

c. The disaster recovery team shall meet on at least an annual basis to:
    i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Cylerity;
    ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and
    iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

Security Awareness and Training

Statement of Policy

To establish a security awareness and training program for all members of Cylerity's workforce, including management.

All workforce members shall receive appropriate training concerning Cylerity's security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

Procedure

1. Security Training Program
    a. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of the HIPAA Security Rule including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.
    b. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats.
2. Security Reminders
    a. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse

pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

b. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

3. Protection from Malicious Software
    a. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
        i. Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
        ii. The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
        iii. Instructions to never download files from unknown or suspicious sources,
        iv. Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
        v. The importance of backing up critical data on a regular basis and storing the data in a safe place,
        vi. Damage caused by viruses and worms, and
        vii. What to do if a virus or worm is detected.
4. Password Management
    a. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:
        i. Passwords must be changed every 120 days.
        ii. A user cannot reuse the last 12 passwords.
        iii. Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters; Cylerity recommends memorable phrases up to 64 characters.
        iv. Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
        v. A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.

vi. Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.
vii. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
viii. Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
ix. Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

Security Management Process

Statement of Policy

To ensure Cylerity conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Cylerity.

Cylerity shall conduct an accurate and thorough risk analysis to serve as the basis for Cylerity's HIPAA Security Rule compliance efforts. Cylerity shall re-assess the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business Cylerity's and technological advancements.

Procedure

1. The Security Officer shall be responsible for coordinating Cylerity's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.
2. The risk analysis shall proceed in the following manner:
    a. Document Cylerity's current information systems.
        i. Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization's information system network is configured.
        ii. Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.
        iii. For each application identified, identify each licensee (i.e., authorized user) by job title and describe the manner in which authorization is granted.
        iv. For each application identified:
            1. Describe the data associated with that application.
            2. Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.

3. Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
4. Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.
5. Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.
6. For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

v. Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Cylerity. Consider the following:
    1. Natural threats, e.g., earthquakes, storm damage.
    2. Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
    3. Human threats
        a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls
        b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment
        c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail
        d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction

4. Identify and document vulnerabilities in Cylerity's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to ePHI, modification of ePHI, denial of service, or repudiation (i.e., the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

vi. Determine and document probability and criticality of identified risks.
   1. Assign probability level, i.e., likelihood of a security incident involving identified risk.
      a. "Very Likely" (3) is defined as having a probable chance of occurrence.
      b. "Likely" (2) is defined as having a significant chance of occurrence.
      c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.
   2. Assign criticality level.
      a. "High" (3) is defined as having a catastrophic impact on the medical Cylerity including a significant number of medical records which may have been lost or compromised.
      b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the Cylerity which may have been lost or compromised.
      c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.
   3. Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

vii. Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high risk

scores, as well as specific security measures and safeguards required by the Security Rule.

viii. Develop and document an implementation strategy for critical security measures and safeguards.
    1. Determine timeline for implementation.
    2. Determine costs of such measures and safeguards and secure funding.
    3. Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
    4. Make necessary adjustments based on implementation experiences.
    5. Document actual completion dates.

ix. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

3. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:
    a. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.
    b. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, Cylerity shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

Emergency Operations Procedures

Purpose

To provide procedures for managing when systems are unavailable due to planned or unexpected outages.

Procedures

Notification

The Information Systems or Technology Manager shall notify Cylerity management as soon as practicable in the event of:

- planned downtime of systems,
- unexpected outage of systems, and
- resumption of services following an outage such that normal operations may resume.

Notes should be kept for loading into Microsoft Azure instance when operational and normal operations resume.

Additional Functions

Cylerity is responsible for maintaining an adequate stock of paper forms in anticipation of system downtime.

Sanction Policy

Policy

It is the policy of the Cylerity that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Cylerity will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

The Cylerity will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Cylerity's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of HIPAA, Cylerity's security policies, Directives, and/or any other state or federal regulatory requirements.

Definitions

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Sensitive information, includes, but not limited to, the following:

- Protected Health Information (PHI) – Individually identifiable health information that is in any form or media, whether electronic, paper, or oral.
- Electronic Protected Health Information (ePHI) – PHI that is in electronic format.
- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Cylerity.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Cylerity.
- Financial/accounting records – Any records related to the accounting or financial statements of Cylerity.

- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and useable upon demand by an authorized person.

Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.

Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	Accessing information that you do not need to know to do your job. Sharing computer access codes (user name & password). Leaving computer unattended while being able to access sensitive information. Disclosing sensitive information with unauthorized persons. Copying sensitive information without authorization. Changing sensitive information without authorization. Discussing sensitive information in a public area or in an area where the public could overhear the conversation. Discussing sensitive information with an unauthorized person. Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.

Level	Description of Violation
2	Second occurrence of any Level 1 offense (does not have to be the same offense). Unauthorized use or disclosure of sensitive information. Using another person's computer access code (user name & password). Failing/refusing to comply with a remediation resolution or recommendation.
3	Third occurrence of any Level 1 offense (does not have to be the same offense). Second occurrence of any Level 2 offense (does not have to be the same offense). Obtaining sensitive information under false pretenses. Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions

In the event that a workforce member violates the Cylerity's privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Level	Recommended Disciplinary Action
1	Verbal or written reprimand Retraining on privacy/security awareness

Level	Recommended Disciplinary Action
	Retraining on Cylerity's privacy and security policies Retraining on the proper use of internal or required forms
2	Letter of Reprimand*; or suspension Retraining on privacy/security awareness Retraining on the Cylerity's privacy and security policies Retraining on the proper use of internal or required forms
3	Termination of employment or contract Civil penalties as provided under HIPAA or other applicable Federal/State/Local law Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, Cylerity shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Cylerity.

Employee Background Checks

Cylerity will conduct employment reference checks, investigative consumer reports, and background investigations on all candidates for employment prior to making a final offer of employment, and may use a third party to conduct these background checks. Cylerity will obtain written consent from applicants and employees prior to ordering reports from third-party providers, and will provide a description of applicant and employee rights and all other documentation as required by law to each applicant or candidate in accordance with FCRA and applicable state and federal statutes (Appendix G). All background checks are subject to these notice and consent requirements.

An investigative consumer report compiles information on a candidate's general reputation, personal characteristics, or mode of living. This information may be gathered online including social networking sites, through public or educational records, or through interviews with employers, friends, neighbors, associates, or anyone else who may have information about the employee or potential employee. In the pre-employment process, investigative consumer reports typically include such things as criminal records checks, education verification checks, and employment verification checks.

The type of information that will be collected by the Cylerity in background checks may include, but is not limited to, some or all of the following:

- Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to suitability for employment
- Education (including degrees awarded and GPA)
- Employment history, abilities, and reasons for termination of employment
- Professional licensing board reports
- Address history
- Credit reports
- Social security number scans
- Civil court filings
- Motor vehicle and driving records
- Professional or personal references

This information may also be sought out at other times during employment, such as during reassignment or promotional periods, and following safety infractions or other incidents.

The Cylerity will conduct background checks in compliance with the federal Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), and all other applicable local, state, and federal laws and regulations. Applicants and employees may request and receive a copy of requested "investigative consumer reports."

A reported criminal offense conviction will not necessarily disqualify a candidate from employment. The nature and seriousness of the offense, the date of the offense, the surrounding circumstances, rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached. Cylerity will follow FCRA requirements, other applicable statutes, and Cylerity procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

Cylerity reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.

Background check reports shall be maintained in separate, confidential files and retained in accordance with Cylerity's document retention procedures.

Discovery Policy: Production and Disclosure

Policy

It is the policy of this organization to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

Purpose

The purpose of this policy is to outline the steps in the production and disclosure process for e-discovery for pending litigation.

Scope

This policy addresses e-discovery production and disclosure procedures related to the Federal Rules of Civil Procedures. Health information and records include both paper and electronic data related to relevant patient medical records and enterprise sources.

Procedure

Subpoena Receipt and Response

Responsible	Action
Litigation Response Team	Upon receipt, subpoenas should be reviewed to determine that all elements are contained, the parties and the purpose are clearly identified, and the scope of information requested is clear. Validate the served subpoenas before official acceptance. The validation process includes at a minimum:
Litigation Response Team, continued	Verification of appropriate service of the subpoena and that the organization is under legal obligation to comply with it, and Verification that the seal and clerk of the court signature are present and valid Review of the venue and jurisdiction of the court for the case and verification that the court is located within legal distance/mileage requirements.

Responsible	Action
Litigation Response Team	Notify the Litigation Response Team that subpoena has been received and determine if a legal hold is in place. If not, the Litigation Response Team should determine whether a legal hold should be applied.
Litigation Response Team/Legal Services	Provide direction to HIM in the processing of the subpoena, including the specific information to produce, agreed upon file formats and forms of production, whether an objection will be filed, timeframe to produce and disclose, and whether on-site testing/sampling will be conducted by the requesting party.
Litigation Response Team/Legal Services	If an outside firm is retained, such as outside counsel or discovery/litigation consultants, perform an analysis to determine if the contracted firm will have access to PHI and will need to sign a Business Associate Agreement with this organization. Execute Business Associate Agreement as appropriate.

Search and Retrieve Process

Responsible	Action
Litigation Response Team	Identify the potential sources of information which may hold potentially relevant information, such as: Local area servers for the office Personal shares or personal folders on servers Dedicated servers for the organization Laptop and/or department computers Home computers, PDAs, SmartPhones, iPads E-mail, including archived e-mail and sent e-mail E-mail trash bin, desktop recycle bin

Responsible	Action
Litigation Response Team, continued	Text/instant message archives Removable storage media (e.g., disks, tapes, CDs, DVDs, memory sticks and thumb drives) Department/office files such as financial records Personal desk files Files of administrative personnel in department/office Files located in department/office staff home Web site archives
Data Owners	Based on direction from the litigation response team on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (patient identifiers, search terms, key words, etc.) and conduct the search process. Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.
IT	Provide assistance to Data Owners in the search and retrieval process for various systems and data sources.
Data Owners	Screen or filter the search results, eliminating inappropriate information (e.g., wrong patient, outside the timeframe, not relevant to the proceeding, etc.).
Legal Services	Review the content of the data/data sets found to determine relevancy to the proceeding and identify information that is considered privileged.

Responsible	Action
Legal Services, Data Owners	Determine the final list of relevant data/data sets, location, and search methodology.

Production of Records/Data

Responsible	Action
Data Owners, IT	Determine the format the information will be disclosed, such as: paper, ASCII, PDF, TIF, screen shot, mirror copy of data file, or review of material on-line. The format will vary depending on data, source, and agreement made in the Discovery Plan/Form 35.
Data Owners, IT	Produce the information in the agreed-upon format as outlined in the discovery plan/Form 35.
Legal Services, Data Owners, IT	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
Legal Services	Conduct final review of information before disclosing to requesting party.
Legal Services	Retain a duplicate of information disclosed to requesting party.

Charges for Copying and Disclosure

Responsible	Action
Data Owners, IT	For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using the organization's established formula and governmental formulas for reproduction charges.
Legal Services	Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.

Testing and Sampling

Responsible	Action
Legal Services	A party to the legal proceeding may request to test and sample the search and retrieve methodology. Testing and sampling should be discussed and agreed upon during the pretrial conference and part of the discovery plan, including whether an external party will test and sample the search and retrieve methodologies. The costs and charges should also be determined and negotiated.
Data Owners	Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
Litigation Response Team	Assign a monitor for the outside party during their testing protocols.

Attorney/Third Party Request to Review Electronic Data

Responsible	Action
Litigation Response Team	Determine the procedures for allowing an attorney or third party to review the electronic records and search results on-line. This includes where the review will occur, system access controls, monitoring during the review session, and the charges, if any.
Legal Services, IT, Data Owners	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
Data Owners	Verify the outside party is allowed access to the record and systems by reviewing all supporting documentation (e.g., signed consent, credentials from retained firm, etc.).
Data Owners	Prepare for access by identifying the types of information that party is allowed to access. If an authorization has been signed by a patient or legal representative, allow access to legal medical records and/or other information as outlined in the authorization. If other types of information will be reviewed, access is allowed based on the subpoena, court order, state/federal statutes, or agreed-upon discovery plan.

Responding to Interrogatories, Deposition, Court Procedures

Responsible	Action
Legal Services	Legal Services manages the process for completion of the interrogatories and will coordinate processes related to depositions and testifying in court.

Responsible	Action
IT (official system custodian)	IT may provide information for an interrogatory, be deposed, or testify in court. IT is the official custodian of the information system and may testify about the technical infrastructure, system architecture, security Cylerity's, source applications, and the good faith operations from a technical infrastructure perspective.
Data Owners	Data owners may provide information for an interrogatory, be deposed, or testify in court. The data owners may testify about the specific issues related to their department/business process area.
Primary/Direct Custodian	Primary/direct custodians may provide information for an interrogatory, be deposed, or testify in court. The primary/direct custodians are those person(s) who work with the data directly or have direct involvement/knowledge of the events the litigation. For example, a staff nurse who has made an entry into the medical record and is knowledgeable about the events of a case in litigation.
Business Associates/Third Parties	Business Associates/Third Parties may provide information for an interrogatory, be deposed, or testify in court. These include contractors and others who serve a variety of functions associated with a party's information but who themselves are not parties to the litigation. Examples include Internet service providers, application service providers such as a claims clearinghouse, and other providers who provide services ranging from off-site data storage to complete outsourcing of the IT Department.

e-Discovery Policy: Retention

Policy

It is the policy of this organization to maintain and retain enterprise health information and records in compliance with applicable governmental and regulatory requirements. This organization will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements.

Purpose

The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic health information and records will be stored, retained, and destroyed after they are no longer active for patient care or business purposes; and to ensure appropriate availability of inactive records.

Scope

This policy applies to all enterprise health information and records whether the information is paper based or electronic. It applies to any health record, regardless of whether it is maintained by the Health Information Management Department or by the clinical or ancillary department that created it.

Definitions

- Data Owners: Each department or unit that maintains patient health records, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in his or her area are preserved, maintained, and retained in compliance with records management policies and retention schedules established by the Health Information Management Department *[or other designated authority]*.
- Property Rights: All enterprise health information and records generated and received are the property of the organization. No employee, by virtue of his or her position, has any personal or property right to such records even though he or she may have developed or compiled them.

- **Workforce Responsibility:** All employees and agents are responsible for ensuring that enterprise health information and records are created, used, maintained, preserved, and destroyed in accordance with this policy.
- **Destruction of Enterprise Health Information and Records:** At the end of the designated retention period for each type of health information and record, it will be destroyed in accordance with the procedures in this policy unless a legal hold/preservation order exists or is anticipated.
- **Unauthorized Destruction**: The unauthorized destruction, removal, alteration, or use of health information and records is prohibited. Persons who destroy, remove, alter or use health information and records in an unauthorized manner will be disciplined in accordance with the organization's Sanction Policy.

Procedure

Responsible	Action
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the Records Committee and Litigation Response Team.
IT/Data Owners	IT/Data Owners will ensure that electronic storage of enterprise health information and records is carried out in conjunction with archiving and retention policies.
Legal Services	Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters. It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.

Guidelines for Retention of Records/Information and Schedules:

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.

E-mail Communication Retention	Depending on content, e-mail messages between clinicians and between patients and clinicians and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format. The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content. Users should be aware of *Messaging Policies* that establish disposal schedules for e-mail and manage their e-mail accordingly.

Development of Records Retention Schedules	Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. *[Note: minimum retention schedules are attached to this policy]*. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database. Changes to Retention Schedule: Proposed changes to the record retention schedules will be submitted to the Records Committee for initial review. The Records Committee, in consultation with the Legal Services Department, will research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records will be maintained and provide an identifying code. The proposed revisions will be submitted to the Records Committee for review and approval. The approved changes will be published and communicated to the designated Records Coordinators. Retention of Related Computer Programs: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, then data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion. Data Owners should work closely with IT personnel in order to comply with this section. Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT department. Retention of Records on Individual Workstations: Primary responsibility for retention of data created at the desktop level—

	typically with e-mail, Microsoft "Office" applications such as Word, Excel, PowerPoint, Access, or other specialized but locally run and saved computer applications—shall be with the user/author. The user/author will ensure that the documents are properly named and saved to be recognizable by the user in the future, and physically saved to a "shared drive." By saving a copy in this manner, IT will create an archive version of the saved document for a specified number of years after the user deletes the copy from the shared drive. Records with retention periods in excess of this period will require an alternative means of retention. Users are responsible for the security of any confidential information and/or protected health information created or maintained on their workstations.

Storage and Destruction Guidelines

Active/Inactive Records	Records are to be reviewed periodically by the Data Owner to determine if they are in the active, inactive, or destruction stage. Records that are no longer active will be stored in the designated off-site storage facility. Active stage is that period when reference is frequent and immediate access is important. Records should be retained in the office or close to the users. Data Owners, through their Records Coordinator, are responsible for maintaining the records in an orderly, secure, and auditable manner throughout this phase of the record life-cycle.

Active/Inactive Records, continued	Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be cataloged and moved to the designated off-site storage facility. Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.
Storage of Inactive Records	All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.

Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site storage facility manager. Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal health information or other forms of confidential corporate, employee, member, or patient information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed.

Records Destruction, continued	Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods. CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.

Breach Notification Procedures

Purpose

To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and/or state breach notification purposes.

Scope

This applies to all employees, volunteers, and other individuals working under contractual agreements with the Cylerity.

Definitions

- State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality, or integrity of the Personal Information.
- Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.
- HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.
- Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.
- Individually Identifiable Health Information (IIHI) – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

- Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Number, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.
- Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.
- Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

Procedure

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the Cylerity will immediately inform their supervisor/manager, and the Privacy Officer.
2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may contact the Privacy Officer directly at
   kenneth.penkowski@cylerity.com
   (888) 803-3886 x 888
    a. Provide the Privacy Officer with as much detail as possible.
    b. Be responsive to requests for additional information from the Privacy Officer.
    c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
4. The Privacy Officer, in conjunction with the Cylerity's Legal Counsel, will decide whether or not to notify the CEO as appropriate by taking into consideration the seriousness and scope of the breach.

Containing the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.

a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
    i. Stopping the unauthorized Cylerity
    ii. Recovering the records, if possible
    iii. Shutting down the system that was breached
    iv. Mitigating the breach, if possible
    v. Correcting weaknesses in security Cylerity's
    vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with the Cylerity's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
        i. The Privacy Breach Assessment tool will help aid the investigation.
    b. The Privacy Officer, in collaboration with the Cylerity's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations
        ii. Legal obligations – the Cylerity's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
        vi. Number of individuals affected

Notification

1. The Privacy Officer will work with the department(s) involved, the Cylerity's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information
        ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Cylerity's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, the Cylerity will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the Cylerity if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the Cylerity in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Cylerity's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, the Cylerity will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Cylerity's Sanction Policy.