



INFORMATION SECURITY POLICY

Last Revision Date

January 25, 2017

Document Owner

M. Wade Wingle – Security Officer

Legal Notice:

All templates are provided to you to serve as examples for creating your own documentation and agreements and are not to be construed as legal advice. All templates that you adapt for your organization should be carefully reviewed and modified as necessary to ensure that they accurately reflect your practices. Policy and form approval should follow your standard operating procedures including, as applicable, consultation with your legal counsel.

Disclaimer of Liability:

The information contained herein is for informational purposes only and is provided on an “as is” basis. Purdue Healthcare Advisors, and their employees make no representation concerning the suitability or accuracy of this information for any purpose. Neither Purdue Healthcare Advisors nor any of their employees makes any warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights and shall not be liable for any damages whatsoever arising from the use of or reliance on any information contained herein.

Table of Contents

Introduction.....	1
Purpose	1
Scope	1
Acronyms / Definitions	2
Applicable Statutes / Regulations.....	3
Privacy Officer.....	3
Security Officer.....	3
Confidentiality / Security Team (CST).....	3
Employee Responsibilities	5
Employee Requirements	5
Prohibited Activities	5
Electronic Communication, E-mail, Internet Usage ¹²	6
Internet Access	8
Reporting Software Malfunctions.....	8
Report Security Incidents.....	8
Transfer of Sensitive/Confidential Information	8
Transferring Software and Files between Home and Work	9
Internet Considerations.....	9
Installation of authentication and encryption certificates on the e-mail system	10
Use of WinZip encrypted and zipped e-mail	10
De-identification / Re-identification of Personal Health Information (PHI).....	10
Identification and Authentication.....	11
User Logon IDs	11
Passwords.....	11
Confidentiality Agreement.....	12
Access Control	12
User Login Entitlement Reviews	12
Termination of User Logon Account	13
Network Connectivity	14
Dial-In Connections	15
Dial Out Connections.....	15
Telecommunication Equipment.....	15
Permanent Connections.....	14
Emphasis on Security in Third Party Contracts	14
Firewalls	15
Malicious Code:	16
Antivirus Software Installation	16
New Software Distribution	16
Retention of Ownership.....	17
Encryption.....	18
DEFINITIONS	18
OVER VIEW	18
PURPOSE	18
SCOPE	18
POLICY	18
EXCEPTIONS	19
Building Security	20
Telecommuting.....	22
General Requirements	22
Required Equipment	22
Hardware Security Protections.....	23

Data Security Protection	23
Disposal of Paper and/or External Media	24
Removable Media	25
Definitions	25
Removable Media Usage Standards and Policy	25
Mobile Devices	27
Definitions	27
Mobile Device Usage Standards and Policy	27
Mobile Phones	29
Definitions	29
Mobile Phone Usage Standards and Policy	29
Retention / Destruction of Medical Information	31
Disposal and Reuse of Electronic Media	32
Overview	32
Purpose	32
Scope	32
Policy	32
Disposal	33
Reuse	33
Change Management	34
Statement of Policy	34
Procedure	34
Audit Controls	35
Statement of Policy	35
Procedure	35
Information System Activity Review	36
Statement of Policy	36
Procedure	36
Data Integrity	38
Statement of Policy	38
Procedure	38
Contingency Plan	39
Statement of Policy	39
Procedure	39
Security Awareness and Training	42
Statement of Policy	42
Procedure	42
Security Management Process	45
Statement of Policy	45
Procedure	45
Emergency Operations Procedures	49
Purpose	49
Definitions	49
Procedures	49
Notification:	49
Scheduling:	49
Patient Encounters:	50
System Restoration:	50
Additional Functions:	50
Emergency Access “Break the Glass”	51
Policy Summary	51
Purpose	51
Definitions	51
Policy	52
Scope/Applicability	52
HIPAA Security	52

Scenario.....	52
Policy Authority/Enforcement	52
Procedures.....	52
Note:	53
Enforcement.....	53
Sanction Policy.....	54
Policy	54
Purpose	54
Definitions	54
Violations.....	55
Recommended Disciplinary Actions.....	55
Exceptions.....	56
References.....	56
Related Policies	56
Acknowledgment.....	56
Employee Background Checks.....	57
e-Discovery Policy: Production and Disclosure	58
Policy	58
Purpose	58
Scope	58
Procedure	58
Accurate Patient Identification.....	58
Subpoena Receipt and Response	58
Search and Retrieve Process	59
Production of Records/Data.....	60
Charges for Copying and Disclosure	60
Testing and Sampling	60
Attorney/Third Party Request to Review Electronic Data	61
Responding to Interrogatories, Deposition, Court Procedures	61
APPROVALS:	62
e-Discovery Policy: Retention.....	63
Policy	63
Purpose	63
Scope	63
Definitions	63
Procedure	64
Guidelines for Retention of Records/Information and Schedules:	65
Storage and Destruction Guidelines	67
APPROVALS:	68
Breach Notification Procedures.....	69
Purpose	69
Scope	69
Definitions	69
Procedure	70
Containing the Breach	70
Notification.....	71
Prevention	72
Compliance and Enforcement	72
Attachments.....	76
Related Policies	72
Appendix A – Confidentiality Form	73
Appendix B: Bring Your Own Device Agreement	74

Updates to Document

Date	User	Section	Content	Version
12/29/2010	CoP	All	Document Creation	v1.0
2/5/2011	CoP	All	Reference Threat/Vulnerability Statements (TVSxxx) to Security Risk Assessment Spreadsheet	v1.1
6/23/2011	CoP	All	Several sections added to include many new tools presented by a member of the CoP Toolkit Workgroup.	v2.2
6/25/12	CoP	All	Added Security Officer to Introduction, revised Confidentiality Agreement and disclaimer along with minor typo and format changes.	V2.4
1/18/2013	CoP	Encryption; Removable Media; Media Re-use; Mobile Devices; Mobile Phones; BYOD agreement	Revised policies for Encryption, Removable Media and Media Re-use. Added Mobile Devices, Mobile Phones and BYOD agreement	V2.5
December 15, 2016	MWW	Update and adopt for Easterseals Crossroads purposes	Complete review and update	V3.0

Easterseals Crossroads	
Policy and Procedure	
Title: INTRODUCTION	P&P #: 810.01
Approval Date: January 25, 2017	Review: Annual
Effective Date: January 25, 2017	Information Technology (TVS001)

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 Easterseals Crossroads⁶, hereinafter, referred to as the Agency. 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 Agency with policies and guidelines concerning the acceptable use of Agency 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 Agency employees or temporary workers at all locations and by contractors working with the Agency as subcontractors.

Scope

This policy document defines common security requirements for all Agency 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 the Agency, entities in the private sector, in cases where Agency has a legal, contractual or fiduciary duty to protect said resources while in Agency custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Agency network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Agency in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Agency domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Agency 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 practices of the company.

CIO – The Chief Information Officer (duties performed by Security Officer)

CMO – The Chief Medical Officer.

CO – The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues. (duties performed by Privacy Officer)

CPO – The Chief Privacy Officer is responsible for HIPAA privacy compliance issues. (duties performed by Privacy Officer)

CST – Confidentiality and Security Team

DoD – Department of Defense

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 – i.e., CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

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 defining the working relationship between the parties, which includes 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 Agency 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.

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

Privacy Officer

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

Scott Fogo
sfogo@eastersealscrossroads.org
4740 Kingsway Drive
Indianapolis, IN 46205
317-466-2013

Security Officer

The Agency has established a Security Officer as required by the HIPAA Security Rule. This Security Officer will oversee all ongoing activities related to the development, implementation, maintenance, and oversight of the policies and procedures and training program required for HIPAA Security Rule compliance and other federal and state laws as may be applicable. The current Security Officer for the Agency is:

Wade Wingler
wwingler@eastersealscrossroads.org
4740 Kingsway Drive
Indianapolis, IN 46205
317-466-2013

Confidentiality / Security Team (CST)

The Agency has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Agency 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 Agency most responsible for the overall security policy planning of the organization - the CEO, Privacy Officer, Security Officer. The current members of the CST are:

CEO – Patrick Sandy
Privacy Officer – Scott Fogo
Security Officer – Wade Wingler

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 Agency and act as the first line of defense in enhancing the security posture of the Agency.

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 Agency. This log will also be reviewed during the quarterly meetings.

Easterseals Crossroads	
Policy and Procedure	
Title: EMPLOYEE RESPONSIBILITIES	P&P #: 810.02
Approval Date: January 25, 2017	Review: Annual
Effective Date: January 25, 2017	Information Technology (TVS002, TVS003)

Employee Responsibilities

Employee Requirements

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

Wear Identifying Badge so that it may be easily viewed by others -

In order to help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in Agency facilities are provided with different colored identification badges¹⁰. Other people who may be within Agency facilities should be wearing visitor badges and should be chaperoned.

Challenge Unrecognized Personnel - It is the responsibility of all Agency personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Agency office location, you should challenge them as to their right to be there. All visitors to Agency offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the Agency. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

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. Agency policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15)¹¹ minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Agency Corporate Assets - Only computer hardware and software owned by and installed by the Agency is permitted to be connected to or installed on Agency equipment. Only software that has been approved for corporate use by the Agency may be installed on Agency equipment. Personal computers supplied by the Agency 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 Agency for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Agency are the property of the Agency unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Agency 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 Agency 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 Agency 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 Agency computers must be approved by the Agency.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Agency 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 the Agency is strictly prohibited.
- Solicitation. Use of agency systems to solicit others for selling, fundraising (other than for Easterseals Crossroads) or other kinds of solicitation is prohibited.

Electronic Communication, E-mail, Internet Usage¹²

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

Agency 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 Agency 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 Agency information resources for personal or commercial profit is strictly prohibited.
- d) Political Activities – All political activities are strictly prohibited on Agency premises. The Agency encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Agency assets or resources.
- e) Harassment – The Agency strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Agency 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 Agency to monitor the content of any electronic communication, the Agency is responsible for servicing and protecting the Agency’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 Agency 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 Agency 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.

Reporting Software Malfunctions

Users should inform the appropriate Agency 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, the Agency 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 Agency IT department 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 IT manager and Security Officer 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 Agency 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 Agency 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 Agency 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 Agency 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 the Agency and hold all data in the strictest confidence. Any purposeful release of data to which an employee

may have access is a violation of Agency 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 Agency computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Agency purchased software on home or on non-Agency computers or equipment.

Agency 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 the Agency without written consent of the respective supervisor or department head. It is crucial to the Agency 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 Agency data to a non-Agency 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.

The Agency Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the Agency does not control non-Agency personal computers, the Agency cannot be sure of the methods that may or may not be in place to protect Agency sensitive information, hence the need for this restriction.

Internet Considerations

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

The following security and administration issues shall govern Internet usage.

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

- An Internet, or other external network connection, is established;
- Agency 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 Agency. The network can be used to market services related to the Agency, 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 Agency 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.

Use of encrypted e-mail

The Agency email encryption system allows Agency personnel to exchange e-mail with remote users who have PDF reading software on their system. Please see the email encryption tutorial on the Agency intranet site for further details.

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.

Easterseals Crossroads	
Policy and Procedure	
Title: IDENTIFICATION and AUTHENTICATION	P&P #: 810.03
Approval Date: January 25, 2017	Review: Annual
Effective Date: January 25, 2017	Information Technology (TVS008, TVS015, TVS016, TVS023)

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 yearly¹³ and all inactive logon IDs are revoked. The Agency 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 five (5)¹⁴ unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Agency systems or networks must have worked with their supervisor to complete a new employee access form.

Passwords

User Account Passwords

User IDs and passwords are required in order to gain access to all Agency 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 characters¹⁵.

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 90 days¹⁶. Compromised passwords shall be changed immediately.

Reuse - The previous twelve¹⁷ passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper or stored within an unencrypted 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 Agency information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix A). 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 Agency 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 Agency 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 New Employee Form by the user's supervisor.

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, network, or EHR **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 Agency, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by way of a support ticket with 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 in

the ticket 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 completing the User Termination Form on the agency intranet. 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 supervisor shall be responsible for insuring that all keys, ID badges, and other access devices as well as Agency equipment and property is returned to the Agency prior to the employee leaving the Agency 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, including access to the clinical electronic medical record system ("EMR") and Active Directory, 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 Agency, the department head will immediately notify the IT Department of the employee's termination status and submit the updated User Termination Form (on Agency intranet).

Easterseals Crossroads		Policy and Procedure	
Title: NETWORK CONNECTIVITY		P&P #: 810.04	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology	

Network Connectivity

Permanent Connections

The security of Agency systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required the value of the information, the security measures employed by the third party, and the implications for the security of Agency systems. The Security Officer or appropriate personnel should be involved in the process, design and approval.

Emphasis on Security in Third Party Contracts

Access to Agency computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Agency Information Security Policy have been reviewed and considered.
- Policies and standards established in the Agency information security program are enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Agency computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreed upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.

- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Processes should be in place to ensure that security measures are followed by all parties to the agreement.
- Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Firewalls

Authority from the Security Officer or appropriate personnel must be received before any employee or contractor is granted access to a Agency router or firewall.

Easterseals Crossroads		Policy and Procedure	
Title: MALICIOUS CODE		P&P #: 810.05	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS018)	

Malicious Code:

Antivirus Software Installation

Antivirus software is installed on all Agency personal computers and servers. Virus update patterns are updated daily on the Agency servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration - The antivirus software currently implemented by the Agency is Vipre. Updates are received directly from Vipre which is scheduled daily.

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 – A record of virus patterns for all workstations and servers on the Agency network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Security Officer or appropriate personnel.

New Software Distribution

Only software created by Agency application staff, if applicable, or software approved by the Security Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained on the company network. 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 Security 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 Agency computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Agency 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 Agency computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Agency 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 Agency 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 Agency are the property of the Agency unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Agency ownership at the time of employment. Nothing contained herein applies to software purchased by Agency employees at their own expense.

Easterseals Crossroads		Policy and Procedure	
Title: ENCRYPTION		P&P #: 810.06	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS012, TVS015)	

Encryption

DEFINITIONS

- **Encryption:** 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.
- **Confidential Data:** Confidential information that may include, but is not limited to:
 - o any individuals' Protected Health Information ("PHI");
 - o financial and operational information of Easterseals Crossroads; and
 - o information regarding personnel of Easterseals Crossroads that is confidential in nature (e.g., compensation, benefits, and disciplinary records).

OVERVIEW

Protected Health Information ("PHI") and other confidential information is used, stored, received and transmitted on a number of electronic devices. It is the policy of this organization to use encryption solutions in order to maintain this data as securely as possible.

PURPOSE

To secure confidential information in the possession of this organization as required under applicable requirements and regulations, such as by PCI Data Security Standard Requirements 3 and 8.4, the HIPAA Security Rule § 164.312(a)(2)(iv) and § 164.312(e)(2)(ii) as well as any other applicable federal and state laws. Encrypted data cannot be viewed or otherwise discovered in the event of theft, loss or interception of data, thus protecting the confidential data from unauthorized access.

SCOPE

This policy covers all confidential data created, maintained, stored, received or transmitted on any electronic device of this organization.

POLICY

All electronic devices that store, receive and/or transmit confidential data must use Easterseals Crossroads approved encryption methods to secure the information stored, received or transmitted from that device.

Equipment Encryption (data at rest): Full disk and/or boot disk encryption must be used for laptops and workstations that contain confidential data. Boot disk encryption will not allow access to the operating system thus rendering the device inoperable to an unauthorized user. Full disk encryption encrypts all data on the device offering yet another layer of protection.

Confidential data stored servers must be saved using full disk encryption, an application (such as a database) that uses an approved encryption scheme, in an encrypted virtual drive or encrypted folder.

Transmitted Data (data in motion): If, following a comprehensive risk analysis, it is determined that encryption is a reasonable and appropriate security control for electronically transmitting confidential data, such confidential data and files must be encrypted using a Agency approved encryption solution. When encrypted data is transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Agency shall establish the criteria in conjunction with the Security Officer or other appropriate personnel. Prior to transmitting any confidential data, the Security Officer must be contacted to ensure that the proper encryption technology is in place. Processes by which confidential data transmissions can be encrypted include the following methods:

- Encrypting files and folders using a variety of commercially available encryption products. Users sending and receiving these files would need to share private keys that are used to both encrypt and decrypt each transmission. These “keys” must be shared in a distinctly different communication from the encrypted data; preferably via phone.
- The transport layer can be encrypted, as implemented by the server (web browsing and file transfer are typically encrypted with SSL, TLS or secure FTP; network access typically with a VPN). All data sent over such connections would be encrypted.
- E-mail Encryption: Users desiring to exchange secure e-mail with an outside party may exchange public keys with the outside party. Once verified, a digital certificate can be installed on each end of the communication that will allow the transmission of secure e-mail.
- **External Device Encryption (data at rest):** Confidential data stored on portable devices such as USB drives, DVDs, CDs, external hard drives, and smart phones must be encrypted. Data on these devices will be considered secure as long as the encryption key is kept separate from the device.

EXCEPTIONS

- Point of care devices that record PHI in the process of use and that cannot use encryption because of technology limitations may be exempted from this policy. These devices must be covered under a risk assessment to ensure that risks are addressed via appropriate compensating controls to protect data.
- Additional information is available at:
- HIPAA Security Rule
- <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>
- NIST Guide to Storage Encryption
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf>

Easterseals Crossroads		Policy and Procedure	
Title: BUILDING SECURITY		P&P #: 810.07	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS009, TVS010)	

Building Security

It is the policy of the Agency to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Agency strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the Agency. All other facilities, if applicable, have similar security appropriate for that location.

Easterseals Crossroads Willowbrook is a five-story stone building located at 4740 Kingsway Drive in Indianapolis and has a backup generator for elevator use only.

Easterseals Crossroads South is a single story building located at 3215 E Thompson Rd in Indianapolis and has no backup generator.

Crossroads Industrial Services is a single story factory located at 8302 East 33rd Street in Indianapolis and has no backup generator.

- Entrance to the buildings during non-working hours is controlled by a security code system²¹. Attempted entrance without this code results in immediate notification to the police department.
- Only specific Agency employees are given the security code for entrance. Disclosure of the security code to non-employees is strictly prohibited.
- The security code is changed on a periodic basis and eligible employees are notified by company e-mail or voice mail. Security codes are changed upon termination of employees that had access.
- The Willowbrook and South reception areas are staffed at all times during business hours.
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge (excluding patients), and be accompanied by an Agency staff member. In some situations, non-Agency personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times

Information Security Policy

- The first floor of the Willowbrook building has motion detection sensors that are activated after hours. Any movement within the building will result in immediate notification to the police department²⁴.
- The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24 hour a day 365 day per year basis²⁶.
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

Easterseals Crossroads <div style="text-align: right;">Policy and Procedure</div>	
Title: TELECOMMUTING	P&P #: 810.08
Approval Date: January 25, 2017	Review: Annual
Effective Date: January 25, 2017	Information Technology

Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Agency considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Agency office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Agency network and/or hosted EHR, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Agency's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

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 90 days²⁷, 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 Agency 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:

Agency Provided:

- Agency supplied workstation²⁸.
- If printing, an Agency supplied printer.
- If approved by your supervisor, an Agency supplied phone.
- If use of a personal computer is approved by a supervisor, all

Agency-related business must be conducted solely within the secure Remote Desktop environment and no data shall be saved outside of that secure environment on an employee or contractor's computer, flash drive or other storage device.

Employee Provided:

Broadband connection and fees.
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 Agency 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.

Firewall Use: Established procedures must be rigidly followed when accessing Agency information of any type. The Agency requires the use of a firewall device. Disabling a virus scanner or firewall is reason for termination.

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 15²⁹ minutes of inactivity.

Data Security Protection

Data Backup: Backup procedures have been established that encrypt the data being moved to an external media. 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 appropriate Agency personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to the Agency: Transferring of data to the Agency requires the use of an approved secure 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 Agency.

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 Security Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Agency Networks: Extreme care must be taken when connecting Agency equipment to a home or hotel network. Although the Agency actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Agency has no ability to monitor or control the security procedures on non-Agency 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 Security 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 Agency: All external transfer of data must be associated with an official contract, non-disclosure agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside the Agency without the written approval of your supervisor.

Disposal of Paper and/or External Media

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-Agency 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 confidential, sensitive, or protected information in the trash.
- Return all external media to your supervisor.
- External media must be wiped clean of all data. The Security Officer or appropriate personnel have specific 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.

Easterseals Crossroads		Policy and Procedure	
Title: Removable Media		P&P #: 810.09	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS020)	

Removable Media

Definitions

Removable Media – Any portable electronic device or media used primarily to store information electronically. Examples of portable media may include, but are not limited to: CDs, DVDs, tapes, USB storage devices (thumb drives, removable hard drives, etc.), other removable storage/memory devices (Compact Flash cards, Secure Digital and MicroSD cards, Memory Sticks, etc).

Confidential Information – Any individual's Protected Health Information (PHI) as defined by HIPAA; financial, operating or other proprietary of the Agency; and other information of the Agency that is confidential in nature (i.e., employee compensation, benefit and disciplinary records).

Removable Media Usage Standards and Policy

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

The use of removable media in various formats is common within the Agency. All users must be aware that confidential information could potentially be lost or compromised when moved outside of the Agency environment. Removable media received from an external source could potentially pose a threat to the Agency environment.

USB devices are convenient 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 other removable media formats, such as diskettes, CDs, or DVDs. The software drivers necessary to use a USB device are normally included on the USB device itself and install automatically when connected to computer equipment. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and carry, but unfortunately also easy to be lost or stolen.

Rules governing the use of removable media within the Agency include:

- Confidential information is never to be stored on removable media unless the data is maintained in an approved encrypted format.
- All USB devices used to store Agency data or confidential information must use an encrypted USB device issued by the Security Officer or appropriate personnel.
- The use of personal USB or other removable media devices within the Agency is strictly prohibited.
- Non-Agency workstations and laptops may not have the same security protection standards required by the Agency, and accordingly malicious software could be transferred from a non-Agency device to the removable media and then back to a Agency workstation.

Example: Do not copy a work spreadsheet to your USB device and take it home to connect to your personal computer.

- Data may be exchanged between Agency workstations/networks and workstations used within the Agency. 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 device for audit purposes.

- Only removable media issued by the Agency is permitted to be connected and used with Agency computers.
- Before initial use and before any confidential information is transferred to removable media, the removable media must be sent to the Security Officer or other appropriate personnel to ensure appropriate and approved encryption is installed. Copy confidential information only to the encrypted location on the removable media. Non-confidential information may be transferred to unencrypted space on the removable media.
- All employees and contractors are required to report the loss of any removable media to your supervisor or department head immediately. It is important that the CST team is notified either directly from the employee or contractor or by the employee's or contractor's supervisor or department head immediately.
- When an employee or contractor leaves the Agency, all removable media in their possession must be returned to the Security Officer or other appropriate personnel for data sanitization conforming to HIPAA guidelines for the reuse or disposal of electronic media.

When no longer in productive use, all removable media must be wiped of data in a manner which conforms to HIPAA regulations. To ensure proper reuse and disposal procedures are followed, all removable media must be returned to the Security Officer or other appropriate personnel for data erasure when no longer in use.

Easterseals Crossroads		Policy and Procedure	
Title: Mobile Devices		P&P #: 810.10	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS012)	

Mobile Devices

Definitions

Mobile Devices – Any portable computer device capable of receiving, transmitting and/or storing confidential information. Examples of mobile devices may include, but are not limited to: laptops, tablets, personal digital assistants (PDAs), etc.

Confidential Information – Any individual's Protected Health Information (PHI) as defined by HIPAA; financial, operating or other proprietary of the Agency; and other information of the Agency that is confidential in nature (i.e., employee compensation, benefit and disciplinary records).

Mobile Device Usage Standards and Policy

This policy outlines the processes and procedures for acquiring wireless access privileges, using wireless networks, and ensuring the security of Agency mobile devices.

Agency owned mobile devices are permitted to connect to the Agency network. Personally owned devices are permitted subject to the Bring Your Own Device (BOYD) policy.

Approval Procedure – For permission to use the wireless network interface on your Agency mobile device you will be required to receive the approval of your immediate supervisor or department head and the Security Officer or other appropriate personnel of the Agency. Use the New Employee form on the company intranet to make this request. Once this form is completed and approved you will be contacted by appropriate Agency personnel to setup your mobile device and schedule training.

General Requirements – All of the Agency's standard computer equipment security requirements are in effect for mobile devices as well. These requirements include, but are not limited to:

- Authentication using a unique user id and strong password
- Prohibition of installing unauthorized software
- Prohibition of modifying mobile device configuration settings

Other Requirements – The portable nature of mobile devices requires procedures which may not be applicable for workstations or similar computer equipment. Your mobile device training will include these mobile device specific requirements. These requirements include, but are not limited to:

- Your duty to report a lost or stolen mobile device to the Agency Security Officer immediately.
- Receiving approval from your supervisor prior to working on your mobile device after hours or after the number of hours for an applicable work period has been reached.
- Receiving approval from your supervisor prior to removing an Agency mobile device from the Agency.

- If you have received approval to travel with a Agency mobile device, the device must be:
 - Powered off or locked while not in use
 - Kept in a secure location while not in use
 - Never left unattended
- Unless specifically authorized by Agency management, recording any video, still pictures or audio with a mobile device is strictly prohibited.

Software Requirements - The following is a list of the minimum software requirements for any Microsoft Windows based mobile device used within the Agency:

- Microsoft Windows 7 (with Firewall enabled)
- Easterseals Crossroads approved anti-virus/anti-malware software
- Easterseals Crossroads approved encryption solution
- Easterseals Crossroads approved secure VPN client (if applicable)
- Internet Explorer 8.0 or greater

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

Training Requirements - Once you have approval for wireless access on your Agency mobile device, you will be required to attend a mobile device usage and security training session provided by the Security Officer or other appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your mobile device 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 has been approved, and in most cases will include several individuals at once.

End of Use - When no longer in productive use, all mobile devices must be wiped of data in a manner which conforms to HIPAA regulations. To ensure proper reuse and disposal procedures are followed, all mobile devices must be returned to the Security Officer or other appropriate personnel for data erasure when no longer in use.

Employee/Contractor Termination - When an employee or contractor leaves the Agency, any mobile devices in their possession must be returned to the Security Officer or other appropriate personnel by the employee's or contractor's supervisor or department head for data sanitization conforming to HIPAA guidelines for the reuse or disposal of electronic equipment.

Easterseals Crossroads		Policy and Procedure	
Title: Mobile Phones		P&P #: 810.11	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS012)	

Mobile Phones

Definitions

Mobile Phones – Any portable phone device (smart or otherwise) that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing confidential information. Examples of mobile phones may include, but are not limited to: cell phones, smartphones, etc.

Confidential Information – Any individual's Protected Health Information (PHI) as defined by HIPAA; financial, operating or other proprietary of the Agency; and other information of the Agency that is confidential in nature (i.e., employee compensation, benefit and disciplinary records).

Mobile Phone Usage Standards and Policy

Agency owned mobile phones and personal phones subject to the BYOD agreement are permitted for conducting Agency business requiring the use of a mobile phone.

Approval Procedure – For permission to activate and use an Agency mobile phone you will be required to receive the approval of your immediate supervisor or department head and the Security Officer or other appropriate personnel of the Agency. Use the Support Ticket system to make this request. If the use of a personal mobile phone has been approved for an employee, the employee must also agree to and sign the Personal Mobile Electronic Device. Once this form is completed and approved you will be contacted by appropriate Agency personnel to setup your mobile device and schedule training.

General Requirements – All of the Agency's standard computer equipment security requirements are in effect for mobile phones as well. These requirements include, but are not limited to:

- Strong authentication using password, PIN and/or biometric security
- Prohibition of installing unauthorized software
- Prohibition of modifying configuration settings

Other Requirements – The portable nature of mobile phones requires procedures which may not be applicable for workstations or similar computer equipment. These requirements include, but are not limited to:

- Your duty to report a lost or stolen mobile phone to the Agency Security Officer immediately.
- Your mobile phone must be kept in a secure location when not in use and never left unattended.
- Unless specifically authorized by Agency management, recording any video, still pictures or audio with a mobile phone is strictly prohibited.

Software Requirements – Mobile devices must be running the most recent available version of the device's operating system. Phones may not be jailbroken or modified to bypass any security measures.

Training Requirements - Once you have approval for the use of your Agency mobile phone, you will be required to attend a mobile phones usage and security training session provided as part of the HIPAA training on the Relias system.

End of Use - When no longer in productive use, all mobile phones must be wiped of data in a manner which conforms to HIPAA regulations. To ensure proper reuse and disposal procedures are followed, all mobile phones must be returned to the Security Officer or other appropriate personnel for data erasure when no longer in use.

Employee/Contractor Termination - When an employee or contractor leaves the Agency, any mobile phones in their possession must be returned to the Security Officer or other appropriate personnel by the employee's or contractor's supervisor or department head for data sanitization conforming to HIPAA guidelines for the reuse or disposal of electronic equipment.

Easterseals Crossroads Policy and Procedure	
Title: RETENTION / DESTRUCTION of PAPER DOCUMENTS	P&P #: 810.12
Approval Date: January 25, 2017	Review: Annual
Effective Date: January 25, 2017	Information Technology (TVS020, TVS021)

Retention / Destruction of Medical Information

Many state and federal laws regulate the retention and destruction of medical information. The Agency actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 7 years³⁰.

Record Destruction - All hardcopy medical records that require destruction are shredded using NIST SP 800-88 guidelines.

Easterseals Crossroads and Logo	
Policy and Procedure	
Title: DISPOSAL AND REUSE OF ELECTRONIC MEDIA	P&P #: 810.12
Approval Date: January 25, 2017	Review: Annual
Effective Date: January 25, 2017	Information Technology (TVS021)

Disposal and Reuse of Electronic Media

Overview

A tremendous amount of information is created, stored, and transmitted using electronic media in every type of business and organization. This information includes personal data, financial data and in the case of a medical organization Protected Health Information (“PHI”). It must be assumed that any electronic media of the Agency contains PHI or other confidential information. Therefore, before reusing, retiring or disposing of computers, disks, flash drives, compact flash and similar memory card devices, external USB storage devices, backup tapes and cartridges, smart phones, point of care devices, or any other type of electronic media or device which may contain electronic media, it must be properly sanitized.

Purpose

To ensure that all data is protected from unauthorized access and to comply with the Health Insurance Portability and Accountability Act (HIPAA) and any other applicable federal and state laws that may be applicable as well as internal information security policies.

Scope

This policy covers all electronic media and all personnel who use or are responsible for equipment and systems that could contain PHI. This includes all vendors and/or contractors who have access to the equipment, electronic media and/or computer systems.

Policy

General

- 1) All media that stores PHI shall be accountable via control logs showing what it is, where it is located, what its intended use is and what individual is responsible for that media.
- 2) All media that stores PHI shall have procedures in place for proper use, storage and disposal.
- 3) PHI that is no longer needed or that is on equipment that is to be either reused or disposed of shall be removed in a manner so as to permanently, completely, and irreversibly delete said PHI so as to prevent future access or use by unauthorized individuals.
- 4) It is the responsibility of each employee to identify electronic media for which he or she is responsible for and to follow this policy to ensure the secure disposal of said media.
- 5) When no longer needed, all media must be returned to the Security Officer or other appropriate personnel for proper disposal.
- 6) The Security Officer or other appropriate personnel will store media in a secure area until such time that the media can undergo proper disposal pursuant to NIST SP 800-88 guidelines.

Methods for media purge and destruction

- 1) Overwriting via approved sanitization software that uses at a minimum three passes of systematic overwriting.

- 2) Destruction of the media. Physically destroying the media so that it cannot be used or read in any manner. Disintegration, incineration, pulverizing and/or melting are some methods of physical destruction.
- 3) Other methods as defined within NIST SP 800-88 Media Sanitization guidelines.
- 4) Clearing the data. Reformatting or deleting information is *NOT* an acceptable means of sanitizing media.

Disposal

- 1) Prior to disposal all media should be sanitized. In the event that the media will not accept sanitization the media should be physically destroyed in a manner that renders it totally useless.
- 2) Media must *NEVER* be thrown into the trash as a method of sanitization/destruction for disposal.
- 3) Following proper sanitization and/or destruction, media can be disposed of in the manner consistent with local waste disposal requirements.
- 4) Records must be maintained that identify the destruction and disposal method, date of destruction and disposal, the party responsible for destruction and disposal, and identification (e.g., serial number) of the media.

Reuse

- 1) Upon proper purging of media by the Security Officer or other appropriate personnel, media or devices containing may be reused for various purposes which may include, but are not limited to:
 - a. spare parts,
 - b. emergency equipment replacements,
 - c. use in a testing environment,
 - d. as a backup for another system, or
 - e. as an additional temporary or permanent resource for personnel requiring more than one system or device.

Additional information is available at:

[HIPAA Security Rule](#)

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>

NIST Special Publication 800-88 Guidelines for Media Sanitization

http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

US Department of Health and Human Services (HHS)

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

Easterseals Crossroads		Policy and Procedure	
Title: CHANGE MANAGEMENT		P&P #: 810.13	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS024)	

Change Management

Statement of Policy

To ensure that Agency 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 Agency employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system. (Changes are logged in the Spiceworks ticketing system in a Slack channel dedicated to that purpose.)
 - a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component or electronic health record (EHR) updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
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.

Easterseals Crossroads		Policy and Procedure	
Title: AUDIT CONTROLS		P&P #: 810.14	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS013, TVS014, TVS019)	

Audit Controls

Statement of Policy

To ensure that Agency 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 Agency is committed to routinely auditing users’ activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Agency 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.
3. The Agency 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.

Easterseals Crossroads		Policy and Procedure	
Title: INFORMATION SYSTEM ACTIVITY REVIEW		P&P #: 810.15	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS014, TVS017, TVS019)	

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. Agency 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 Agency's information systems that contain or use ePHI.
2. The Information Technology Services shall be responsible for conducting reviews of Agency'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 Agency 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 – Review 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.

- 5. 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 Agency'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).

Easterseals Crossroads		Policy and Procedure	
Title: DATA INTEGRITY		P&P #: 810.16	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS012, TVS013)	

Data Integrity

Statement of Policy

Agency 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 Agency's ePHI from improper alteration or destruction.

Procedure

1. Agency shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.
2. To prevent transmission errors as data passes from one computer to another, Agency will use encryption, as determined to be appropriate, to preserve the integrity of data.
3. Agency will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.
4. To prevent programming or software bugs, Agency will test its information systems for accuracy and functionality before it starts to use them. Agency will update its systems when IT vendors release fixes to address known bugs or problems.
5. Agency will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
6. 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.

Easterseals Crossroads		Policy and Procedure	
Title: CONTINGENCY PLAN		P&P #: 810.17	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS026)	

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.

Agency is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing ePHI. Agency 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. Practice, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.
- b. At five minute intervals, throughout the day, data systems are backed up to an internal digital backup system. Several times each day, data is backed up to an encrypted, secure, cloud-based system.
- c. The IT Manager shall monitor storage and removal of backups and ensure all applicable access controls are enforced.
- d. The IT Manager shall test backup procedures on an annual basis to ensure that exact copies of ePHI 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 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 of ePHI and/or systems necessary to make ePHI 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 operations plans shall include the following:

- i. Current copies of the information systems inventory and network configuration developed and updated as part of Agency'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 with patients.
- iv. The Agency's Executive Leadership Team (ELT) serves as the emergency response team and shall be responsible for the following:
 - 1. Determining the impact of a disaster and/or system unavailability on Agency'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 as necessary to restore operations.
- v. Procedures for responding to loss of electronic data including, but not limited to, retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of Agency's risk analysis
- vi. 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. Facilities at which backup data is stored,
 - 3. Information systems vendors, and

4. All current workforce members.
- c. The disaster recovery team shall meet on an at least an annual basis to:
 - i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Practice;
 - 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 operations plans and make appropriate changes to the plans. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer shall also be responsible for revising the plans based on the recommendations of the disaster recovery team.

Easterseals Crossroads		Policy and Procedure	
Title: SECURITY AWARENESS AND TRAINING		P&P #: 810.18	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS006)	

Security Awareness and Training

Statement of Policy

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

All workforce members shall receive appropriate training concerning Agency'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

a. Security Training Program

- i. The Security Officer, in coordination with the Human Resources Director and Privacy 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.
- ii. 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.
- iii. Security training is provided and monitored within the Relias learning system.

b. Security Reminders

- i. The Security Officer shall generate and distribute to all workforce members routine security reminders on a periodic 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, and discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, etc. The Security Officer shall be

responsible for maintaining appropriate documentation of all periodic security reminders.

- ii. 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.

c. Protection from Malicious Software

- i. 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:
 - a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
 - b) The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
 - c) Instructions to never download files from unknown or suspicious sources,
 - d) Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
 - e) The importance of backing up critical data on a regular basis and storing the data in a safe place,
 - f) Damage caused by viruses and worms, and
 - g) What to do if a virus or worm is detected.

d. Password Management

- i. 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:
 - a) Passwords must be changed every 90 days.
 - b) A user cannot reuse the last 12 passwords.
 - c) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.
 - d) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.

- e) A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.
- f) 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.
- g) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
- h) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
- i) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

Easterseals Crossroads		Policy and Procedure	
Title: SECURITY MANAGEMENT PROCESS		P&P #: 810.19	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology	

Security Management Process

Statement of Policy

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

Agency shall conduct an accurate and thorough risk analysis to serve as the basis for Agency's HIPAA Security Rule compliance efforts. Agency 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 practices and technological advancements.

Procedure

- a. The Security Officer shall be responsible for coordinating Agency's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.
- b. The risk analysis shall proceed in the following manner:
 - i. Document Agency's current information systems.
 - a) 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.
 - b) 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.
 - c) For each application identified, identify each licensee (*i.e.*, authorized user) by job title and describe the manner in which authorization is granted.
 - a) For each application identified:
 - i) Describe the data associated with that application.
 - ii) 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.

- iii) 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.
 - iv) 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.
 - v) 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.
 - vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.
- e) Identify and document threats to the confidentiality, integrity, and availability (referred to as “threat agents”) of ePHI created, received, maintained, or transmitted by Practice. Consider the following:
- i) Natural threats, e.g., earthquakes, floods, storm damage.
 - ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
 - iii) 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
 - iv) Identify and document vulnerabilities in Agency’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.

- f) Determine and document the probability and criticality of identified risks.
 - i) Assign probability level, i.e., the likelihood of a security incident involving an 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.
 - ii) Assign criticality level.
 - a. "High" (3) is defined as having a catastrophic impact on the medical Agency 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 Agency 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.
 - iii) 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.
- g) 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.
- h) Develop and document an implementation strategy for critical security measures and safeguards.
 - i) Determine timeline for implementation.
 - ii) Determine costs of such measures and safeguards and secure funding.
 - iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

- iv) Make necessary adjustments based on implementation experiences.
 - v) Document actual completion dates.
 - i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.
- C. 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:
 - i. 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.
 - ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, Agency shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvements.

Easterseals Crossroads		Policy and Procedure	
Title: Emergency Operations Procedures (EHR outage)		P&P #: 810.20	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS026)	

Emergency Operations Procedures

Purpose

To provide procedures for managing and documenting patient encounters when Electronic Health Record (EHR) and Agency Management (AM) systems are unavailable due to planned or unexpected outages.

Definitions

Electronic Health Record (EHR) – Electronic records of patient encounters in a healthcare delivery setting. An electronic health record typically consists of information including: patient demographics, progress notes, medication history, vital signs and laboratory results.

Agency Management (AM) – An Agency Management System is usually a computer-based system used to manage the day-to-day operations of a healthcare practice. Tasks typically performed by a PM system include: scheduling appointments, maintaining patient and insurance information, billing functions and generating various reports.

Procedures

Notification:

The Information Technology Manager shall notify Agency Executive Leadership as soon as practicable in the event of:

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

Scheduling:

If the EHR system is not operational or is otherwise unavailable, the schedule printed the previous day is retrieved. The database manager is tasked with maintaining a copy of this schedule or assigning this duty as appropriate.

If phones are operational, patient appointments may not be made. The operator should ask for pertinent contact information and record a message using a paper telephone encounter form.

Patient Encounters:

Paper backup data collection forms should be used to document services provided during an EHR outage. These forms are kept and maintained by the database manager and available for photocopying for use during an outage.

Paper backup data collection forms should be kept for data entry following the EHR outage.

System Restoration:

Additional Functions:

The database manager is responsible for maintaining an adequate stock of paper forms or facilitating the photocopying of forms in the event of system downtime.

All other phone/fax information will be scanned into the patient's record when the EHR system is operational and normal operations have resumed.

Easterseals Crossroads		Policy and Procedure	
Title: Emergency Access “Break the Glass”		P&P #: 810.21	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS026)	

Emergency Access “Break the Glass”

Policy Summary

The Agency has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The Agency has a formal, documented emergency access procedure enabling Agency workforce members to access the minimum EPHI necessary to effectively and efficiently treat patients in the event of a major medical emergency.

Purpose

This policy reflects Agency commitment to have emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency.

Definitions

Medical emergency means medically necessary care that is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.

Electronic protected health information (EPHI) means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

Electronic media means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

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.

Policy

1. The Agency has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The procedure includes:
 - Identifying and defining which the Agency workforce members authorized to access EPHI during an emergency.
 - Identifying and defining manual and automated methods to be used by authorized Agency workforce members to access EPHI during a medical emergency.
 - Identify and define appropriate logging and auditing that must occur when authorized Agency workforce members access EPHI during an emergency.
2. The Agency has a formal, documented emergency access procedure enabling Agency workforce members to access the minimum EPHI necessary to treat patients in the event of a medical emergency. Such access must be authorized by a member of the Executive Leadership Team (ELT).
3. Regular training and awareness on the emergency access procedure is provided to all Agency workforce members.
4. All appropriate Agency workforce members have access to a current copy of the procedure and an appropriate number of current copies of the procedure should be kept off-site.

Scope/Applicability

This policy is applicable to all divisions and workforce members that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information, as described in definitions below.

HIPAA Security

Regulatory Category: Technical Safeguards

Regulatory Type: REQUIRED Implementation Specification for Access Control Standard

Regulatory Reference: 45 CFR 164.312(a)(2)(ii)

Rule Language:

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information (EPHI) during a medical emergency."

Scenario

"Break the Glass" refers to the Agency of enabling a licensed practitioner to view a patient's medical record, or a portion thereof, under emergency circumstances, when that practitioner does not have the necessary system access privileges.

Policy Authority/Enforcement

The Agency Security Officer is responsible for monitoring and enforcement of this policy.

Procedures

Mechanism to Provide Emergency Access to EPHI

1. This process will bypass formal access procedures and is limited to medical emergencies.
2. Any Workforce Member may request ELT-approval for emergency access.
3. The request should contain:
 - a. The individual being granted the emergency access,
 - b. Job title

- c. Reason for emergency access
 - d. Date and time granted access
 - e. The name of the individual granting access.
4. The Security Officer³¹, or designated person, records information about emergency users and the emergency access rights assigned to them.
5. The system administrator and Security Officer³¹ have created 2 administrator accounts solely for the purpose of emergency access. These accounts should be obviously named, such as breakglass01 and breakglass02 to allow for easy tracking of actions. These accounts and passwords are stored <these accounts need to be located where it would be obvious if they have been used or are missing, as though they were in a fire alarm box which required the glass to be broken to pull the alarm. A location such as in a sealed envelope taped to the side of a monitor in a very conspicuous place such as the nurses' station. Or, they can be locked in an area and require two employees, such as a manager and building security to access. There are a few EHR vendors who have "break glass" access available in their software, but that is not a common ability at this time.>³¹
6. The emergency access will be tracked and documented based on capabilities of the EHR. The tracking documentation will be reviewed by the Security Officer to determine that emergency access was appropriate.
7. At the conclusion of the event that precipitated the granting of emergency access, the Security Officer ensures the break-glass accounts are disabled, and new ones created in anticipation of the next emergency.
8. Any inappropriate use of emergency access will be treated as a security incident, and may subject an employee to disciplinary action, up to and including termination.
9. Documentation concerning emergency access will be retained and maintained for at least seven years from the date of creation.

Note:

When using a specific user account that provides full access to all EPHI (an administrator account) consider the following:

- Creating an extremely complicated password (but one an employee will be able to enter while under the stress of an emergency situation).
- Securing the password.
- Periodically changing the password.

Enforcement

Please refer to *810.22 Sanction Policy* for details regarding disciplinary action against employees, contractors, or any individuals who violate this policy.

Easterseals Crossroads		Policy and Procedure	
Title: Sanction Policy Security Violations and Disciplinary Action		P&P #: 810.22	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Human Resources (TVS001)	

Sanction Policy

Policy

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

The Agency will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Agency'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, Agency'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 Agency.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Agency.
- Financial/accounting records – Any records related to the accounting practices or financial statements of the Agency.
- 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	<ul style="list-style-type: none">• 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.
2	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 Agency'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.

Violation Level	Recommended Disciplinary Action
1	<ul style="list-style-type: none"> • Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Agency's privacy and security policies • Retraining on the proper use of internal or required forms
2	<ul style="list-style-type: none"> • Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the Agency's privacy and security policies • Retraining on the proper use of internal or required forms
3	<ul style="list-style-type: none"> • 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, the Agency 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 Agency.

References

U.S. Department of Health and Human Services
Health Information Privacy. Retrieved April 24, 2009, from
<http://www.hhs.gov/ocr/privacy/index.html>

Related Policies

Information Security Policy

Acknowledgment

I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for Easterseals Crossroads.

Dated this _____ day of _____, 20_____.

Signature of Employee/Contractor

Easterseals Crossroads		Policy and Procedure	
Title: EMPLOYEE BACKGROUND CHECKS		P&P #: 810.23	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Human Resources (TVS007)	

Employee Background Checks

The Agency 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.

Refer to PRE & POST HIRE SCREENING / ORIENTATION policy 103.6 for details.

Easterseals Crossroads		Policy and Procedure
Title: e-Discovery Policy Production and Disclosure of Health Information and Records for e-Discovery		P&P #: 810.24
Approval Date: January 25, 2017		Review: Annual
Effective Date: January 25, 2017		Information Technology

e-Discovery Policy: Production and Disclosure

--THIS NEEDS INPUT FROM SCOTT--

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 health information and records related to 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

Accurate Patient Identification

Responsible	Action
HIM	For litigation involving an individual's medical records, verify the patient's identity in the master patient index, including demographic information and identifiers including the medical record number. <i>[Note: When conducting searches, it is critical to accurately identify the correct patient and relevant information.]</i>
HIM	Note multiple medical record numbers, identifiers, aliases, etc., that will be used during the search process to find relevant information.

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. <ul style="list-style-type: none"> • Validate the served subpoenas before official acceptance. The validation process includes at a minimum: • 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.
HIM	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.
HIM	If the subpoena requests “any and all records,” HIM and/or Legal Services should work with the judge and/or plaintiff’s attorney to clarify the scope and type of information being requested. <i>[Note: The e-discovery process will identify vast volumes of data which can overwhelm a case; the parties should identify information that is necessary and relevant rather than providing all information.]</i>
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: <ul style="list-style-type: none"> Legal Health Record/EHR System (including source information systems such as nursing, ED, lab, radiology, etc.) 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 E-mail, including archived e-mail and sent e-mail E-mail trash bin, desktop recycle bin 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
HIM, 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 HIM and Data Owners in the search and retrieval process for various systems and data sources.
HIM, 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.
Legal Services, HIM, Data Owners	Determine the final list of relevant data/data sets, location, and search methodology.

Production of Records/Data

Responsible	Action
HIM, 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.
HIM, Data Owners, IT	Produce the information in the agreed-upon format as outlined in the discovery plan/Form 35.
Legal Services, HIM, 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
HIM, 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.
HIM	Invoice requesting parties for allowable charges related to the reproduction of health information and records.
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.
HIM, 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, HIM	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, HIM, Data Owners	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
HIM, 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.).
HIM, 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.
HIM (official record custodian)	HIM may provide information for an interrogatory, be deposed, or testify in court. HIM is the official custodian of the record and can testify whether the records were kept in the normal course of business and the authenticity of the records. In addition, HIM also addresses the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters.
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 practices, 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.

APPROVALS:

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	
<i>[Specify Other Departments]</i> ³¹		Date:	

Easterseals Crossroads		Policy and Procedure
Title: e-Discovery Policy Retention, Storage, and Destruction of Paper and Electronic Health Information and Records		P&P #: 810.25
Approval Date: January 25, 2017		Review: Annual
Effective Date: January 25, 2017		Information Technology

e-Discovery Policy: Retention

--THIS NEEDS INPUT FROM SCOTT--

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.
Record Committee	<p><i>[Note: This may be an existing committee, such as the Medical Record Committee, that has membership representing Legal, Compliance, IS/IT, Information Security, HIM, Clinical, and others as appropriate]</i></p> <p>The record committee's role is to authorize any changes to the Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.</p>
HIM	<p>HIM will convene the Record Committee as needed <i>[or at regular intervals]</i> and maintain responsibility for the following:</p> <ul style="list-style-type: none"> • Review, maintain, publish, and distribute retention schedules and records management policies. • Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings to Record Committee. • Serve as point of contact for Records Coordinators. • Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance. • Oversee operation of designated offsite record storage center(s) for archival storage of paper health information and records or serve as contract administrator for such services. • Contract for destruction of paper and electronic records and certification thereof.
IT/HIM/Data Owners	IT/HIM/Data Owners will ensure that electronic storage of enterprise health information and records is carried out in conjunction with archiving and retention policies.
Records Coordinators	Records coordinators are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of

	<p>responsibility to accomplish the following:</p> <ul style="list-style-type: none"> • Transfer records to storage • Identify, control, and maintain records in storage • Retrieve and/or return records from/to storage • Document the destruction of records and the deletion of records from the records inventory • Monitor the records management process <p>Record coordinators will obtain (if not already trained) and maintain records management skills.</p>
Legal Services	<p>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.</p> <p>It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.</p>

Guidelines for Retention of Records/Information and Schedules:

Record Retention	<p>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.</p>
Non-record Retention	<p>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.</p> <p>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.</p> <p>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.</p>
E-mail Communication Retention	<p>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.</p> <p>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 <i>Messaging Policies</i> that establish disposal schedules for e-mail and manage their e-mail accordingly.</p>

Development of Records Retention Schedules	<p>Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. <i>[Note: minimum retention schedules are attached to this policy]</i>. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
--	---

Storage and Destruction Guidelines

Active/Inactive Records	<p>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. 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.</p>
Storage of Inactive Records	<p>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.</p>
Records Destruction	<p>General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules.</p> <p>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.</p> <p>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. The approved methods to destroy records include: <i>[Note: specify based on local, state, and federal rule; these could potentially include recycling, shredding, burning, pulping, pulverizing, and magnetizing.]</i>³¹ 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.</p> <p>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.</p>

	<p>This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction.</p> <p>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.</p> <p>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. These methods include: <i>[Note: specify based on local, state, and federal rules; these could potentially include: burning, shredding, or some other approach which renders the media unusable; degaussing, which uses electro-magnetic fields to erase data; or, preferred for magnetic media when media will not be physically destroyed, “zeroization” programs (a process of writing repeated sequences of ones and zeros over the information)]</i>³¹. CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed.</p> <p>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.</p>
--	--

APPROVALS:

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	
<i>[Specify Other Department]</i>			

Easterseals Crossroads		Policy and Procedure	
Title: Reporting and Managing a Privacy Breach Procedure		P&P #: 810.25	
Approval Date: January 25, 2017		Review: Annual	
Effective Date: January 25, 2017		Information Technology (TVS025)	

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 Agency.

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 Agency 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 a member of the Executive Leadership Team (ELT) within twenty-four (24) hours of the initial report.
3. You may call the Privacy Officer directly at 317-752-4907.
 - 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 Agency's Legal Counsel, will decide whether or not to notify the President/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 practice
 - 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 practices
 - 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 Agency'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 Agency'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 Agency'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 Agency'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 Agency'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 Agency 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 Agency 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 Agency in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Agency'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 Agency 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 Agency's Sanction Policy.

Related Policies

IT-2.0 Sanction Policy

Appendix A – Confidentiality Form

Easterseals Crossroads Confidentiality Agreement

I understand and acknowledge that as an employee of Easterseals Crossroads, I may have access to, use or disclose Confidential Information. Confidential Information may include, but is not limited to:

1. any individuals' Protected Health Information (PHI);
2. financial and operational information of Easterseals Crossroads; and
3. information regarding personnel of Easterseals Crossroads that is confidential in nature (e.g., compensation, benefits, and disciplinary records).

I hereby agree that I will protect Confidential Information at all times during and after my employment with Easterseals Crossroads and further agree to the following:

1. I understand that Confidential Information within the Agency can take many forms including: electronic data, paper records and oral conversations; and I agree to be diligent in protecting Confidential Information in whatever form it may take.
2. I will abide by Easterseals Crossroads' "Minimum Necessary" policies by only accessing, using, and disclosing the minimum amount of Confidential Information required for the performance of my assigned job duties, as allowed by Easterseals Crossroads' policies.
3. I will only share Confidential Information with those who have the legal right to receive it.
4. I will take all reasonable precautions to secure Confidential Information to which I have access including, but not limited to, shredding and encrypting Confidential Information pursuant to Easterseals Crossroads' policies.
5. I understand that I am solely responsible for all activity conducted on computer systems logged into with my username and password.
 - a. I will log off when I leave my computer(s) and mobile device(s) unattended.
 - b. I will not share my password with anyone, including my friends and co-workers.
 - c. I will not use the user names and passwords of others.
6. I understand that Easterseals Crossroads reserves the right to audit any information accessed or sent by me without my knowledge, and share information from such audits with appropriate authorities.
7. I will never use tools or techniques to break and/or exploit system security measures.
8. I will notify Easterseals Crossroads' Privacy Officer if I suspect that any Confidential Information has been misused or improperly disclosed.
9. I will notify Easterseals Crossroads Security Officer if my password, computer, or portable device is lost or stolen.
10. I will seek the guidance of the Privacy Officer if I am ever unsure about the proper use or disclosure of Confidential Information.
11. I will notify Easterseals Crossroads Security Officer if my password, computer, or portable device is lost or stolen.
12. I understand that my obligations for protecting Confidential Information extend to activities outside of the workplace and will continue after my employment with Easterseals Crossroads ceases.
13. I understand that any violation of this Confidentiality Agreement will subject me to Easterseals Crossroads' disciplinary policies and disciplinary action, up to and including termination of employment or business relationship.
14. I understand that any violation of this Confidentiality Agreement may constitute a violation of federal, state and/or local statutes that may result in civil and/or criminal prosecution.

Signature

Date

Name (Printed)

Appendix B: Bring Your Own Device Agreement

Easterseals Crossroads Personal Mobile Electronic Device Agreement

I understand and acknowledge that as an employee of Easterseals Crossroads, I may have access to, use or disclose Confidential Information made available to me on electronic devices. Such Confidential Information may include, but is not limited to:

1. any individuals' Protected Health Information (PHI);
2. financial and operational information of Easterseals Crossroads; and
3. information regarding personnel of Easterseals Crossroads that is confidential in nature (e.g., compensation, benefits, and disciplinary records).

Whereas, I wish to have access to or use Confidential Information on my personal mobile electronic device to conduct the business of Easterseals Crossroads,

I hereby agree that my personal mobile electronic device ('mobile device') will be subject to restrictions and conditions to protect Confidential Information and further agree to the following:

1. The use of my mobile device is not permitted without prior approval and inspection by the Agency's Security Officer or other appropriate personnel.
2. Approval for the use of my mobile device will not be considered until I have successfully completed the mobile device training session.
3. That certain security standards and, possibly, applications may be required to be installed, configured and controlled by Easterseals Crossroads on my mobile device. Such standards and applications may include, but are not limited to:
 - a. Encryption for data at rest (stored) and data in motion (transmitted/received)
 - b. Device management software to remotely manage my mobile device by the Agency
 - c. Remote wipe capabilities to delete data from my mobile device
 - d. Device authentication by PIN, password, biometric or other secure method
 - e. Automatic lock screen requiring authentication to access my mobile device after a defined period of inactivity
4. That any Confidential Information or any other Agency data which may be stored on or transmitted to or from my mobile device is owned by the Agency.
5. Easterseals Crossroads reserves the right to access, view or otherwise inspect my mobile device at any time, in person or by remote means, to ensure that Confidential Information is kept secure.
6. I will notify the Agency immediately if I believe my mobile device has been lost or stolen.
7. I will notify the Agency when I decide to upgrade, change or stop using my mobile device.
8. If I am no longer using my previously approved mobile device for conducting Agency business, I will present my mobile device to the Agency and allow the Agency Security Officer or other appropriate personnel to ensure that any Confidential or other Agency information is securely deleted from my mobile device.
9. I will not share my mobile device with other people and will keep my PIN, password and/or other authentication information private and known only to myself.
10. I authorize the Agency, if it has a reasonable belief that my mobile device has been lost, stolen or in any way compromised, to remotely wipe any and all data (including my own personal data) from my mobile device.
11. That, whenever possible, my mobile device should only be used to access secure applications and computer equipment of the Agency to access Confidential Information and should not have any Confidential Information stored or downloaded to my mobile device.

12. In the event that Confidential Information must be downloaded or stored to my mobile device, the storage of such Confidential Information must be kept in an encrypted form using an encryption solution approved by the Agency.
13. If Confidential Information is stored on my mobile device, I will take steps to securely delete Confidential Information from my mobile device once it is longer required according to Agency approved secure deletion procedures.
14. Any electronic transmissions between my mobile device and any other electronic device in which Confidential Information is transmitted must be encrypted using an encryption solution approved by the Agency.
15. Although the Agency will make reasonable efforts to assist me with the secure use of my mobile device to conduct Agency business, I understand that this device is not an Agency asset and that support the Agency provides to me for the use of my mobile device may be limited or none at all.
16. I will not disable or modify any of the configuration settings applied and/or applications installed by the Agency on my mobile device.
17. I will maintain my mobile device and apply application and operating system updates to keep my mobile device current with any security fixes.
18. I will not 'jailbreak' my mobile device or otherwise bypass my mobile device manufacture's or the Agency's security measures.
19. I understand that in no event shall Easterseals Crossroads be held liable for any damages (direct, indirect, punitive, special, consequential or any other type of damages) for any of the actions and activities taken by Easterseals Crossroads in order to secure, maintain and control my mobile device. Such actions and activities may include but are not limited to the surveillance of any and all activities conducted on my mobile device, the deactivation of my mobile device and the secure and irreversible removal any and all data, including my personal data, from my mobile device.
20. I also understand that the use of my mobile device for business purposes may increase costs associated with the service plan for my mobile device and that any reimbursement for the increase in costs associated with the business use of my mobile device will not be reimbursed by Easterseals Crossroads.

Employee Signature

Date

Employee Name (Printed)