Compliance, Privacy & Security Policies and Procedures

Approved by the Board of Directors: February 10, 2016

TABLE OF CONTENTS

INTRODUCTION

There are two main categories of regulations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Privacy Regulations and the Security Regulations. The Privacy Regulations establish certain minimum standards for (a) the use and disclosure of patients' health information by health care providers and (b) access and control by individuals of their own health information. The Security Regulations provide for the integrity and security of patients' health information when that information is stored or transmitted electronically. The Privacy Regulations and the Security Regulations are found in the Code of Federal Regulations, 45 CFR Parts 160 and 164. This manual contains information to help employees understand the expectations under HIPAA and its regulations. However, the provisions in this manual are not intended to create, and do not create, contractual obligations with respect to any matters covered in the manual or with regard to any employee's employment.

1. DEFINITIONS

HIPAA created a new lexicon for health care providers. On the following pages is a glossary of terms that all employees of Easter Seals should understand. These terms are contained in many of the policies and procedures contained in this Manual.

Term	Definition
Access	**Access** refers to the ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.
Access Control	**Access Control** refers to a method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, and classification.
Authentication	**Authentication** refers to the corroboration that a person or entity is who he/she/it claims to be.
Business Associate	Business Associate means, with respect to a covered entity, a person who: **(i)** On behalf of such covered entity or of an organized health care arrangement assists in the performance of: **(A)** A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or **(B)** Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR 164.501), management, administrative, accreditation,

Term	Definition
	or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
Code Set	**Code Set** means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.
Covered Entity	**Covered Entity** means: **(1)** A health plan. **(2)** A health care clearinghouse. **(3)** A health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Regulations For the purposes of this Manual, Easter Seals is considered a Covered Entity
Designated Record Set	**Designated Record Set** means: **(1)** A group of records maintained by or for a covered entity that is: **(i)** The medical records and billing records about individuals maintained by or for a covered health care provider; **(ii)** The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or **(iii)** Used, in whole or in part, by or for the covered entity to make decisions about individuals. **(2)** For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
Disclosure	**Disclosure** means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Encryption	**Encryption** (or encipherment) refers to transforming confidential plaintext into cipher text to protect it. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over

Term	Definition
	unsecured lines. Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.
Health care	**Health care** means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: **(1)** Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and **(2)** Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health Care Operations	**Health Care Operations** means any of the following activities of the covered entity: **(1)** Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; **(2)** Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; **(3)** Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable; **(4)** Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; **(5)** Business planning and development, such as conducting cost-management and planning-related

Term	Definition
	analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and **(6)** Business management and general administrative activities of the entity, including, but not limited to: **(i)** Management activities relating to implementation of and compliance with the requirements of the HIPAA Regulations **(ii)** Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. **(iii)** Resolution of internal grievances; **(iv)** Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and **(v)** Consistent with the applicable requirements of § 164.514, creating de- identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).
Marketing	**Marketing** means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. **(1)** Marketing does not include communications that meet the requirements of paragraph (2) of this definition and that are made by a covered entity: **(i)** For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or **(ii)** That are tailored to the circumstances of a particular individual and the communications are: **(A)** Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or

Term	Definition
	(B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care. **(2)** A communication described in paragraph (1) of this definition is not included in marketing if: **(i)** The communication is made orally; or **(ii)** The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.
Password	**Password** refers to confidential authentication information composed of a string of characters.
Protected Health Information ("PHI") .	**Protected Health Information** means any information, whether oral or recorded in any form or medium, that: **(1)** Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and **(2)** Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual
Psychotherapy notes	**Psychotherapy notes** means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. It excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Term	Definition
Treatment	**Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
Transaction	**Transaction** means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: ▪ Health care claims or equivalent encounter information. ▪ Health care payment and remittance advice. ▪ Coordination of benefits. ▪ Health care claim status. ▪ Enrollment and disenrollment in a health plan. ▪ Eligibility for a health plan. ▪ Health plan premium payments. ▪ Referral certification and authorization. ▪ First report of injury. ▪ Health claims attachments. ▪ Other transactions that the Secretary of the U.S. Department of Health and Human Services may prescribe by regulation
Unsecured PHI	**Unsecured PHI** is PHI that is not secured through the use of a technology (such as encryption) that renders the PHI unusable, unreadable and undecipherable to unauthorized users.
Workforce	**Workforce** means employees, volunteers, trainees, 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

2. CUSTOMER ACCESS TO AND AMENDMENT OF HEALTH RECORDS

Background

Patients should be able to view, copy, and amend information collected and maintained about them. Until HIPAA, however, a patient's rights to access his or her own information varied greatly from state-to-state. If state law provides greater access than what HIPAA provides, then the state law is controlling.

An individual has the right to request that Easter Seals amend his or her health information. Easter Seals may require individuals to make such requests in writing and to provide a reason to support the amendment, provided that it informs individuals in advance of such requirements.

Easter Seals may deny the request for amendment if the health information that is the subject of the request:

- was not created by Easter Seals, unless the originator is no longer available to act on the request
- is not part of the individual's health record
- is accurate and complete

Easter Seals must act on an individual's request for amendment no later than sixty (60) days after receipt of the request. Provided that Easter Seals gives the individual a written statement of the reason for the delay, and the date by which the amendment will be processed, Easter Seals may have a one-time extension of up to thirty (30) days for an amendment request.

If the request is granted, Easter Seals must:

- insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment
- inform the individual that the amendment is accepted
- obtain the individual's identification of and agreement to have Easter Seals notify the relevant persons with whom the amendment needs to be shared
- within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified by the individual, and persons, including Business Associates, that Easter Seals knows have the PHI that is the subject of the amendment and that may have relied on or could foresee ably rely on the information to the detriment of the individual.

If Easter Seals denies the requested amendment, it must provide the individual with a timely, written denial, written in plain language, which contains:

- the basis for the denial
- the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement
- a statement that if the individual does not submit a statement of disagreement, the individual may request that Easter Seals provide the individual's request for amendment and the denial with any future disclosures of PHI
- a description of how the individual may complain to Easter Seals or the Secretary of the U.S. Department of Health and Human Services
- the name or title, and telephone number of the designated contact person who handles complaints for Easter Seals.

Easter Seals staff must permit the individual to submit to Easter Seals for inclusion in his/her record a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Easter Seals may reasonably limit the length of a statement of disagreement.

Easter Seals may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, Easter Seals must provide a copy to the individual who submitted the statement of disagreement.

Easter Seals must, as appropriate, identify the record of PHI that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, our denial of the request, the individual's statement of disagreement, if any, and our rebuttal, if any.

If the individual has submitted a statement of disagreement, Easter Seals must include the material appended or an accurate summary of such information with any subsequent disclosure of the PHI to which the disagreement relates.

If the individual has not submitted a written statement of disagreement, Easter Seals must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.

When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, Easter Seals may separately transmit the material required.

A Covered Entity that is informed by another Covered Entity of an amendment to an individual's PHI must amend the PHI in written or electronic form, as applicable.

The Easter Seals Compliance Officer and his/her designee shall be responsible for receiving and processing requests for amendments.

Policy

A. Access

Customers of Easter Seals shall be provided access to their PHI upon request except for psychotherapy notes and information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative proceedings. Customers of Easter Seals shall be provided access to psychotherapy notes if they sign a separate authorization specifically indicating their consent to release of these specialized notes. Easter Seals shall provide customers with copies of their medical records within ten (10) days of receipt of such a request. On a case-by-case basis, Easter Seals may charge customers a reasonable fee for the copying of their records.

B. Amendment

Customers who believe information in their health records maintained by Easter Seals is incomplete or incorrect may request an amendment or correction to the information as outlined below.

Procedure

A. Access

If a customer requests a copy of his or her medical record, Easter Seals staff must request that the customer put the request in writing (either a hard copy or email is acceptable). Staff should then pull the appropriate records and obtain a page count except for those exempt categories specified in Policy A above. Easter Seals may charge $0.25 per page for copies of medical records and should inform the customer of the cost before copying the records. The medical record copying fee should be collected before the customer picks up the copies or before the copies are mailed to the customer. Easter Seals will make reasonable efforts to provide customers with copies of their medical records within ten (10) days of receipt of the request. If circumstances exist (e.g., the records are particularly voluminous or are stored off-site) that require more time, the customer should be informed of the estimated time required to prepare the copies. Easter Seals staff must verify that the person requesting the record and the person picking up the copies or to who the copies are sent is, in fact, the customer or the authorized representative of the customer.

A customer also has the right to review his or her medical record (without obtaining copies). If a customer requests to review his or her medical record, Easter Seals staff must request that the

customer put the request in writing (either a hard copy or email is sufficient). Easter Seals staff should arrange a convenient time for the customer to come to the Easter Seals office to review the records. Easter Seals will make reasonable efforts to schedule a time for a customer to review his or her medical records within ten (10) days of receipt of the request. If circumstances exist (e.g., the records are particularly voluminous or are stored off-site) that require more time for Easter Seals staff to retrieve the records, the customer should be informed of the estimated time required. Easter Seals staff must verify that the person who comes to review the record is, in fact, the customer or the authorized representative of the customer. Easter Seals shall not charge the customer any fee in connection with the Customer's in person review of his or her record. To ensure that a customer does not alter records, the customer should not be permitted to bring any pens, pencils, white-out, etc. into the room in which he or she will review the records. If possible, an Easter Seals staff member should be present during such review.

B. Amendment

If the customer believes there is an error in the records, the customer may approach the Compliance Officer or the author of the entry, point out the error, and ask the Compliance Officer or the author to correct it.

The author can correct the entry or add a progress note to clarify content.

If necessary, Easter Seals staff will assist the customer in completing the health record correction/amendment form.

Upon completion of the form, Easter Seals will give a copy of the form to the customer, place a copy in the Customer's health record immediately, and route another copy to the author.

If the author chooses to add a comment to the amendment/correction form, the second copy of the form will be routed to the customer with the author's comments.

The original correction/amendment with the author's signature will replace the copy previously placed in the Customer's record.

Copies of the correction/amendment form will be furnished to those individuals or organizations the customer deems necessary and documents on the correction/amendment form.

Copies of the correction/amendment form will also be furnished to any Business Associates or others who have the information subject to the amendment and that may have relied or might rely on that information to the detriment of the customer.

Disclosures will be noted on the correction/amendment form with a short notation indicating to whom the correction/amendment form was sent, the date, and the staff member processing the disclosure.

When a correction/amendment form is used, the Easter Seals staff will make an entry at the site of the information that is being corrected or amended indicating, "See correction/amendment," and will date and sign that entry. The correction/amendment form will be attached to the incorrect or amended entry.

Whenever a copy of the corrected/amended entry is disclosed, a copy of the correction/amendment form will accompany the disclosed entry.

A Form "**Request for Correction/Amendment of Health Information**" is included in the Appendix.

3. BUSINESS ASSOCIATES

Background

Business Associates are people or entities who perform a function or activity for or on behalf of a covered entity such as Easter Seals in a manner that requires the use or disclosure of PHI. The Appendix includes a "**Business Associate Flow Chart**" which Easter Seals staff may use to determine if a vendor or contractor meets the definition of a Business Associate.

The HIPAA Privacy Regulations require all covered entities to enter into special contracts with Business Associates called "Business Associate Agreements" ("BAAs"). The BAA imposes certain privacy and security obligations upon the Business Associate and provides Easter Seals with certain rights and remedies if the Business Associate breaches the BAA.

The federal HITECH Act (passed in February 2009) imposes certain privacy and security obligations directly upon Business Associates, and the BAA must contain certain provisions whereby the Business Associate agrees to comply with those obligations.

Policy

Easter Seals shall, at least annually, take an inventory of all vendors and contractors and determine which of them qualify as Business Associates. Every Business Associate will be required to execute the Easter Seals "**Business Associate Agreement**", in the form contained in the Appendix.

Procedure

The Compliance Officer shall take an inventory of all vendors and contractors of Easter Seals and shall determine which, if any, are Business Associates. The Appendix contains a "**Business Associate Flow Chart" to** assist the Compliance Officer in making such determination. The Compliance Officer shall ensure that each Business Associate has executed the "**Business Associate Agreement**" form contained in the Appendix and shall retain all BAAs on file.

4. NOTICE OF PRIVACY PRACTICES

Background

Timely, accurate, and complete health information must be collected, maintained, and made available to members of an individual's treatment team so that members of the team can accurately provide services. Most customers understand and have no objections to this use of their information.

On the other hand, customers may not be aware of the fact that their health information may also be used:

- In a legal proceeding such as a personal injury lawsuit
- To verify services for which the individual or a third-party payer is billed
- As a tool in evaluating the adequacy and appropriateness of care for quality improvement
- As a training tool for members of the Easter Seals staff
- As a source of data for clinical research
- As a source of information for tracking disease by state and federal public health officials
- In connection with certain mandatory reporting obligations, such as suspected child abuse

Although customers trust their health care providers to maintain the privacy of their health information, they are often skeptical about the security of their information when it is computerized or disclosed to others. Increasingly, customers want to be informed about what information is collected and to have some control over how their information is used.

The HIPAA Privacy Regulations require Easter Seals entities to provide customers with a "Notice of Privacy Practices" informing the customer of the uses and disclosures that Easter Seals will make with their PHI.

Policy

Easter Seals shall provide a copy of its Notice of Privacy Practices to each customer at the time of intake and shall post the Notice in all facilities and on the Easter Seals website.

Procedure

The Easter Seals staff member handling the intake of a new customer shall provide the customer (or his/her parent or guardian as the case may be) with a copy of the Easter Seals Notice of Privacy Practices. The staff member shall obtain the Customer's signature on the Receipt of Notice of Privacy Practices, indicating that the customer received the Notice and shall file the Receipt in the Customer's file. The staff member handling the intake shall ask the customer if he or she has any questions about the Notice and shall answer all questions to the best of his/her ability. Any questions that the intake staff member is unable to answer shall be directed to the Easter Seals Compliance Officer. The "**Notice of Privacy Practices**" form is included in the Appendix.

5. DISCLOSURE OF PHI

Background

A customer has the right to direct Easter Seals to disclose his/her PHI to the customer him or herself (see Section 2 of this Manual) and to third parties designated by the customer. When a customer consents to treatment by Easter Seals, he or she consents to the use of his or her PHI by Easter Seals for payment, treatment and healthcare operations ("PTO") as described in the Easter Seals Notice of Privacy Practices (see Section 4 of this Manual). Except in certain circumstances when state or federal law either permits or requires the disclosure, PHI is not to be used or disclosed for purposes other than PTO without the customer's written authorization.

Policy

Except as necessary for PTO as provided in the Easter Seals Notice of Privacy Practices, and other than in the exceptions enumerated in Subsections D, E, and F of this policy, no PHI shall be released to any third party without a valid written authorization from the customer or his or her duly authorized representative.

Procedure

A. Requirements for Valid Authorization

To be valid, an authorization for release of PHI must meet the following criteria (45 CFR 164.508(c)):

- Be signed and dated by the customer or his/her legal representative;
- State specifically the person(s) to whom the information is to be released, and the purpose for which the information is required;
- State specifically what information is to be released, with dates of service;
- State each purpose of the requested use or disclosure: "at the request of the individual" shall suffice;
- Be addressed to Easter Seals;
- Include an expiration date, if desired by the customer; otherwise, authorization expires within ninety (90) days of receipt thereof;
- Contain a statement that authorization may be revoked at any time (together with a description of how it is to be revoked), except to the extent that disclosure is made in reliance on the authorization;
- Contain a statement that the information disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by 42 CFR 160 et seq.; and
- If the customer's legal representative signed the authorization, the authorization must contain a description of the representative's authority to act for the customer (e.g., parent, guardian).

The Appendix contains an "**Authorization for the Use or Disclosure of Protected Health Information**," which Easter Seals staff shall encourage customers to use whenever possible, although any form that meets the criteria above is acceptable.

Any such authorization received by Easter Seals shall be kept on file with the customer's medical record along with documentation of the information that has been released.

B. Who May Authorize the Release of PHI?

In the case of a minor (anyone under eighteen (18) years of age), a court appointed legal guardian must sign the authorization (unless the minor is allowed to consent to treatment under applicable law) and unless the parent is the authorized party, proof of appointment by a court of competent jurisdiction should accompany the authorization. In the case of a minor with divorced parents, the signature of either parent will suffice as a valid authorization.

C. Documentation of Disclosed PHI

Each transaction disclosing PHI shall be documented as to the nature and dates of the information released, to who released, and the date of release.

D. Court Orders

Upon receipt of a court order (a document issued by a state court with jurisdiction or a federal court sitting in the state in which the particular Easter Seals facility is created) ordering the release of PHI, Easter Seals staff should consult with legal counsel. In most instances, the court order constitutes sufficient authority for the release of the designated records, but the advice of an attorney should be sought to ensure that the Customer's privacy rights are protected.

E. Subpoenas

There are two types of subpoenas, (1) a subpoena requiring someone to appear in court or at a deposition to testify and (2) a subpoena seeking the production of documents only. Staff should seek the advice of an attorney prior to responding to any subpoena.

1. Subpoenas Requiring Witness to Appear in Court or at a Deposition to Testify

Upon receipt of a subpoena which is not accompanied by a written authorization signed by the customer or the Customer's legal representative, Easter Seals staff should consult legal counsel. Prior to providing any testimony, Easter Seals staff should be counseled by an attorney about any applicable legal privilege that would preclude his or her testifying about certain subject matters (e.g. statutes protecting from disclosure certain customer information, quality assurance activities, etc.).

2. Subpoena Requiring the Production of Documents Only

Upon receipt of a subpoena that requires the production of documents only (sometimes known by the Latin name *Subpoena Duces Tecum*), Easter Seals staff should consult legal counsel. If a Subpoena Duces Tecum is not accompanied by a proper authorization signed by the customer or the customer's legal representative or by a court order or a "letter of satisfactory assurances" required by HIPAA (45 CFR 164.512(e)), then Easter Seals should not release the information and may need to file a legal motion to "quash" the subpoena through legal counsel.

F. Additional Instances Justifying Release of PHI without Customer Authorization

There are other circumstances when disclosure of PHI is permitted without a Customer's authorization, such as:

- Release to accrediting agencies and licensing agencies as required by state and federal law; with respect to quality improvement material or other sensitive documents seek advice of legal counsel.
- Release to other health care providers who are directly involved in the medical care of the customer or involved in the financial or administrative review of the Customer's record.

- Release directly to customers upon request of the customer.
- Release to report suspected child abuse or neglect.
- Release to report suspected domestic violence.
- Release for certain public health activities specified in 45 CFR 164.512(b).
- Release to health oversight agencies for use in certain audits, civil and criminal investigations, licensure or disciplinary actions, or civil or criminal proceedings.
- Release for use in certain judicial and administrative proceedings, and for certain law enforcement purposes.
- Release to law enforcement when a crime has occurred on the premises.
- Release to coroners and medical examiners in connection with a death.

6. THE "MINIMUM NECESSARY" POLICY

Background

The HIPAA Privacy Regulations require in general that a Covered Entity limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure. In addition, Covered Entities must limit their requests for PHI held by other entities to the minimum necessary to accomplish the intended purpose of their request. Disclosures that are not for treatment purposes must exclude direct identifiers of a customer, to the extent possible. Covered Entities are also required to implement standard protocols for disclosures that occur on a routine and recurring basis to ensure that such disclosures are limited to the amount necessary to accomplish the purpose of the disclosure.

Policy

Easter Seals staff shall follow the procedures set forth below with respect to the use and disclosure of the minimum necessary amount of PHI necessary to accomplish the staff member's purpose.

Procedure

The Compliance Officer and/or his/her designee shall implement standard protocols for disclosures that occur on a routine and recurring basis. For example, the Compliance Officer with the Compliance Committee shall implement a standard protocol for appointment reminders. Appointment reminders should not refer to the Customer's diagnosis or the purpose of the appointment.

Easter Seals staff should direct all non-routine requests for PHI to the Compliance Officer or the Compliance Committee. For non-routine disclosures, the Compliance Officer with the Compliance Committee must develop criteria by which to evaluate requests for PHI and should review requests for disclosures of PHI on a case-by-case basis. The Compliance Officer may rely on the representation of a person or entity that the request is limited to the minimum necessary required for the purpose of the disclosure when the following persons or entities request PHI:

- A public official
- Another covered entity
- Another member of the Easter Seals workforce
- Entities that request PHI for research purposes

The Compliance Officer and the Compliance Committee may rely on the person's or entity's request only if reliance is reasonable under the circumstances. It is also important to remember that the type of disclosure the person or entity requests must be otherwise permitted by the Privacy Rule (i.e., payment purposes or other healthcare operations purposes).

The Minimum Necessary Policy does not apply to:

- Easter Seals' requests for PHI for treatment purposes
- Disclosures of PHI to other health care providers for treatment purposes
- Disclosures of PHI to the customer or his or her personal representative
- Uses or disclosures made pursuant to a written authorization (See Section 5 of this Manual)
- Uses or disclosures that are required by law (See Section 5 of this Manual)

- Disclosures made to the Secretary of the U.S. Department of Health and Human Services for the purposes of compliance reviews and investigations

Finally, the Compliance Officer with the Compliance Committee must:

- Identify the persons on the Easter Seals workforce who need access to PHI to carry out their duties.
- For each such person, identify the types of PHI to which the person needs access and any appropriate conditions to such access (e.g., a member of the billing staff generally does not need access to the entire medical record of a customer).

Then the Compliance Officer and/or his/her designee must limit the access of the persons identified to the types of PHI to which they should have access. Routine disclosures to members of the Easter Seals workforce do not need to be evaluated on a case-by-case basis; rather each person's job description should identify the limits of that person's access to PHI.

7. INFORMATION SECURITY

Background

The use of computers and computer networks has become an integral part of the Easter Seals service system. These technologies have brought and will continue to bring enormous advantages to our industry and will continue to enable us to innovate in the means of delivering services to customers. These technologies have also brought significant risks regarding customer confidentiality and privacy.

Policy

Easter Seals shall implement reasonable technological and physical safeguards to protect the security and integrity of all electronically maintained PHI.

Procedures

A. Reporting Security Problems

- If any customer's PHI is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Easter Seals Compliance Officer and/or member of the Compliance Committee must be notified immediately.
- If any unauthorized use of Easter Seals' Information systems has taken place, or is suspected of taking place, the Compliance Officer and/or member of the Compliance Committee must be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Compliance Officer and/or member of the Compliance Committee must be notified immediately.
- Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported to the Compliance Officer and/or member of the Compliance Committee. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.
- Easter Seals shall not probe security mechanisms at either Easter Seals or other Internet sites unless they have first obtained permission from Compliance Officer and/or member of the Compliance Committee. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

B. Responsibilities of the Compliance Officer and Compliance Committee

As defined below, Easter Seals staff members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

- Information Technology staff will establish an Internet security infrastructure consisting of hardware, software, policies and standards, and department staff will provide technical guidance on PC security to all Easter Seals' staff. The IT department will also organize a computer emergency response team (CERT) to respond to virus infestations, hacker intrusions, and similar events. The CERT Team is identified in Easter Seals' Disaster Recovery Plan.
- IT staff will monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the Internet security policy established in this document. IT staff will

also provide administrative support and technical guidance to management on matters related to Internet security.

- IT staff will periodically, and no less than semi-annually conduct a risk assessment of each production information system they are responsible for to identify risks and vulnerabilities.
- IT staff will check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
- IT staff will check that user access controls are defined on these systems in a manner consistent with the need-to-know.
- Easter Seals' information owners will see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.
- Easter Seals program directors will ensure that:

    - Employees under their supervision implement security measures as defined in this document.
    - Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
    - Employees who are authorized to use personal computers, portable computers or handheld devices are aware of and comply with the policies and procedures outlined in this manual and all Easter Seals documents that address information security.
    - Employees and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.
    - Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable

C. Responsibilities of All Easter Seals Employees

All Easter Seals Employees shall:

- Know and follow the appropriate Easter Seals' policies and practices pertaining to Internet and computer security.
- Not permit any unauthorized individual to obtain access to Easter Seals Internet connections, or data, including but not limited to, the PHI of Easter Seals' customers.
- Not use or permit the use of any unauthorized device in connection with Easter Seals' personal computers.
- Only use Easter Seals Internet resources (software/hardware or data) for authorized company purposes.
- Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
- Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess. (See Password Protection policy).
- Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
- Report to the VP of IT, IT staff, or Compliance Committee any incident that appears to compromise the security of Easter Seals' information resources. These include missing data, virus infestations, and unexplained transactions.
- Access only the data and automated functions for which he/she is authorized in the course of his/her normal job functions.

- Obtain supervisor authorization for any uploading or downloading of information to or from any Easer Seals multi-user information system if this activity is outside the scope of normal business activities.
- All Agency data should be maintained on an Easter Seals network storage location.

8. RECEIVING AND SENDING FAXES INCLUDING PHI

Background

Easter Seals staff and customers or organizations with which Easter Seals interacts may need to transmit or receive PHI by fax. Easter Seals staff could, in error, send faxes to unauthorized recipients; faxes could be intercepted or lost in transmission; or Easter Seals may not receive a fax intended for it because of one of these or other reasons.

Policy

All Easter Seals staff must strictly observe the following standards relating to fax communication of customer PHI:

- Easter Seals staff shall send PHI by fax only when the original record or mail-delivered copies will not meet the needs of immediate customer care or when it is impractical to send the PHI via encrypted email.

- Easter Seals staff shall transmit PHI by fax to the customer upon the Customer's request or to a third party upon the Customer's request, provided the customer has provided a signed authorization (see Authorization for Release of PHI, in this Manual).

- Easter Seals staff shall transmit PHI by fax when required by a third-party payer for payment purposes.

- Easter Seals staff must limit PHI transmitted to only that amount that is necessary to meet the requester's needs.

- Easter Seals staff may not send by fax especially sensitive medical information, including, but not limited to, AIDS/HIV information, mental health and developmental disability information, alcohol and drug abuse information, and other sexually transmissible disease information without the express authorization of the Director of Health Information Management.

- The cover page accompanying the fax transmission must include the "**Fax Confidentiality Notice**" contained in the Appendix.

- Easter Seals staff must make reasonable efforts to ensure that they send the fax transmission to the correct destination. Easter Seals staff must preprogram frequently used numbers into the machine to prevent misdialing errors. For a new recipient, the sender must verify the fax number before sending the fax, must verify the recipient's authority to receive PHI, and must confirm by telephone that the recipient received the information.

- Fax machines must be in secure areas where incoming faxes are not visible to unauthorized persons. Incoming faxes must not be left sitting on or near the machine, but shall be distributed to the proper recipient expeditiously while protecting confidentiality during distribution.

- Easter Seals staff must report any misdirected faxes to the Compliance Officer, or a member of the compliance committee.

- The Compliance Officer and/or his/her designee will periodically and/or randomly check all speed-dial numbers to ensure their currency, validity, accuracy, and to verify the authority of the recipient to receive PHI.

- **Users must immediately report violations of this policy to their department head, the Compliance Officer, or a member of the compliance committee.**

9. PASSWORD PROTECTION

Background

Because much of Easter Seal's customer information is stored in electronic computer networks and devices, Easter Seals must take great care to ensure that access to those computers, networks, and devices is strictly limited to authorized staff with a need to know and/or view that information. A key element of Easter Seals' access control policy is the use of access codes and passwords. This policy outlines the specific policies and procedures for management of those codes and passwords.

Policy

The confidentiality and integrity of data stored on Easter Seals computers and other devices must be protected by Access Controls to ensure that only authorized employees have access. Each employee with a need to use Easter Seals computer systems and networks shall have a unique user name and password as follows:

- Each password will not be less than 8 characters in length.
- Passwords must comply with at least three of these four rules.
    (1) English upper case letters – A, B, C, …Z
    (2) English lower case letters – a, b, c, …z
    (3) Westernized Arabic numerals – 0, 1, 2, …9
    (4) Non-alphanumeric "special characters" - #, &, etc.
- The password expires every 90 days.
- A password may not be reused in less than 36 months.
- Passwords should not be associated with personal information (e.g., PIN used for bank cards, date of birth for self or family members, telephone numbers, first or last name of self or family members, passwords used for Internet accounts).

Procedure

A. Information Technology Department Responsibilities

- The Information Technology department shall be responsible for the administration of Access Controls to all company computer systems.
- The Information Technology department will deploy and maintain a set of system/network access and password procedures that require unique user identification codes and passwords that conform to the characteristics outlined above.
- The Information Technology department will assign responsibility for maintenance of the access code and password assignment to a qualified individual in the Information Technology department. Additionally, a back-up staff person of the department will also be assigned these duties as a backup to the primary staff person.
- The Information Technology department will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.
- Deletions may be processed by an oral request prior to reception of the written request.
- The Information Technology department will conduct an audit of the access code and password policies to ensure that Easter Seals staff is complying with these procedures. This will be done monthly by selecting 20 random active directory accounts.

B. Employee Responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not disclose his/her password to others.
- Shall immediately change his/her password if it is suspected that it has become known to others. In the event that an employee suspects or knows that his/her password has become known to an unauthorized person, the employee should immediately report this event to:
    - IT Help Desk and perform a password change.
- Shall not record his/her password where it may be easily obtained. Employees shall not display passwords in any area that can be viewed by others. For example, passwords should not be written on "sticky" notes on the monitor, placed on paper and taped to the bottom of the keyboard, etc.
- Shall use passwords that will not be easily guessed by others.
- Shall log out when leaving a workstation for more than 30 minutes or when leaving the premises for any length of time.

Supervisor's Responsibility

Managers and supervisors should notify the Information Technology department promptly whenever an employee leaves the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Human Resources responsibility

The Human Resources department will notify the Information Technology department monthly of employee transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

Violations and Penalties

Penalties for violating this policy will vary depending on the nature and severity of the specific violation. Any employee who violates the policy will be subject to:

- Disciplinary action as described in the Easter Seals employee handbook, including but not limited to reprimand, suspension, and/or termination of employment.
- Civil or criminal prosecution under federal and/or state law.

Acknowledgment of Password Protection Policy

This form is used to acknowledge receipt of and compliance with the Easter Seals' Password Protection Policy.

A **"Password Protection Policy Acknowledgement"** form is included in the Appendix. All Easter Seals employees shall complete the Password Protection Policy Acknowledgment, which shall be retained in the employee's personnel records.

10. USING E-MAIL TO SEND OR RECEIVE PHI

Background

Customers of Easter Seals often want to communicate with Easter Seals staff via email. Transmitting PHI by email, however, has a number of risks, both general and specific, that customers should consider before using email. Among general email risks are the following:

- E-mail can be immediately broadcast worldwide and be received by many intended and unintended recipients.
- Recipients can forward email messages to other recipients without the original sender's permission or knowledge.
- Users can easily misaddress an email.
- E-mail is easier to falsify than handwritten or signed documents.
- Backup copies of email may exist even after the sender or the recipient has deleted his or her copy.
- E-mail containing information pertaining to a patient's diagnosis and/or treatment must be included in the customer's medical records. Thus, all individuals who have access to the medical record will have access to the email messages.
- Employees do not have an expectation of privacy in email they send or receive at their place of employment. Thus, customers (or their parents/guardians) who send or receive email from their place of employment risk having their employer read their email.
- Although Easter Seals and its employees and agents will endeavor to read and respond to email promptly, Easter Seals cannot guarantee that any particular email message will be read and responded to within any particular period of time. Behavioral health and human service providers rarely have time between appointments, consultations, staff meetings, meetings away from the facility, and meetings with customers and their families to continuously monitor whether they have received email. **Email should never be used in a medical emergency.**

Policy

Easter Seals shall make all email messages sent or received that concern the diagnosis or treatment of a customer part of that customer's medical record and will treat such email messages with the same degree of confidentiality as afforded other portions of the medical record. Easter Seals will use reasonable means to protect the security and confidentiality of email information, including encryption of email communication when it is affordable and practicable. Because of the risks associated with email communication of PHI, customers must consent to the use of email for communication of PHI after having been informed of the above risks.

Consent to the use of email includes agreement with the following conditions:

- All emails to or from the customer concerning diagnosis and/or treatment will be made a part of the customer's medical record. As a part of the medical record, other individuals, such as other physicians, nurses, physical therapists, customer accounts personnel, and the like, and other entities, such as other healthcare providers and insurers, will have access to email messages contained in medical records.

- Easter Seals may forward email messages within the facility as necessary for diagnosis, treatment, and reimbursement. Easter Seals will not, however, forward the email outside the facility without the consent of the customer or as required by law.

- If the customer sends an email to Easter Seals, one of its staff members, another healthcare provider, or an administrative department, Easter Seals will endeavor to

read the email promptly and respond promptly, if warranted. However, Easter Seals can provide no assurance that the recipient of a particular email will read the email message promptly. **Because Easter Seals cannot assure customers that recipients will read email messages promptly, customers must not use email in a medical emergency.**

- If a customer's email requires or invites a response, and the recipient does not respond within a reasonable time, the customer is responsible for following up to determine whether the intended recipient received the email and when the recipient will respond.

- Because some medical information is so sensitive that unauthorized disclosure can be very damaging, customers should not use email for communications concerning diagnosis or treatment of AIDS/HIV infection; other sexually transmissible or communicable diseases, such as syphilis, gonorrhea, herpes, and the like. Customers should be aware that information concerning mental health or developmental disability; or alcohol and drug abuse has the same sensitivities and risks.

- Because employees do not have a right of privacy in their employer's email system, customers should not use their employer's email system to transmit or receive confidential medical information.

- Easter Seals cannot guarantee that electronic communications will be private. We will take reasonable steps to protect the confidentiality of customer email but is not liable for improper disclosure of confidential information not caused by Easter Seals gross negligence or wanton misconduct.

- If the customer consents to the use of email, he/she is responsible for informing Easter Seals of any types of information the customer does not want to be sent by email other than those set out in paragraph 3, above.

- Customer is responsible for protecting his/her password or other means of access to email sent or received from Easter Seals to protect confidentiality. We are not liable for breaches of confidentiality caused by customer.

- Any further use of email by the customer that discusses diagnosis or treatment by the customer constitutes informed consent to the foregoing. **The Customer may withdraw consent to the use of email at any time by email or written communication to Easter Seals, attention: Compliance Officer.**

Procedure

If a customer wishes to communicate PHI via email, an Easter Seals staff member must review the risks of email communication set forth in the Background, above and must provide the customer with a copy of this Policy. After the customer has been advised of the risks, the Easter Seals staff member shall provide the customer with the "**Consent to Use of E-mail**" form included in the Appendix and shall request that the customer sign the form. The original, signed form shall be provided to the Compliance Officer and a copy shall be provided to the customer.

11. SOFTWARE AND HARDWARE POLICY

It is important to the success our organization to ensure the quality and upkeep of our software and hardware. Without an effective software/hardware policy in place, Easter Seals cannot adequately protect these expensive and vital investments. This software/hardware policy outlines the acceptable use of both software and hardware, defines standard software and hardware equipment, and explains the penalties for inappropriate use of organizational software and hardware.

Acceptable Use

This section defines the boundaries for the "acceptable use" of Easter Seals' electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by Easter Seals are to be used only for creating, researching, and processing Easter Seals-related materials. By using Easter Seals' hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable Easter Seals policies, as well as city, state, and federal laws and regulations, including the HIPAA Privacy Rule and the HIPAA Security Rule.

Software

All software acquired for or on behalf of Easter Seals or developed by Easter Seals' employees or contract personnel on behalf of Easter Seals is and shall be deemed Easter Seals' property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

Software Purchasing

All purchasing of Easter Seals' software shall be centralized with the Information Technology department to ensure that all applications conform to corporate software standards and are purchased at the best possible price. All requests for corporate software must be submitted to the budget administrator for that department for approval. The request must then be sent to the Information Technology department, which will then determine the appropriate software that best accommodates the desired request.

Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on Easter Seals' computers. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of the Easter Seals' Software/Hardware Policy.

Software standards

Employees needing software other than those programs that are part of the standard suite of software installed on Easter Seals computers must request such software from the Information Technology department. Each request will be considered on a case-by-case basis in conjunction with the software-purchasing section of this policy.

Hardware

All hardware devices acquired for or on behalf of the Easter Seals or developed by Easter Seals' employees or contract personnel on behalf of the Easter Seals is and shall be deemed Easter Seals property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

Hardware Purchasing

All purchasing of Easter Seals' computer hardware devices shall be centralized with the Information Technology department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price. All requests for corporate computing hardware devices must be submitted to the budget administrator for that department for approval. The request must then be sent to the Information Technology department, which will then determine standard software that best accommodates the desired request.

Violations and penalties

Penalties for violating the Software/Hardware Policy will vary depending on the nature and severity of the specific violation. Any employee who violates the Software/Hardware Policy will be subject to:

(i) Disciplinary action as described in the Easter Seals employee handbook, including but not limited to reprimand, suspension, and/or termination of employment.
(ii) Civil or criminal prosecution under federal and/or state law.

Procedure

All Easter Seals staff who use Easter Seals software or hardware shall:

1. Read the Information Technology Policy.
2. Sign and date the Acknowledgement of the Information Technology Policy form.
3. Return the Acknowledgement of the Information Technology Policy form to the Human Resources Department.

12. LAPTOP AND PORTABLE DEVICE POLICY

Background

Laptop computers and other portable electronic devices pose a significant security risk because they may contain customer PHI and, being portable, are more at risk for loss, theft, or other unauthorized access than Easter Seals' desktop computers. In addition, laptop computers may be more vulnerable to viruses and other threats because the user may not regularly use virus protection software and other electronic safeguards that Easter Seals does on its network. In addition, portable computer use is more difficult for Easter Seals to audit; thus security breaches may be more difficult to identify and to correct.

Policy

No Easter Seals staff may use a personally-owned computer or portable electronic device for Easter Seals business purposes without the written authorization of the VP of Information Technology. No user may, for any purpose, download, maintain, or transmit customer PHI onto a personally-owned computer or personally-owned portable electronic device without the written authorization of the VP of Information Technology upon the recommendation of the department head.

The Easter Seals Information Technology Department may issue company-owned laptops or portable electronic devices to an Easter Seals workforce member who is determined by his or her supervisor and the department head to have a demonstrated need for such technology. The Easter Seals Information Technology Department shall keep a record of all workforce members who have been issued such equipment.

Procedure

A. VP of Information Technology

The Easter Seals VP of Information Technology or his or her designee shall:

- Provide a copy of this Laptop and Portable Device Policy to each Easter Seals workforce member to whom a laptop or portable electronic device has been given.
- Keep a written record of all workforce members who have been issued company-owned laptop computers or portable electronic devices.
- Ensure that such devices maintain up-to-date virus protection software.
- Conduct random audits of such devices to ensure that they are being used solely for Easter Seals business.
- Ensure that users do not download any software onto the devices except as are authorized by the VP of Information Technology.

B. Employee Responsibilities

Employees who have been issued company-owned computers or portable electronic devices shall:

- Notify the IT Department of any virus or of any unusual behavior of the device.
- Use the computer or other device only for Easter Seals business.
- Use only batteries and power cables provided by Easter Seals.
- Not connect any additional peripherals (keyboards, printers, modems, etc.) without the express authorization of the IT Department.
- Keep the computer or device secure within their homes, cars, and other locations.
- Not leave computers or devices unattended unless they are in a secured location.
- Not leave mobile computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.
- Use the proper carrying cases when transporting computers and other devices.
- Not alter any serial numbers or any sticker or other item identifying the computer or device as property of Easter Seals.
- Not permit anyone else to use the computer or device for any purpose, including, but not limited to, the user's family and/or associates, customers, customer families, or unauthorized members of the Easter Seals staff.
- Not share their passwords with any other person and shall safeguard their passwords. (See the Password Protection Policy in this Manual).
- Report any breach of password security immediately to the Information Technology department.
- Maintain customer confidentiality when using such computers or devices.
- Properly log out and turn off the computer or other device when it is not in use.
- Immediately report to the Information Technology department any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality.

Enforcement

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment.

13. REMOTE ACCESS POLICY

Background

Remote access is a generic term used to describe the accessing of Easter Seals' computer network by individuals not located at the organization's primary office. This may take the form of traveling employees, employees who regularly work from home, or employees who work both from the office and from home. In many cases, both the Agency and the employee may benefit from the increased flexibility provided by a remote access program.

As with any innovation, however, the benefits may be countered by risks if the purposes and methods of the program are not fully understood by all participants.

> **To optimize the efficiency of our remote access program, we have created a clear policy governing eligibility, obligations and responsibilities of remote users.**

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting Agency needs. The Agency may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

Policy and Procedures

Easter Seals' policies for remote access are as follows:

Acceptable Use

Hardware devices, software programs, and network systems purchased and provided by the Agency for remote access are to be used only for creating, researching, and processing Agency-related materials. By using Easter Seals' hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable Agency policies, as well as City, State and Federal laws and regulations.

Your eligibility to remotely access Easter Seals' computer network will be determined by your manager and the Information Technology department.

Equipment & Tools

Easter Seals will provide tools and equipment for remotely accessing the corporate computer network in a secure manner. This may include computer hardware, software, phone lines, email, voicemail, VPN hardware and software, connectivity to host applications, and other applicable equipment as deemed necessary.

The use of equipment and software provided by Easter Seals for remotely accessing the computer network is limited to authorized persons and for purposes relating to Agency business. Easter Seals will provide for repairs to Agency equipment. When the employee uses her/his own equipment, the employee is responsible for maintenance and repair of equipment.

Password and Privacy Protection

By using the Agency's hardware, software and network systems employees assume personal responsibility for their appropriate use and agree to comply with the Easter Seals' Password Protection policy. In addition, employees agree to take maximum precautions to prevent unauthorized access and/or viewing of customer's PHI during remote access sessions. To do this, employees must agree to place the computer in a secure environment (not in open living rooms or other common spaces) and to log-off of the Agency network when absent from the computer.

Use of Personal Computers and Equipment

There are literally thousands of possible interactions between the software needed by the remote user and the average mix of programs on most home computers. Troubleshooting software and hardware conflicts can take hours, and can result in a complete reinstall of operating systems and application software as the only remedy for problems. For that reason the Information Technology department will only provide support for equipment and software provided by Easter Seals.

The employee is solely responsible for backing up data on their personal machine before beginning any Agency work. At its discretion, Easter Seals will disallow remote access for any employee using a personal home computer that proves incapable, *for any reason*, of not working correctly with the Agency-provided software, or being used in a production environment. If the employee has a critical need for remote access and the employee's personal computer(s) is unsuitable for the task, the employee should submit a formal request for Agency equipment to be provided. This request should flow through the employee's direct supervisor to the Information Technology department.

Because of the extreme security and privacy risks associated with the use of remote access and personal computers, employees are strictly prohibited from downloading, copying, or otherwise keeping customer's PHI on personal computers. Because of these risks, employees agree to allow site visits by Information Technology staff for purposes of auditing the security features of remote access systems.

Violations and Penalties

Penalties for violation of the Remote Access Policy will vary depending on the nature and severity of the specific violation. Any workforce member who violates the Remote Access Policy will be subject to:

(i) Disciplinary action as described in the Easter Seals' employee handbook including but not limited to reprimand, suspension and/or termination of employment or contract
(ii) Civil or criminal prosecution under Federal and/or State law

Acknowledgment of Remote Access Policy

This form is used to acknowledge receipt of, and compliance with, the Easter Seals' Remote Access Policy.

14. REPORTING A BREACH OF CONFIDENTIALITY

Background

The federal HITECH Act, which was part of the American Recovery and Reinvestment Act of 2009, requires a Covered Entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured protected health information" to notify each individual "whose Unsecured PHI has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, or disclosed" because of the breach.

Policy

Easter Seals will take all reasonable steps to maintain the confidentiality of Unsecured PHI. In the event of a breach of confidentiality of Unsecured PHI, we will notify the customer, and if necessary, federal authorities and local media outlets, pursuant to the policy below.

Procedure

"Unsecured PHI" is PHI that is not secured through the use of a technology (such as encryption) that renders the PHI unusable, unreadable and undecipherable to unauthorized users. For example, electronic PHI that has not been encrypted is considered "unsecured" because it could be accessed by an unauthorized user and, once accessed it would be useable and readable. Paper copies of written PHI are also Unsecured PHI because the records would be easily usable and readable if an unauthorized user accessed them.

The following are examples of a breach of Unsecured PHI:

- A staff member takes a portion of a customer's record with her to the coffee shop and inadvertently leaves the record behind.
- A staff member has a customer's chart in her car and the car is stolen.
- A staff member has Unsecured PHI on her laptop and her laptop is stolen.

Easter Seals staff who become aware of a breach of Unsecured PHI shall immediately report the incident to the Compliance Officer and/or a member of the compliance committee.

The following circumstances do not require Easter Seals to notify the customer of a breach:

- Unintentional acquisition, access, or use of PHI by a member of our workforce or an individual acting under our authority, provided that such unintentional activity was done in good faith, within the course of his or her duties and does not result in further use or disclosure that is not permitted by the HIPAA Privacy Regulations.

- Inadvertent disclosure of PHI by a person with authority to access PHI to another person who also has authority to access PHI (including a Business Associate), provided the recipient does not further disclose the information in violation of the HIPAA Privacy Regulations.

- Unauthorized disclosures where, based on the good faith belief of the disclosing person, the recipient to whom the PHI is disclosed would not reasonably have been able to retain the information.

The Compliance Officer and/or his/her designee shall investigate the incident and confirm (1) whether Unsecured PHI was involved (2) whether a breach occurred, (3) whether the breach affected more than 500 customers, and (4) the identity of the customers whose Unsecured PHI was breached.

Easter Seals will notify a customer in writing by U.S. Mail or by email of any breach of the customer's Unsecured PHI as soon as possible, but in any event, no later than sixty (60) days following the discovery of the breach. If the breach involves ten (10) or more customers whose contact information is out of date, Easter Seals will post a notice of the breach on the home page of our website. If the breach involves more than five hundred (500) customers, we will send a notice of the breach to a prominent media outlet in the state in which the affected Easter Seals facility is located, and we will immediately notify the Secretary of the US Department of Health and Human Services. If the breach involves less than five hundred (500) customers, Easter Seals shall disclose the breach in its annual breach notification reporting to the US Department of Health and Human Services.

The Notices required under this policy shall include the following:

- A brief description of the breach, including the date of the breach (if known) and the date of its discovery;
- A description of the types of Unsecured PHI involved in the breach;
- Steps the customer should take to protect himself/herself from potential harm resulting from the breach;
- A brief description of the actions Easter Seals is taking to investigate the breach, mitigate losses, and protect against further breaches;
- Contact information, including a toll-free telephone number, email address, or postal address to permit the customer to ask questions or obtain additional information; and
- Any sanctions imposed on any workforce member involved in the breach.

The Compliance Officer and the Compliance Committee shall compile a log of breaches of Unsecured PHI and shall evaluate Easter Seals' Policies and Procedures to minimize such breaches.

15. STAFF TRAINING FOR SECURITY AND PRIVACY

Background

The HIPAA Privacy Rule and the HIPAA Security Rule both require that appropriate training be provided to all workforce members concerning the privacy and security of PHI. All workforce members must have some degree of basic training concerning the policies and procedures in this Manual. Some staff members will require more training than others, depending upon their functions within Easter Seals.

Policy and Procedures

Easter Seals trains all members of its staff on the policies and procedures with respect to PHI as necessary and appropriate for the members of the staff to carry out their respective functions within the agency.

This training is:

- Provided to each member of Easter Seals' workforce, including volunteers, affiliates, contractors, students, residents, and other persons who are likely to have contact with PHI.
- Provided to all new hires within 30 days of hiring; and
- Provided to each staff member whose functions are affected by a material change in the policies or procedures of Easter Seals, within a reasonable period of time after the material change becomes effective. acknowledgement

Easter Seals will document that the training has been provided.

The training on security and privacy will include the following topics:

- General awareness of security and privacy issues, including specific awareness of HIPAA regulations and requirements
- Easter Seals policies and procedures with respect to PHI and information security
- Vulnerabilities of health information in Easter Seals' environment
- Security responsibilities of each staff member
    - General security awareness and responsibility
    - Password protection
    - Virus prevention
    - Data backup procedures
    - Remote access
    - Removal of information from Easter Seals
    - Customer records outside of the official medical record
    - Proper authorization and consent to release procedures
    - Workstation acceptable use policies and practices
    - Customer rights and responsibilities regarding medical records
- Procedures to follow in case of a suspected breach of security or privacy
- Disaster plan and emergency procedures

Once this training program has been received and acknowledged by all current staff, Easter Seals will deploy a continuing training plan that includes the following features:

- Basic security awareness training as outlined above will be repeated for all staff at least once every three years after the initial training. Staff members receiving this follow-up training will complete another acknowledgement of training receipt form.

- At least every six months, the Human Resources department, in conjunction with Information Technology, and the Compliance Committee, will publish a security reminder via email to all staff.

The Appendix contains an **ON-SITE INSPECTION CHECKLIST** form, which will be used by the Information Systems department to conduct inspections of Easter Seals facilities to confirm compliance with the privacy and security policies and procedures in this Manual.

16. DISASTER RECOVERY AND SECURITY

Background

Easter Seals recognizes that it has an obligation to protect the confidentiality and integrity of its customers' PHI and that it must have an appropriate plan to continue to provide services to its customers in the event of a disaster that might affect the operability of Easter Seals' computers and other electronic devices. It is imperative that Easter Seals' hardware and software assets be protected from all kinds of disasters and that a plan be implemented that minimizes inconvenience and provides accessibility to these assets in the event of an emergency.

Policy

The viability of the core Agency applications and networks are critical to the operation of Easter Seals. Because almost all members of the Easter Seals workforce use Easter Seals' hardware and software in the performance of their duties or as part of the Agency's business and clinical processes, all members of the workforce should have a basic familiarity with this Disaster Recovery Plan.

It is the goal of the Easter Seals Disaster Recovery Plan to restore service to critical components of its information technology infrastructure no more than one (1) business day from the time of the disaster. User offices must be prepared to operate on their own during that one-day outage and should have a means of catching up with the information once the access is restored. It is the goal of the Disaster Recovery Plan to restore access to non-critical components could be restored within one business week.

Implementation of the Plan

In the case of a declared disaster, all or part of the disaster recovery team will assemble to assess the situation. In the case of a partial outage, the team coordinator will work directly with the person responsible for the affected component or service and take the necessary steps to restore service according to the priorities as outlined in the plan. In the event of a major disaster such as extensive loss of hardware components or inaccessibility to facilities, the team will require access to other resources on a priority basis. Users will be notified of the disaster and given frequent updates on the status of restoring services. All communications to users, customers, and the general community will flow through the Public Relations Coordinator.

Plan attachments

The following items are not distributed, but filed with the plan:

- Information Technology department complete organization chart
- Inventory listing of all hardware, software, network, telecommunications, and other Fixed Assets
- Inventory listing of core application server components
- Site Evacuation charts
- Primary Network Distribution Center Recovery Procedure
- Vendor Maintenance Agreements and Emergency Contacts
- Off-site backup Service Level Agreement and Emergency Contacts
- Hot (or cold) site backup Service Level Agreement and Emergency Contacts

DISASTER RECOVERY AND SECURITY

I. Introduction

The main premise of the plan is to distribute mission critical computer infrastructure to the primary business and clinical service locations of Easter Seals. The most critical components will be located at the primary site, *555 Auburn Street, Manchester, NH 03103* and the secondary site, *Colospace, 70 Innerbelt Road, Somerville, MA 02370*. This reduces the necessity of making any one facility fail safe from disaster.

The plan describes the composition of the disaster recovery team and procedures to follow in the event of a disruption in service to a mission critical component. Since timely action is critical, backup personnel are identified if the designated team leaders cannot be reached. Depending on the extent of the disaster, a subset of the team or the entire team may be involved in resolving the problem.

II.A. Physical Facilities

Primary Site: *555 Auburn Street, Manchester, NH 03103*, the existing information technology center, will be the primary location for housing the mission critical infrastructure equipment. This site contains the most up-to-date equipment:

- Fire protection with Halon and sprinklers
- A commercial uninterruptible power system
- Hook-up to the main Agency emergency power generator
- Close access to a main telecommunications hub
- Limited secured access
- On-site staff.

There is plenty of expansion space and the state of the facility is excellent. It is also conveniently available to all authorized IT personnel.

Alternate Site: The alternate site will be located at *Colospace, 70 Innerbelt Road, Somerville, MA 02370* and shall be accessible on a limited basis by authorized persons only. The site is equipped with raised flooring, adequate air conditioning, standalone uninterruptible power units and dedicated connections to a main telecommunications hub. The site will be equipped with monitoring devices that will allow IT staff to view the room through the network. This will be very helpful during hours when the site is closed. In the event the primary site is severely damaged and will be out of commission for a prolonged period, the alternate site will become the primary site.

II.B. Critical Components

These components provide mission critical services to the Easter Seals that need to be restored within one business day from the point of the declared disaster. The resources that make up these components have been distributed to separate locations outside the main computer room to reduce the possibility of complete failure. As a part of the plan, a diagram and complete inventory of the equipment is attached. A general description of each critical component is identified and described below:

MAIN APPLICATION SERVER: These computers provide access for staff to electronic mail, administrative and clinical software applications. Half of this resource will be kept at the primary site and half at the alternate site. If the resource cannot be equally distributed, the major resource will be located at the primary site. The computers will be clustered and connected with dedicated high speed fiber.

Disk Sub-system: The main disk sub-system unit will reside at the primary site and a duplicate will be placed in the alternate location. These systems will be connected to the computer cluster in each location and through software will shadow (duplicate updated information) each other. In the case one site is lost; the software will keep track of the updates and catch up all transactions once the connection is reestablished. As an extra precaution, each disk sub-system is equipped with instant fail-over from loss of either a power supply or a controller (initially, the alternate site will not have two controllers). In the case an individual disk unit is lost; spares will be kept at both sites to make restoration timely and efficient. The functioning site will continue to allow updates during the outage.

Network: The main network switch is located in *555 Auburn Street, Manchester, NH 03103* and is separate from the computer room. A dedicated fiber path will be established to connect the main network switch to the secondary site switch and then to the alternate site. This is done to provide uninterrupted and non-competing service between the clusters at high speeds.

LAN (Local Area Network): These Intel-based computers will be distributed to locations in the primary site connected with high speed dedicated fiber. These computers provide access to all licensed supported PC software to staff. The number of these units will be increased over time to minimize the risk of equipment failure or loss of any one location due to a disaster.

Web Server: Web functions are currently performed by computers with the following operating systems and platforms: 2003 – 2008. The Agency is standardized on one major platform and provides duplicate systems in separate locations to minimize an outage in the event of a disaster.

Voice Response: These Intel-based computers will be distributed to two locations in the primary site. It is important to keep these units accessible to IT personnel, so there will not be units distributed to alternate sites. These units are higher-end computers with voice cards, so it is possible to obtain replacement cards and use other units on campus in the event we lose one or more of these units.

Team Headquarters: If the primary site is usable, the team will assemble in the Board Room at 555 Auburn Street, Manchester, NH 03103. In the event the building or room is unavailable, the team will meet at an alternate site. The first option is a conference room in the secondary site, to be assigned at the time by the CEO or designee, and the second option would be space assigned by the VP of IT.

Duties and Responsibilities: The disaster recovery team members and responsibilities follow the organization structure of Information Technology Services.

Disaster Recovery Coordinator - The Vice President of IT will serve in the capacity of the Disaster Recovery Coordinator. The responsibilities are:

- Determine the extent and seriousness of the disaster.
- Invoke the Disaster Recovery Plan.
- Coordinate the disaster recovery activities.
- Name replacements to fill in for disabled disaster recovery team members.
- Inform Easter Seals senior management of recovery activities and information.

Systems Programming and Operations Recovery Team Coordinator - The IT Coordinator <OR EQUIVALENT> will serve in the capacity of the Systems Programming and Operations Recovery Team Coordinator. The responsibilities are:

- Assume the responsibilities of the Disaster Recovery Coordinator in the event he/she is disabled or not available.
- Inform the Disaster Recovery Coordinator of recovery activities and information.
- Negotiate with vendors and managers of backup facilities.
- Coordinate scheduling for programming and computer time.
- Coordinate activities of the systems recovery and operations recovery team leaders.

Systems Recovery Team Leader - The IT Coordinator will serve in the capacity of the Systems Recovery Team Leader. The responsibilities are:

- Determine the extent of systems file and communications disability.
- Inform Operations Recovery Team Leader of which backup files are needed.
- Provide technical advice and assistance to Operations recovery Team.
- Oversee and coordinate all interim systems and programming functions and systems recovery.
- Schedule and direct return to normal operations.
- Assist the Quality Control Recovery Team Leader in meeting production schedule.
- Review production cycles and prioritize applications with users.
- Identify required involvement of application and user personnel.
- Coordinate required activities for applications staff and users as necessary.

Operations Recovery Team Leader - The IT Administrator will serve in the capacity of the Operations Recovery Team Leader. The responsibilities are:

- Determine the extent of equipment disability.
- Assist with negotiations with vendors and managers of alternate site facilities.
- Notify operations personnel of required activities, locations and schedules.
- Oversee and coordinate all interim operations functions and equipment recovery.

- Secure backup material from off-site storage and coordinate delivery to appropriate sites.
- Schedule and direct return to normal processing operations.

Note: The PC Support Coordinator will assist and also serve as backup to the Operations Recovery Team Leader.

Quality Control Recovery Team Leader - The Database Administrator will serve in the capacity of Quality Control Team Leader. The responsibilities are:

- Determine the extent of disability to documentation and tape library material.
- Coordinate retrieval of backup material from off-site storage facility.
- Notify quality control personnel of required activities, locations and schedules.
- Oversee and coordinate all interim quality control functions and recovery.
- Schedule and direct return to normal quality control operations.

Note: The Business Systems Coordinator will assist and also serve as backup to the Quality Control Recovery Team Leader.

Historian/Secretary for Recovery Team - The Help Desk/IT Liaison will serve in the capacity of historian/secretary for the recovery team. The responsibilities of the historian/secretary are:

- Record all disaster recovery activities pursuant to the Disaster History Outline.
- Provide support for the coordinator.

Network Support System Recovery Team Leader - The IT Coordinator Manager will serve in the capacity of the Computer Network Recovery Team Leader. The responsibilities are:

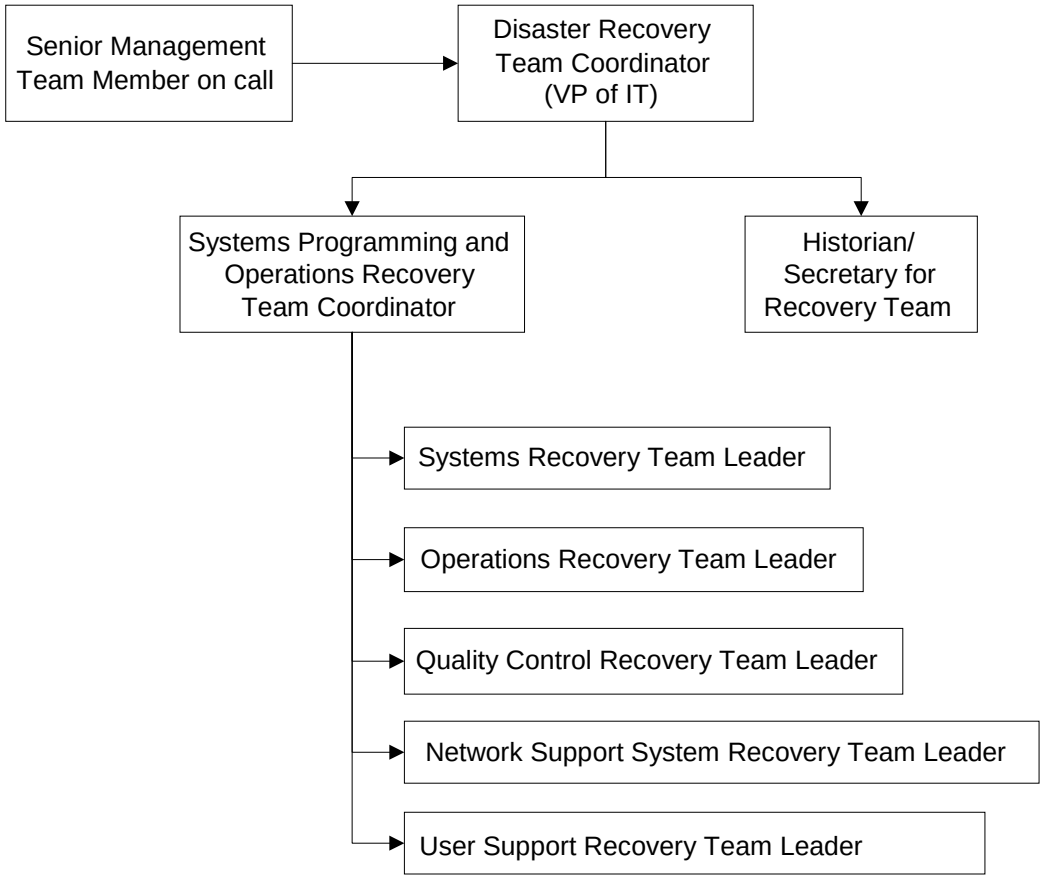
- Determine the extent of network disability or outage.
- Negotiations with vendors to acquire equipment.
- Notify subordinate personnel of required activities, locations and schedules.
- For equipment malfunctions, place maintenance call for repair.
- Coordinate distributing load to other available LANs.
- If unit is damaged beyond repair, initiate replacement process.
- Restore services to normal upon repair or replacement.

User Support Recovery Team Leader - The PC Support Coordinator will serve in the capacity of the User Support Recovery Team Leader. The responsibilities are:

- Determine the extent of equipment disability.
- Ascertain disability of software and training program materials.
- Coordinate acquisition of replacement materials and products.
- Notify End User Support personnel of required activities, locations and schedules.
- Oversee and coordinate all interim activities.
- Define criteria for establishing a temporary backup facility.
- Schedule and direct unit return to normal operations.

The chart on the following page outlines the structure of the Disaster Recovery Team.

Disaster Recovery Team Structure



II.D. Equipment Maintenance and Replacement

In the event of breakage, damage or loss of equipment, various approaches are taken to restore the service provided by the component. Decisions about the approach are dependent upon the critical nature of the equipment, cost and number of units in service. In some cases, the equipment is protected against loss with full replacement protection under a service or insurance policy. In other cases, spare components may be kept on hand and swapped in the event of a failure. Most critical components are placed under vendor maintenance service agreements for normal service requirements. Refer to Appendix for list of major components and the method used to maintain and/or replace them. Copies of all vendor agreements will need to be kept with the plan at the primary and alternate site location.

The following describe the major services provided by external vendors:

Vendor Maintenance - For protection against outages due to normal wear and tear, outside vendors are contracted to perform maintenance services. This is usually the manufacturer of the equipment, but not necessarily in all circumstances.

Normal contracted maintenance conditions include:

- Call window - 8 a.m. - 5 p.m., (Monday through Friday)
- Parts - furnished.
- Labor - furnished.
- Response time - within four (4) hours of notification, or next business day.
- Type of maintenance included:
  - Preventive
  - Continued Remedial - (Customer approved/action plan after 4 hours)
  - Remote Diagnostics
  - Installation of Engineering Modifications

Equipment Replacement - In some cases, services are used for full product repair and/or replacement for damage caused by accidents or incidents not covered under service agreements. These plans expand service to cover fire, water damage, natural disasters, power failure, sprinkler leakage, theft, etc. It provides reimbursement for the cost of transportation, removal of damaged equipment, installation of replacement equipment, and replacement of fire protection chemicals, restoration of damaged system software and restoration of customer data from backup disks/tapes. The preceding service is in reference to services provided by HP Financial Services.

These services are only available on items under full maintenance coverage and chargeable at a percentage of the annual fee for that component or through special agreements as attachments to vendor contracts.

For critical and non-critical items, the extra cost of replacement services and insurance would have to come from existing Agency resources. Decisions of whether to cover items would also take into consideration the state of technology, the cost of replacement and evaluating the risk of loss versus the on-going annual premium cost. These decisions will be revisited each year during the review process.

II.E. Back-up Procedures

The main application server(s) are backed up to tape on a daily basis using the BACKUP utility. This backup is called an incremental backup. It is done Monday through Friday nights, to copy all files that have been updated since the last BACKUP was performed.

On Saturday night, a full BACKUP of the entire system is taken. On Monday morning, the full backup tapes are sent to the vault, where they are stored until the next full BACKUP of the system is performed.

In tape storage, there are designated tapes that are used in a round-robin fashion for the incremental backups, which means there is at least five days' worth of tapes containing incremental data, and at least two sets of chronicled full system-wide BACKUPS on site, and one current set in the vault.

III. TESTING OF THE PLAN

Testing of the plan to simulate an actual disaster will be done at least once per year. The VP of Information Technology will inform the Disaster Recovery Coordinator or designee that a test disaster has been declared. This notice will include the type of disaster and the plan will be followed to test readiness and completeness as if an actual disaster has taken place. Since critical resource components are limited, the test should not take place while customers are in active service delivery at the primary service delivery location or during peak processing periods.

Although there may be some inconvenience to the users during the test, there will be no prolonged outage to the users. The plan could be tested by a controlled shutdown of the computers in either location, and verify that the other cluster carried the critical load without disruption of service or loss of information.

The test should cover the following activities:

- Notifying the Disaster Recovery Team members.
- Assembling the team at one of the designated locations.
- Visiting the offsite storage location to inventory backup files.
- Visiting and inspect the alternate site.
- Sending notification to affected user areas
- Coordinating associated activities with user areas.
- Recording events of the test, evaluating preparedness and making needed adjustments.

IV. IMPLEMENTATION OF THE PLAN

IV.A. Circumstances to Declare a Disaster

Any event that is likely to significantly disrupt mission-critical services or cause personal injury will require that measures be taken to limit the outage or damage, reduce risk of personal injury and enhance an orderly shutdown. Under these circumstances, a disaster will be declared and the plan followed.

In the event there is a limited outage due to loss of a critical component that doesn't cause widespread loss of service or is temporary, an abbreviated plan of action will be followed. The appropriate person responsible for the service will take measures to correct the problem. In some cases, this may be a service call to the vendor responsible for maintenance.

All events will be documented and discussed as part of the review process to determine whether changes to the plan are necessary to reduce the risk of future failures.

Depending on the time which a disaster is discovered or reported, the following describes the possible scenarios:

IV.B. Major Event Significantly Disrupting Services

Emergency Procedures When the Primary Site is Unoccupied - In the event it is necessary to provide notification of a disaster or emergency during a period when the building is unoccupied, it is expected that senior management team member on call will initiate the notification procedures outlined above until one team member is contacted. The team member notified by the senior management representative on call will complete the notification process. Should the fire detection alarm system activate, the Fire Department is notified through an auto dial system. The fire department will contact the senior management representative on call for building entrance. The senior management representative on call has a key to the computer room entrance door. A key to the fire alarm box is located on the wall at the control panel in the computer room. The senior management representative on call will initiate the above procedure provided that the building is safe to enter.

Operations section team members will report to the primary site, completing the damage assessment evaluation prior to reporting to the team headquarters. The damage assessment team members will be admitted to the building after presenting their Easter Seals I.D. cards to the senior management representative on call at the site.

Emergency Procedures When Building Is Occupied - In the event it is necessary to provide notification of a disaster or emergency during a period when the building is occupied, it is expected that the Operations Manager will initiate the notification procedures. This assumes that the primary site computer room or the adjacent space is involved with the disaster. Otherwise, the Director of IT or designee will initiate the notification procedures.

The following activities may be directed as the situation may require:

- An announcement to evacuate the building. Messengers will be sent for this purpose. A copy of the building evacuation chart is attached.
- Designate individuals to secure the area by activating lockup.
- Initiate shutdown procedures for equipment, electrical service, or air conditioning.
- Direct damage limiting measures to be taken.
- Determine need for and secure emergency support services to insure personnel safety and building security.

IV.C. Procedures to Utilize Alternate Site

In the event of a major disaster that destroys or leaves the primary site unusable for a prolonged period of time, the alternate site and a designated secondary site would be used to restore service. Although mission critical services will be up within one business day, non-critical services may take a week to restore. Please reference the appendices for an inventory of items deemed critical and non-critical. The physical space at the alternate site will be expanded as possible to accommodate the additional equipment.

IV.D. Procedures to Restore Service for Critical Components

The infrastructure is designed to provide reasonable resumption of mission-critical services within one business day from the point of the declared disaster. The procedures for notification of the disaster and duties of the disaster recovery team are found in this document. This section gives a general description of the approach for the restoration of service to the critical components. The approach for each is as follows:

- PRIMARY APPLICATION SERVER HARDWARE - In the event that a single unit malfunctions, a service call is placed and the remaining computers in the cluster will handle the load. In the event that computers are damaged at one site, a service call is placed, an assessment of damage is made by a qualified technician, users would be notified and priority access procedures go into effect. In the event the unit(s) is not repairable, Recover-All procedures are initiated.

- DISK SUB-SYSTEM - In the event that a single unit malfunctions, a service call is placed and the remaining disk sub-system in the other cluster will handle the load. In the event that the unit is damaged at one site, a service call is placed, an assessment of damage is made by a qualified technician and operations would monitor activity to assure proper functioning. In the event the unit is not repairable, Recover-All procedures are initiated. Once the unit is replaced, both manual and software restore procedures are initiated to make sure both units contain identical data. Depending on whether the disk units were damaged and the timing of the outage, this may be an off-shift process to copy from one sub-system to the other.

- NETWORK - In the event that a major network hub is lost, users at sites or locations connected to that hub will lose access. The network design will accommodate redundant links to critical locations, but other sites or locations will be affected. The terms of the maintenance agreement will be initiated for that particular switch, which in most cases is shipping of another unit. This process could take more than one business day to complete.

- If the main network switch is inoperative or damaged, a maintenance agreement is in place to acquire a spare within eight hours. Once we received the switch, it would be replaced and service would be restored. In the event the room is not available due to extensive damage or environmental concerns, the switch would be placed in the secondary site to function as the main hub. After some adjustments are made to the links, service would be restored to the remainder of sites.

- LAN (Local Area Network) - The infrastructure is designed to distribute multiple units and connect them in an efficient manner to the network. If a major unit becomes inoperative, services would be shifted to other LAN units to handle most of the demand. The unit would either be repaired or replaced on a priority basis. These units are not on maintenance and not insured against loss. The cost of replacement and the ability to spread the risk of loss to other units don't warrant the additional cost of insurance.

- WEB SERVER - The primary web server is located in the primary site. In the event of failure, a service call would be placed on an emergency basis. If the outage is prolonged, another computer on the cluster would be designated as the web server and the appropriate files restored from the backups.

- VOICE RESPONSE - The load for this service is handled by three PCs, two located at the primary site and one at the secondary site. In the event of failure on any unit, a service call would be placed on an emergency basis. The load to provide the service would be shifted to the remaining devices. These units are not on maintenance and not insured against loss. The cost of replacement and the ability to spread the risk of loss to other units don't warrant the additional cost of insurance.

IV.E. System Access

Although each location will have multiple computers, that will probably not be sufficient to allow everyone to conduct business without some notice in response time or limiting the number of users, but it will certainly be sufficient to conduct critical business and clinical operations. This may also be an issue related to network access. In the event that controlled access is necessary, a combination of restricting the number of users or by time blocks will be used. For example, administrative use may be restricted to morning hours and clinical use in afternoon hours. For administrative users, the operations section will work with the heads of the user areas to identify key personnel to grant immediate access. At that point, reference would be made to the user area disaster recovery plans.

IV.F. Processing Priorities

In the event that the disaster creates a critical shortage of resources that don't permit all users to access the systems simultaneously, restrictions on access will be initiated and the production schedules altered to process in mission critical order.

Establishing application priorities and schedule planning are limited to short term recovery, which is the period until regular operations are back to normal. It is expected that normal scheduling will be resumed as the alternate and secondary sites are available.

The priority requirements and schedule will be developed and approved as directed by the Operations Manager. This is done after consultation with the major user areas. Timing of the interruption during the production cycle may affect priority requirements and scheduling.

General priorities of systems and functions are considered to be: 1) payroll, 2) financial systems, 3) electronic mail and web access, and 4) clinical record processes (including intake and progress notes).

IV.G. Meeting Space

Primary and alternate meeting sites for the Disaster Recovery Team personnel have already been addressed under Disaster Recovery Team Headquarters. In the event a disaster occurs, relocation of personnel may be necessary until suitable space can be secured. The senior management team is responsible for space scheduling. Information concerning available sites and locations, as well as assistance in the acquisition of needed floor space will be provided by the senior management team member on call.

IV.H. Operational Procedures

A copy of the vendor supplied operation manual is kept in the computer room. Manuals for each auxiliary device are stored with the device.

Task scheduling will be prioritized according to the severity and extent of the disaster.

All documentation for core business and clinical systems on the main application servers are maintained on-line. This provides automatic backup under standardized procedures with off-site storage.

IV.I. History Outline

The Disaster Recovery Team is responsible for establishing and maintaining a record of all disaster recovery activities. This history will be a record of events for subsequent reviews and debriefings with governmental agencies, insurance companies, vendors, and suppliers, et al.

The history outline shall include:

- Chronological log of disaster events
- Chronological log of recovery steps
- Analysis of cause of disaster
- Man hours and estimated costs of recovery tasks
- Statement of the impact of service interruptions
- Evaluation of the effectiveness of activities
- Recommendations to minimize impact of future disaster

V. DISTRIBUTION AND REVISIONS

The Disaster Recovery Plan will be distributed to the following individuals:

- Members of the Disaster Recovery Team and their designated backups
- Senior management team members on call
- President and Board of Directors
- Program Directors and Unit Managers
- Primary off-site contacts where there is no supervisory-level staff present
- Security company contact
- Primary application vendor contact
- Primary hardware vendor contact

A copy of the plan will also be stored in the VP of Information Technology's Office and with the backup files and documentation at the off-site vault location.

The Disaster Recovery Team will review the plan every six months in consultation with the senior management team. Normal updates such as names, telephone numbers, equipment changes, and office relocation will be made routinely and distributed to all holders of the plan. Other revisions to the plan that change procedures and other major aspects will be submitted to the senior management team and Board of Directors for review and approval. These changes will be distributed upon approval.

VI. APPROVAL

This Disaster Recovery Plan has been reviewed and is approved:

_____

President/Chief Executive Officer Date

_____

President, Board of Directors Date

_____

VP of Information Technology Date

- Secondary site is redundant.

Disaster Recovery Team Contact List

CONTACT	POSITION OR FUNCTION	PHONE (W)
ALTERNATES		

Emergency / Senior Management Team Contact List

CONTACT	LOCATION	NUMBER
Fire, Ambulance, Police		

Component Inventory Assessment List

Type:
- Critical
- Non-critical

Maintenance
- Yes
- No

Insured
- Yes (if yes, specify coverage and contact)
- No

Location
- Primary Site
- Secondary Site
- Alternate Site

COMPONENT	TYPE	QUANTITY	MAINT?	INSURED?	LOCATION	COMMENTS
Continue as needed						

Disaster Recovery Team Meeting Checklist

Task	Assignment	Timeline	Status
First Meeting After Declaration of Disaster			
Review status of disaster alert and notification action	Team	Immediate	
Review status of site	Team	Immediate	
Review report on damage assessment	Coordinator	Immediate	
Establish time for next meeting, report on assessment, recommend action	Coordinator	Immediate	
Prepare status notice to Easter Seals officials and users	Coordinator	Immediate	
Subsequent Meetings After Declaration of Disaster			
Obtain and consolidate damage assessments	Team	Immediate	
Identify and quantify production capability	Team	Immediate	
Evaluate need to utilize alternate and/or secondary site	Team	Immediate	
Identify cleanup and repair requirements to support critical systems	Team	Immediate	
Assign responsibility for each team member to perform assigned duties	Coordinator	Immediate	
Follow-up with team leaders on status	Coordinator	Periodic	
Insure all information is recorded for history outline	Team	Continuing	
Notify appropriate authorities of extent of disaster and action required	Coordinator		
Depending on extent of disaster, determine and seek emergency funding	Coordinator		

Damage Assessment Checklist

Description of Item	Damage	Recover Action	Assignment	Estimated Completion
Site - Access				
Hazards				
Building - Structure				
▪ Utilities (Electrical, water, phone)				
▪ Climate Control				
▪ Fire Detection and Suppression				
▪ Office Furnishings				
Primary Site – Application Servers				
▪ Disk Sub-system				
▪ Network Components				
▪ LAN Servers				
▪ Voice Response Units				
▪ UPS				
▪ Power Conditioner				
▪ Tapes 9 track				
▪ Tapes 8mm				
▪ Tapes DLT				
▪ Laser Printers				
▪ Impact Printers				
▪ Modems				
▪ Computer Workstations				
▪ Unit Record Equipment				
▪ Optical Scanners				
▪ Cables				
▪ Records/documentation				
Alternate Site – Application Servers				
▪ Disk Sub-system				
▪ UPS				

17. COMPLIANCE OFFICER AND SECURITY OFFICER

The Easter Seals Compliance Officer / Privacy & Security Officer s Tina Sharby. The Compliance Officer is responsible for overseeing the organizations compliance program inducing monitoring and self-evaluating programs/procedures related to the Agency's legal and regulatory obligations. The Compliance Officer reports directly to the President and CEO.

18. COMPLIANCE COMMITTEE

The Compliance Committee's purpose is to oversee the Agency's implementation of compliance programs, policies and procedures that are designed to be responsive to the various compliance and regulatory risks facing the Agency.

The Compliance Committee shall have representation from each program and administrative areas with the intent of promoting oversight, training, support and leadership. At a minimum the Finance Department, Information Technology department, and Human Resources department is required to have representation.

The Compliance Committee is responsible for ensuring that the organization meets its obligations, including training, reporting and auditing.

Responsibilities of the Compliance Committee include:

- Oversight of the Agency's compliance programs, state and federal compliance requirements, licensing requirements, etc. This includes the;
    - Identification of legal or regulatory compliance exposure
    - Identification of Program regulations that need to be complied with
    - Identification of State and Federal laws that need to be complied with
- Oversight of the Agency's compliance related policies, the Company's Code of Business Conduct, and other relevant laws and regulations.
    - The Committee shall monitor the Company's efforts to implement compliance policies and procedures that are designed to be responsive to the various compliance and regulatory agencies.
    - Internal monitoring and auditing to ensure adherence with various compliance and regulatory agencies.
- Investigating compliance issues, suspected or actual violations of law, regulations, or policy. The Committee may involve others for assistance when and where necessary while performing an investigation.
- Coordination of the review of complaints received from internal and external sources, including the Compliance Hotline.
- Training and Education

19. FALSE CLAIMS

The purpose of this policy is to inform employees, contractors and agents of Easter Seals and its subsidiaries of the provisions of the federal and state false claims acts (FCAs), including their right to report violations of federal and state law. This policy also includes general information regarding Easter Seals' efforts to combat fraud, waste and abuse and to describe the remedies and fines for violations that can result from certain types of fraudulent activities.

Reporting Fraud, Waste and Abuse

All employees, contractors, and agents of Easter Seals must immediately report to the Corporate Compliance Officer any suspicion of fraud, waste, or abuse in connection with the business of Easter Seals. Easter Seals engages in specific compliance efforts to detect and prevent fraud, waste and abuse, such as the Corporate Compliance Program.

For more information on the Easter Seals Corporate Compliance Program and specific compliance policies, or on how to report any concerns, please contact the Compliance Hot Line 1-800-870-8728 ext. 3001 or compliance@eastersealsnh.org.

Detailed Information of the Federal False Claims Act

The federal FCA imposes civil (and in some cases criminal) penalties on people and entities who knowingly submit a false claim, or act in deliberate ignorance of the claim's truth or falsity or act in reckless disregard of its truth or falsity or conspire to defraud the government by getting a false or fraudulent claim paid. Specific intent to defraud is not required.

The FCA includes an important provision that allows private citizens to initiate a lawsuit on behalf of the federal government and to request that the government join in the suit. In return, that citizen may share a percentage of any recovery or settlements. This type of lawsuit is known as a qui tam and the individual, or relator, is a "whistleblower", who brings forth evidence of the alleged improper conduct. The purpose of this qui tam provision is to give an incentive for whistleblowers to come forward to help the government discover and avoid paying fraudulent claims as well as prosecute those who submit false claims by awarding whistleblowers a percentage of the recovery.

To prevail under a lawsuit, the relator must be the "original source" of the information reported to the federal government. Specifically, the relator must have direct and independent knowledge of the false claims activities and voluntarily provide this information to the government. If the matter disclosed is already the subject of a federal investigation, or if the healthcare provider or supplier has previously disclosed the problem to a federal agency, the relator may be barred from obtaining a recovery under the FCA.

A private legal action under the FCA must be brought within six (6) years from the date that the false claim was submitted to the government. Depending upon the circumstances, a government-initiated claim may be brought up to ten (10) years after the false claim.

The FCA is not confined to healthcare claims, but extends to any payment requested of the federal government. The FCA applies to billing and claims sent from Easter Seals NH, Inc.to any government payer program, including Medicare and Medicaid.

It is the policy of Easter Seals that an employee, contractor or agent of Easter Seals NH, Inc. who knowingly submits a false claim will be reported to the necessary authorities. Under the FCA, anyone or any entity that submits a false claim or statement to the government may be fined a civil penalty between $5,500 and $11,000 for each such claim submitted, regardless of the size of the false claim, and the person or entity could be required to pay three (3) times the

amount of the damages that the government sustains. In addition, the government can exclude violators from participating in Medicare, Medicaid, and other federal healthcare programs.

Examples of potential false claims include, but are not limited to: (a) billing of items or services that were never rendered by the health care provider; (b) billing for services that are medically unnecessary; (c) up coding (practice of billing for Medicare/Medicaid using a billing code providing a higher payment rate than the billing code intended to be used for the service or item furnished to the patient); (d) billing separately for services that should be bundled; (e) billing separately for outpatient services that were provided within 72 hours (before or after) an inpatient stay; (f) billing for a discharge in lieu of a transfer.

Whistleblower Protection – Federal Law

The federal FCA protects employees who are discharged, demoted, suspended, harassed, or in any manner discriminated against by their employer because of their participation or assistance (e.g., testimony, initiation of investigation) in a false claim action.

The FCA entitles employees to relief to "make them whole", including restatement with the same seniority status they would have had but for the discrimination, twice the back pay, interest on back pay, and compensation for any special damages sustained as a result of the discrimination including litigation costs and reasonable attorneys' fees.

Detailed Information of the Federal Program Fraud Civil Remedies Act

Individuals or entities that commit fraud against the federal government, by false claims or statement, can be assessed money penalties in addition to the penalties of the FCA under the Program Fraud Civil Remedies Act (PFCRA). PFCRA penalties of $5,000 per false claim or statement apply if an individual or entity submits a claim to the federal government that: the individual or entity knows or has reason to know is false, fictitious, or fraudulent; includes or is supported by written statements containing false, fictitious, or fraudulent information; includes or is supported by written statements that omit a material fact, which causes the statements to be false, fictitious, or fraudulent and the individual submitting the statement has a duty to include the omitted fact; or is for payment of property or services that are not provided as claimed.

The $5,000 penalty also applies if a person or company provides written back-up or materials relating to the claim in which the individual or entity asserts a material fact that is false, fictitious or fraudulent; or omits a fact that the individual had a duty to include, the omission causes the statement to be false, fictitious, or fraudulent, and the statement contains a certification of accuracy.

State False Claims Acts

Each state that Easter Seals provides services in have their own FCA, which are very similar to the federal FCA. Please refer to the regulation grid below for further information.

New Hampshire:

NH RSA 167:61-a et seq.

The Whistleblowers' Protection Act (RSA 275-E)

Vermont:

This state does not currently have a false claims law. Please refer to the state legislature's official website for any recent developments.

Maine:

26 M.R.S.A. 831-840

Rhode Island:

R.I. Gen. Laws §§ 9-1.1-1 through 9-1.1-8

19. DISCIPLINE

All supervisors are responsible for enforcing these Policies and Procedures. Workforce members who violate this policy are subject to discipline up to and including termination of employment/contract.

APPENDIX OF FORMS

FORM NO. 1.

Request for Correction/Amendment of Protected Health Information

Request for Correction/Amendment of Health Information

Customer Name: _____ Date of Birth: _____

Customer Address: _____
_____
_____

Date of Entry to be amended: _____

Please explain how the entry is incorrect or incomplete. What should the entry say to be more accurate or complete? Attach additional pages as necessary.

_____
_____
_____
_____

Would you like this amendment sent to anyone to whom we may have disclosed the information in the past? If so, please specify the name and address of the organization or individual.

_____
_____
_____

Date: _____ _____
Signature of Customer/Customer's Legal Representative

For Easter Seals Use ONLY:

Date Received: _____

Amendment has been: ☐ Accepted ☐Denied

If denied, check reason for denial:

☐ PHI was not created by Easter Seals
☐ PHI is not part of Customer's designated record set
☐ PHI is accurate and complete

Comments of Easter Seals Staff member:

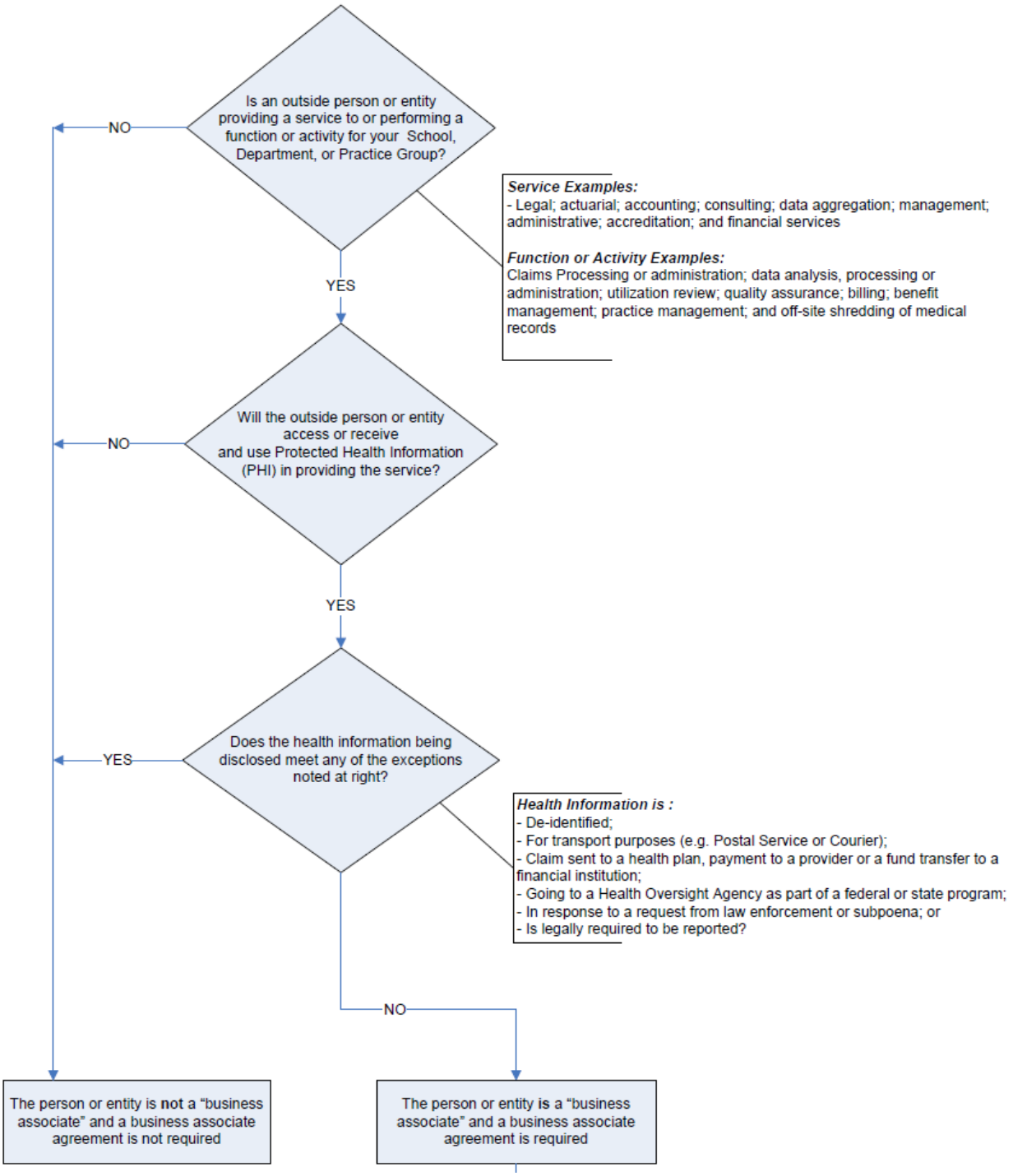
_____
_____

Date: _____ _____
Signature of Staff Member

_____
Printed Name and Title of Staff Member

FORM NO. 2

Flow Chart for Determining Whether Contractor or Vendor is a Business Associate



FORM NO. 3

Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") effective as of _____ _____ 2010 (the "Effective Date") is entered into by and between Easter Seals (the "Covered Entity") and _____ (the "Business Associate").

WHEREAS, the Covered Entity has engaged the Business Associate to perform certain services for the Covered Entity (the "Service Agreement") and the Covered Entity may disclose Protected Health Information (as hereinafter defined) to the Business Associate and the Business Associate may receive, use, disclose, transmit, store and/or maintain (collectively, "Uses and/or Discloses" or, as the context shall require "Use and/or Disclosure") the Protected Health Information in its performance of services for the Covered Entity; and

WHEREAS, the Covered Entity and the Business Associate intend to comply with (a) the Standards for Privacy of Individually Identifiable Health Information codified at 45 C.F.R. Part 160 and Part 164 (the "Privacy Rules"); (b) the Standards for Electronic Transactions codified at 45 C.F.R. Part 162 (the "Transaction Rules"); (c) the Standards for the Security of Individually Identifiable Health Information codified at 45 C.F.R. Part 164 (the "Security Rules"), all promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")(the Privacy Rules, Transaction Rules and Security Rules are sometimes collectively referred to herein as the "HIPAA Rules"); and (d) the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005, and regulations promulgated thereunder (the "HITECH Act") by the United States Department of Health and Human Services ("HHS"); and

WHEREAS, this Agreement sets forth the terms and conditions pursuant to which Protected Health Information that is provided by, or created or received by, the Business Associate from or on behalf of the Covered Entity will be handled, used, disclosed and protected.

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements hereinafter addressed, the parties agree as follows:

1. Definitions. Capitalized terms used in this Agreement that are not defined herein shall have the meaning ascribed to them in the HIPAA Rules and the HITECH Act. For the purposes of this Agreement:

(a) "Administrative Safeguards" has the meaning given in 45 C.F.R. § 164.304, with the exception that it shall apply to the Business Associate's Workforce and not the Covered Entity's Workforce.

(b) "Protected Health Information" has the meaning given in 45 CFR § 160.103 except that it shall also be deemed to include Electronic Protected Health Information.

2. Services. The Business Associate provides services for the Covered Entity that involve the Use and Disclosure of Protected Health Information. Except as otherwise specified

herein, the Business Associate may make any and all uses of Protected Health Information that are necessary to perform its obligations under the Service Agreement. However, the Business Associate may Disclose Protected Health Information for the purposes authorized by this Agreement only (a) to its employees, subcontractors and agents, in accordance with Section 3, or (b) as otherwise directed by the Covered Entity.

3. Responsibilities of Business Associate. With regard to its Use or Disclosure of Protected Health Information, the Business Associate hereby agrees that it shall:

(a) Approved Uses or Disclosures. Use or Disclose the Protected Health Information only as needed to perform its obligations to the Covered Entity under the Service Agreement, provided that such Use or Disclosure would not violate the HIPAA Rules or the HITECH Act if done by the Covered Entity.

(b) Prohibited Uses and Disclosures. Not Use or further Disclose Protected Health Information other than as permitted or required by this Agreement, the Service Agreement or as otherwise required by law. Business Associate shall not Use or Disclose Protected Health Information for Fundraising or Marketing purposes or otherwise receive remuneration, either directly or indirectly, in exchange for Protected Health Information, except with prior written consent of the Covered Entity and as permitted by the HITECH Act; however, this prohibition shall not include payment to Business Associate by the Covered Entity for services provided pursuant to the Service Agreement. Further, Business Associate shall not Disclose Protected Health Information to a Health Plan for Payment or Health Care Operations if the Individual has requested this special restriction, such restriction has been communicated to the Business Associate, and the Individual has paid out of pocket in full for the health care item or service to which the Protected Health Information solely relates.

(c) Minimum Necessary. Use or Disclose only the minimum amount of Protected Health Information necessary to accomplish the purpose of the request, Use or Disclosure. Business Associate understands and agrees that as of the Effective Date regulations and official guidance from HHS concerning the definition of "minimum necessary" have not yet been issued in final form and the Business Associate covenants that it shall keep itself informed of official HHS guidance or regulations issued after the Effective Date and that it shall comply with any such guidance or regulations.

(d) Appropriate Safeguards. Use appropriate safeguards to prevent unauthorized Use or Disclosure of such Protected Health Information.

(e) Cooperate with Covered Entity. Cooperate with the Covered Entity in investigating and in taking (i) prompt corrective action to cure any violation of the HIPAA Rules or the HITECH Act, including but not limited to, making reasonable efforts to mitigate, to the extent practicable, any harmful effects arising from any improper access, Use or Disclosure of Protected Health Information under the terms of this Agreement or any Security Incident or Breach of unsecured Protected Health Information of which it becomes aware, and (ii) any action pertaining to any such violation or breach required by such federal regulations.

(f) Reporting to Covered Entity. Report to the designated Compliance Officer of the Covered Entity, in writing, (i) any Use or Disclosure of Protected Health Information that is not permitted or required by this Agreement, any Breach of Unsecured Protected Health Information and (ii) any Security Incident of which Business Associate becomes aware within

ten (10) days of the Business Associate's discovery of such unauthorized Use or Disclosure or Security Incident.

(g) Employees, Subcontractors, etc. Require all of its employees, representatives, subcontractors or agents that receive or use or have access to Protected Health Information to agree to adhere to the same restrictions and conditions on the Use and/or Disclosure of Protected Health Information as are contained herein.

(h) Access by Individuals. Provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable the Covered Entity to fulfill its obligations under the HITECH Act, including but not limited to those set forth at 42 U.S.C. § 17935(e).

(i) Amendment of Protected Health Information by Individuals. Make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity. If any individual requests an amendment of Protected Health Information directly from Business Associate (or Business Associate's agents or subcontractors), Business Associate shall notify the Covered Entity within ten (10) business days of the request. Any approval or denial of a request to amend Protected Health Information maintained by Business Associate (or Business Associate's agents or subcontractors) shall be the responsibility of the Covered Entity.

(j) Accounting for Disclosures. Document such disclosures of Protected Health Information and make available to the Covered Entity such information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528 and the HITECH Act (specifically, 42 U.S.C.§ 17935(c). At a minimum, Business Associate (and Business Associate's agents and subcontractors) agrees and warrants to document and provide: (i) the date of disclosure; (ii), the name of the person or entity to whom the disclosure and, if known, the address of the person or entity who received Protected Health Information; (iii) a brief description of the Protected Health Information disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual who is the subject of the Protected Health Information of the basis for the disclosure, or a copy of the written request for disclosure. If Business Associate (or Business Associate's agent or subcontractor) directly receives a request for an Accounting of Disclosures, Business Associate shall forward the request in writing to the Covered Entity within ten (10) calendar days of the receipt of such request by Business Associate (or its agent or subcontractor). If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable the Covered Entity to fulfill its obligations under the HITECH Act, including but not limited to those set forth at 42 U.S.C. § 17935(e).

(k) Access by HHS. Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of Protected Health Information to the Covered Entity, or at the request of the Covered Entity to the Secretary of HHS for purposes of determining the Covered Entity's compliance with the HIPAA Rules and the HITECH Act.

(l) Access by Covered Entity. Upon written request, make available during normal business hours at Business Associate's offices all records, books, agreements, policies and procedures relating to the Use and/or Disclosure of Protected Health Information to the Covered Entity within thirty (30) days for purposes of enabling the Covered Entity to determine the Business Associate's compliance with the terms of this Agreement.

(m) Return or Destruction of Protected Health Information. Return to the Covered Entity or destroy in the manner required by this Agreement, as requested by the Covered Entity, within thirty (30) days of the expiration or termination of this Agreement, the Protected Health Information in Business Associate's possession and retain no copies or back-ups of any kind.

(n) Security Safeguards. Implement reasonable and appropriate Administrative, Physical and Technical Safeguards (set forth at 45 CFR §§ 164.308, 164.310 and 164.312) to (i) protect the Confidentiality, Integrity, and Availability of the Protected Health Information that the Business Associate Uses and/or Discloses on behalf of the Covered Entity, and (ii) to prevent the Use or Disclosure of Protected Health Information other than as provided in this Agreement or as otherwise Required by Law. Business Associate shall also comply with the policies, procedures and documentation requirements of the Security Rules as set forth at 45 C.F.R. § 164.316.

(o) Rendering Protected Health Information Unusable, Unreadable or Indecipherable. Use the Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of the HITECH Act as set forth at 74 Federal Register 19006-19010, to:

(i) Determine whether "unsecured protected health information" has been breached, thereby triggering the notification requirements specified in section 13402 of the HITECH Act and its implementing regulations; and

(ii) Dispose of documents and/or electronic media containing Protected Health Information in such a manner as to render it unusable, unreadable or indecipherable (as described in Section 3(p)(ii) below).

(p) Destruction of Documents and Electronic Media Containing Protected Health Information. Except as otherwise provided in this Agreement, including but not limited to Section 5(c), Business Associate shall ensure that Protected Health Information provided to or obtained by Business Associate from the Covered Entity that is contained in any document or electronic media is rendered unusable, unreadable or indecipherable to unauthorized individuals in disposing of any such documents or electronic media either in the normal course of business or under this Agreement by destroying it in one of the following ways:

(i) Paper, film, or other hard copy media shall be shredded or destroyed such that the Protected Health Information cannot be read or otherwise cannot be reconstructed; or

(ii) Electronic media shall be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the Protected Health Information cannot be retrieved.

(q) Pattern or Practice of Breach by Covered Entity. Pursuant to 42 U.S.C. § 17934(b), if Business Associate becomes aware of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations under this Agreement, the Business Associate agrees and warrants to take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, Business Associate agrees to terminate any Underlying Agreement(s) and this Agreement if feasible or, if termination is not feasible, report the problem to the Secretary of HHS. Business Associate shall provide written notice to the Covered Entity of any pattern or practice that Business Associate believes constitutes a material breach or violation of Covered Entity's obligations under this Agreement within five (5) business days of discovery.

4. Responsibilities of the Covered Entity. With regard to the Use and/or Disclosure of Protected Health Information by the Business Associate, the Covered Entity hereby agrees:

(a) To inform the Business Associate of any changes in the form of notice of privacy practices that the Covered Entity provides to individuals pursuant to 45 C.F.R. §164.520 and provide the Business Associate a copy of the notice currently in use;

(b) To inform the Business Associate of any changes in, or withdrawal of, the permission provided to the Covered Entity by individuals whose Protected Health Information may be used or disclosed by Business Associate, if such changes affect Business Associate's permitted or required Uses and/or Disclosures;

(c) To notify the Business Associate, in writing and in a timely manner, of any restrictions on the Use and/or Disclosure of Protected Health Information agreed to by the Covered Entity as provided for in 45 C.F.R. §164.522; and

(d) Not to request Business Associate to Use and/or Disclose Protected Health Information in any manner that would not be permissible under the HIPAA Rules if done by the Covered Entity.

5. Term and Termination.

(a) Term. This Agreement shall become effective on the Effective Date and shall terminate when all of the Protected Health Information provided by Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or, if it is not feasible to return or destroy such Protected Health Information, protections are extended to such information in accordance with Section 5(c) below.

(b) Termination. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation and may terminate this Agreement and the Service Agreement if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity. If the Business Associate has breached a material term of this Agreement and cure is not possible, then the Covered Entity may immediately terminate this Agreement and the Service Agreement. If termination is not feasible, the Covered Entity shall report the breach to the Secretary of HHS.

(c) Effect of Termination.

(i) Except as provided in subparagraph (ii) of this Section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall also apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information. If the Business Associate elects to destroy all Protected Health Information as aforesaid, then Business Associate shall certify in writing to the Covered Entity that such Protected Health Information has been destroyed in accordance with the terms of Section 3(p) of this Agreement, unless the maintenance by Business Associate of such Protected Health Information is required by applicable law or if it is infeasible as described in subparagraph (ii) of this Section.

(ii) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 3 and 5(c) shall survive the termination of this Agreement indefinitely.

7. Amendment. This Agreement may not be modified or amended, except in writing as agreed to by each party. Provided, however, that the parties agree to take such action as is necessary to amend this Agreement to comply with the requirements of the HIPAA Rules and the Health Insurance Portability and Accountability Act, Public Law 104-191.

8. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

9. Notices. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to Business Associate: Attn: _____
_____
_____
_____

If to Covered Entity: _____, Compliance Officer
Easter Seals
_____
_____

10. Inconsistencies. To the extent of any inconsistencies between the Service Agreement and this Agreement, the terms and conditions of this Agreement shall be controlling.

11. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rules and the HITECH Act.

12. Entire Agreement. This Agreement contains the entire agreement of the parties with respect to the subject matter hereof and all other agreements between the parties concerning the subject matter hereof, whether oral or written, are superseded hereby.

IN WITNESS WHEREOF, the parties hereto hereby execute this Agreement as of the Effective Date.

Business Associate:
_____

_____
Witness

By: _____
Name: _____
Title: _____
Date: _____

Covered Entity:
Easter Seals

_____
Witness

By: _____
Name: _____
Title: _____
Date: _____

EASTER SEALS
NH, VT, ME, & RI

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU (OR YOUR CHILD) MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice please contact our Compliance Officer who is Tina Sharby or any member of the Compliance Committee.

This Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services.

We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice, at any time. The new notice will be effective for all protected health information that we maintain at that time. Upon your request, we will provide you with any revised Notice of Privacy Practices. You may request a revised version by accessing our website, or calling the office and requesting that a revised copy be sent to you in the mail or asking for one at the time of your next appointment.

1. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Your protected health information may be used and disclosed by your service provider, our office staff and others outside of our office who are involved in your care and treatment for the purpose of providing health care services to you. Your protected health information may also be used and disclosed to pay your health care bills and to support the operation of your service provider's practice.

Following are examples of the types of uses and disclosures of your protected health information that Easter Seals is permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services.

Payment: Your protected health information will be used and disclosed, as needed, to obtain payment for your health care services provided by us or by another provider.

Health Care Operations: We may use or disclose, as needed, your protected health information in order to support the business activities of Easter Seals. These activities include, but are not limited to, quality assessment activities, employee review activities, training of therapy students, licensing, and conducting or arranging for other business activities.

We will share your protected health information with third party "business associates" that perform various activities (for example, billing or transcription services) for our practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

We may use or disclose your protected health information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. You may contact our Compliance Officer to request that these materials not be sent to you.

Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization or Opportunity to Agree or Object

We may use or disclose your protected health information in the following situations without your authorization or providing you the opportunity to agree or object. These situations include:

Required By Law: We may use or disclose your protected health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, if required by law, of any such uses or disclosures.

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information.

Communicable Diseases: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse or neglect to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Legal Proceedings: We may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the

extent such disclosure is expressly authorized), or in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and as otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of our practice, and (6) medical emergency (not on our practice's premises) and it is likely that a crime has occurred.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Uses and Disclosures of Protected Health Information Based Upon Your Written Authorization

Other uses and disclosures of your protected health information will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization in writing at any time. If you revoke your authorization, we will no longer use or disclose your protected health information for the reasons covered by your written authorization. Please understand that we are unable to take back any disclosures already made with your authorization.

Other Permitted and Required Uses and Disclosures That Require Providing You the Opportunity to Agree or Object

We may use and disclose your protected health information in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your protected health information. If you are not present or able to agree or object to the use or disclosure of the protected health information, then your service provider may, using professional judgment, determine whether the disclosure is in your best interest.

Others Involved in Your Health Care or Payment for Your Care: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.

2. YOUR RIGHTS

Following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

You have the right to inspect and copy your protected health information. This means you may inspect and obtain a copy of protected health information about you for so long as we maintain the protected health information. You may obtain your medical record that contains medical and billing records and any other records that your service provider and the practice use for making decisions about you. As permitted by federal or state law, we may charge you a reasonable copy fee for a copy of your records.

You have the right to request a restriction of your protected health information. This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment or health care operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply.

Your service provider is not required to agree to a restriction that you may request. If your service provider does agree to the requested restriction, we may not use or disclose your protected health information in violation of that restriction unless it is needed for an emergency. With this in mind, please make any request for a restriction on our use or disclosure of your protected health information in writing. Your service provider will then discuss your request with you and notify you whether Easter Seals can accommodate your request.

You have the right to request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to our Compliance Officer.

You may have the right to have Easter Seals amend your protected health information. This means you may request an amendment of protected health information about you in a designated record set for so long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Compliance Officer or any member of the Compliance Committee if you have questions about amending your medical record.

You have the right to receive an accounting of certain disclosures we have made, if any, of your protected health information. This right applies to disclosures for purposes other than treatment, payment or health care operations as described in this Notice of Privacy Practices. It excludes disclosures we may have made to you if you authorized us to make the disclosure, for a facility directory, to family members or friends involved in your care, or for notification purposes, for national security or intelligence, to law enforcement (as provided in the privacy rule) or correctional facilities, as part of a limited data set disclosure. You have the right to receive specific information regarding these disclosures that occur after April 14, 2003. The right to receive this information is subject to certain exceptions, restrictions and limitations.

You have the right to obtain a paper copy of this notice from us, upon request, even if you have agreed to accept this notice electronically.

3. COMPLAINTS

If you feel your privacy rights have been violated, you may file a complaint with us by notifying one of the following Easter Seals employees of your complaint. We will not retaliate against you for filing a complaint.

- Compliance Officer, Elin Treanor: (603) 621-3462 or by e-mail at etreanor@eastersealsnh.org
- Chief Human Resource Officer, Tina Sharby: (603) 621-3417 or by e-mail tsharby@eastersealsnh.org
- Confidential Compliance Hotline: (800) 870-8728 ext 7300
- Human Resources Department: (603) 621-3439 or by e-mail at HRhelp@eastersealsng.org
- Compliance Committee Chairperson, Heath Hooper: (603) 621-3541 or by e-mail hhooper@eastersealsnh.org
- Toll free number to Easter Seals: (800) 870-8728

This notice was published and becomes effective on April 15, 2011.

Receipt of Notice of Privacy Practices

I have received a copy of the Notice of Privacy Practices of Easter Seals

_____ _____
Signature (client, parent, guardian, responsible party) Date

_____
Print name of Signature

FORM NO. 5

Authorization for Use or Disclosure of Protected Health Information

EASTER SEALS

NH, VT, ME, & RI,

AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

General Information Regarding This Authorization

This Authorization permits Easter Seals (the "Provider") to use or disclose your Protected Health Information for purposes other than your treatment, payment to the Provider or the health care operations of the Provider. You have the right to revoke this Authorization by providing the Provider with written notice of revocation. The revocation will be effective upon receipt by the Provider except with respect to uses or disclosures made prior to receipt and in reliance upon this Authorization.

The Provider cannot require you to sign this Authorization as a condition to the provision of services.

Please note that once the requested information is disclosed pursuant to this Authorization, the Provider will no longer have control over the information and there is a potential that it may be re-disclosed by the recipient and will no longer be protected by the privacy rules under the Health Insurance Portability and Accountability Act.

Authorization

I hereby authorize the Provider or any of its staff to use or to disclose, by any acceptable means, including fax or email, my Protected Health Information described as follows:

_____
_____
_____
_____

To the following persons or class of persons (include name, address and telephone number):

_____
_____
_____

The purpose of the requested use or disclosure is:

_____
_____

This Authorization shall expire on _____, 20__, which is no more than one year after its effective date, unless it is revoked prior to the expiration date.

_____ _____
Witness Signature Signature of Client or Legal Representative

_____ _____
Print Name of Witness Print Name of Client

_____
Print Name of Legal Representative

_____
Date signed

FORM NO. 6

Fax Confidentiality Notice

The following Confidentiality Notice is to be included on all fax cover pages:

The information in this fax is confidential and is intended solely for the addressee. Access to this fax by anyone else is unauthorized and may lead to civil and/or criminal penalties. If you have received this message in error, please delete all electronic copies of this message (and the documents attached to it, if any); destroy any hard copies you may have printed or created; and notify Easter Seals immediately at 603-621-3439.

FORM NO. 7

Consent to Use of E-mail

Easter Seals
Consent to Use of E-mail Communication

1. All emails between the patient and Easter Seals ("Easter Seals") that contain protected health information ("PHI") and that concern diagnosis and/or treatment will be made a part of the Customer's medical record. Except as otherwise provided in this Consent, the PHI contained in emails shall be subject to the terms and conditions of the Easter Seals Notice of Privacy Practices.

2. If the customer sends an email to an Easter Seals staff member, he or she will endeavor to read the email promptly and respond promptly, if warranted. However, Easter Seals provides no assurance that the recipient of a particular email will read the email message promptly. **Because Easter Seals cannot assure customers that recipients will read email messages promptly, customers must not use email in a medical emergency.**

3. If a patient's email requires or invites a response, and the recipient does not respond within a reasonable time, the patient is responsible for following up to determine whether the intended recipient received the email and when the recipient will respond.

4. Many employers do not respect the privacy of emails sent or received by employees over the employer's network. Patients should not use their employer's email system to transmit or receive PHI.

5. Easter Seals cannot and does not guarantee that email communications will be private. Easter Seals will take reasonable steps to protect the confidentiality of customer email, but the customer agrees to hold Easter Seals harmless for any email transmission that is intercepted or disclosed in the absence of any gross negligence or wanton misconduct by Easter Seals.

6. The customer may withdraw consent to the use of email at any time by email or written communication to the Compliance Officer of Easter Seals.

The undersigned has been informed of the risks associated with the use of email to transmit PHI, has read and understood this Consent, and hereby consents to the use of email to transmit PHI between the patient and Easter Seals.

Patient Name: _____

_____ _____
Easter Seals Staff Witness Signature of Customer/Parent/Guardian

Date: _____ Date: _____

Form No. 8

ON-SITE INSPECTION CHECKLIST

Program:	
Site Location:	
Review Date:	
Reviewer:	

One of the ways that Easter Seals will remain in compliance with HIPAA is to conduct ongoing audits of the security and privacy practices of the facility. These will be conducted no less than annually. Conducting these audits is the responsibility of the program director. The results will be forwarded to the Compliance Committee of the Agency.

ITEM	YES	NO
PHYSICAL PLANT SECURITY –VISITOR CHECK-IN		
Does this location have a central reception/security desk that verifies access privileges prior to granting access to the facility that contains or can access protected health information?		
If appropriate, does this location maintain a visitor log, or customer sign in sheet--to include a positive identification check (e.g., a photo ID)? What happens to the customer sign in sheet at the end of the day?		
Does this location have a written policy on escorted and unescorted visitor requirements?		
Is there a sign-in sheet/mechanism for admission and tracking of non-staff personnel (consultants, technicians, etc.)? Programmer, Janitor, UPS, meter reader--		
WORK STATION		
Are any passwords displayed in public view? Not even in non-locked desks—where are the passwords? Only be maintained by someone in IT—locked desk file with limited access or database –walk around if you can spot passwords or if they give it to you—middle drawer of desk, under keyboard.		
Are computers/workstations visible from customer areas?		
Are there document shredding capabilities and procedures at this location? Look in waste baskets for PHI that is not shredded.		
Does this location take preventative measures to ensure that unauthorized persons are prevented from accessing others' health information? (Hint: Look for computer screens masks, password-protected screensavers, and paper records left unattended.)		
Does this location maintain a process to ensure that all health information is appropriately labeled? (Look at all media, including backup tapes, diskettes, output devices and forms.) Should not have a back up tape with no label—day and time – folders or unassembled records lying around.		
Does this location take appropriate measures to prevent end-users from bypassing the organization's security mechanisms? (Look for sharing of passwords, temporary badges, unauthorized health information storage locations (unlocked desks). Tight procedures on issuance of badges, regular inspection of file areas.		
SECURITY		
Does this location keep a record of breaches and how they were handled?		

ITEM	YES	NO
Example: Kaiser Permanente had a customer list –part of disease management program was to send e-mails to remind them of things like taking meds, eating well—someone made a mistake and the list went out to others not on the list—1) acknowledged the error, 2) immediately shut down external e-mail 3) called every person on diabetic list and told them what happened and tried to address concerns 4) sent to security committee –anything that we could have done to prevent—answer is yes—we could have tested this prior to sending it out after each system change.		
Is there a separate employee rest room/staff lounge? Is PHI posted in any way? Conversation that is often customer specific.		
FACILITIES, EQUIPMENT, AND COMMUNICATIONS		
Does this location maintain records that document repairs, or modifications to the facility (doors, locks, security systems)? Assumes current inventory and a change order process that is documented.		
Does this location have any of the following equipment on site? Server(s) Hub/Switch(s)—piece of networking equipment that sits between a server and a PC. Connection device. Router(s)—piece of hardware that handles network traffic—tells computers where to go. Firewall appliance(s)—box that essentially blocks intrusion attempts to the network. "Little black box" Modem(s)—may have more than you think!!!!! Backup device(s)—tape drives, optical drive (CD) Personal Computer(s) Mobile devices (PDAs, etc.) Printer(s) Fax Machine(s) Telecommunication hub/controller(s)—phone system –PC or computer device that runs the phone system. Software media (CDs, diskettes, etc.) Other: _____ Other: _____ Other: _____ Other: _____ Other: _____		
Is there is written inventory of the above listed equipment? Model #s, contact phone numbers, procedure or log for removing or moving.		
If yes, is the inventory on site? Where located—who is responsible, and how is it kept current?		
Is there a sign-out procedure/log for removal of equipment? Laptops, or PDAs, or even a server for repair.		
If yes, does the log contain: Staff name Staff department Reason for removal Date of removal Date of return Supervisor signature		
Do all PCs have surge protectors? Not HIPAA requirement –although it is indirectly as it helps manage business continuity. What is on the surge???		
Is the equipment tagged? (View a sample for tags)—		

ITEM	YES	NO
VIRUS SCANNING		
Does this location use virus scanning software on all computer systems? 9-10 products –there are some specifically geared to e-mail, some for network servers. Norton, Symatec, Network Associates,		
Does the virus scanning software automatically download and install new anti-virus software in a timely manner?		
Does this location scan files and email attachments for virus at the network perimeter (i.e. at the Internet firewall and other network access points)? Virus software that is configured for a server and manages it for a server---we recommend that you purchase an enterprise virus protection package.		
Does the virus policy at this location restrict users from downloading and installing unapproved software? Could be the way they install the e-mail customers – can they enforce –This is a network management issue—if I push it out from a server I can set it once for all that no e-mails can be received that have commonly known virus extensions. (These are known to be dangerous).		
Does your virus policy at this location restrict users from opening e-mail attachments from unknown sources?		
SERVER ROOM		
Is the server room on a top or bottom floor? Don't care—just has implications on safety—if it is in a basement—this could be dangers in flooding, lots of windows bad in storms.		
Does the server room have windows?		
If yes, are the windows: Plastic Shatterproof Bulletproof		
Is there a UPS system(s) to provide temporary power to servers and other critical workstations? If yes, indicate the average time provided by the UPS: (Uninterruptible Power Supply) Battery or back up generator 15 minutes 30 minutes 1 hour 4 hours 8 hours Indefinitely		
Is a backup generator system used?		
If yes, has the generator been inspected and approved in the last 3 months?		
Is there a documented schedule and logs for generator testing?		
Is there enough fuel on site for 3 days of operation?		
Does the UPS system perform automatic computer backup and shutdown? Some automatically have software that detects the power failure and starts to shut things down in a uniform manner- to ensure that data is saved and protected.		
Is there a water detection device that will turn off the system and notify a commercial alarm company?		
Is there a power failure detection device that will notify a commercial alarm company?		
Does the alarm company have a current priority list of names and telephone numbers to call to notify someone in case of a problem?		

ITEM	YES	NO
Are there posted procedures for shutting down any hardware that is not essential to the system operation? Something that is not essential is the e-mail server, a particular database server t		
Is there a cellular phone charged and ready?		
Is there a battery-operated radio available?		
Is there a posted procedure designating which computer system should be turned off when a warning sounds?		
Is there a posted procedure for storage of backup media when a warning sounds? Weather alert, beeping when power goes off, temp in server room goes so high.		
Do main server areas have fireproof access doors and nonflammable walls, ceiling and floors? Not required –just a best practice.		
If staff is present, does the extinguisher system turn on automatically after 30 seconds?		
If staff are not present, does the extinguisher system turn on automatically immediately?		
Is there a smoke detection device that will notify a commercial alarm company?		
Does the alarm company have a current priority list of names and telephone numbers to call to notify someone in case of a problem?		
Are computer operations located in a separate building? If they are what is the security for getting in and out of the building—if so not next to street--		
If yes, is this building located away from the perimeter? Car cannot run a red light and crash into the building—KPMG happened to be next to railway--		
Does the ground floor have windows?		
If yes, are the windows bullet-proof?		
Are entryway doors (to server room) constructed of strong fireproof steel with secure locks?		
Is a personal identification system used before staff access is allowed to the server room? If yes, indicate type: Key card Key pad Biometric device Key Sentry Double door gateway		
Does policy prohibit consumption of food and beverages outside of staff lounge(s) –in other words can staff eat or drink in the server room?		
DATA BACK UP		
Is there a documented data backup procedure located on site? Look at it—what does it say?		
If yes, does the procedure address: Media type: CD, tape, Media rotation schedule—daily weekly monthly—or if I use the tape more than once or three times do I discard? Most back up vendors publish these. Off-site storage Periodic testing Personnel responsibilities including backup staff Activity logs Server and local PCs schedules		
Is a fireproof safe(s) or file cabinet used for storing backed-up data and software?		
If yes, is the safe(s) in a different room than the server(s)?		
DATA CONTINUITY		
Is there a copy of the Agency Disaster/Business Continuity Plan on site?		

ITEM	YES	NO
Is staff familiar with roles and responsibilities under the Disaster/Business Continuity Plan? (Question random staff)		
Does this location maintain a list of business critical forms?		
Is there a store of business-critical forms for use in an emergency?		
Does this location maintain the following:		
Copies of critical reference manuals		
Contact information - personnel, hardware/software vendors, utilities, etc.?		
Copies of business critical procedures?		
Copies of procedures to process paper transactions (e.g., manual procedures) of business critical functions?		
A list of equipment required for processing business critical functions?		
A list of personnel required for supporting the business critical functions?		
A list of services required for supporting business critical processes - phone, electricity, mail, etc.?		
A list of all communications required for supporting business critical functions?		
The emergency notification process and responsibilities?		
A list of hardcopy and local backup strategies for business critical functions?		
A list of key vendor information (name, phone numbers, product and serial numbers) to support business critical functions?		
A list of necessary resources to support the recovery mode?		
Provisions for all human elements required to support the business critical functions - who, what, where, contact information?		
The necessary business function support team composition (functional and technical members) including skill set match, training and testing capabilities?		
Procedures and policies regarding the authorization to initiate contingency operations and resume normal operations?		
Policies and procedures for voice communications to support critical business functions especially as they pertain to Business Continuity Plans?		
Procedures and policies for returning to normal operations?		
Public relations and media interaction guidelines? Customer interface procedures been defined for the Emergency Mode Operations Plan?		
Has this location tested the Disaster Recovery/Business Continuity procedures?		

Comments:

ACKNOWLEDGMENT / RECEIPT

I have received a copy of the Easter Seals 2016 Compliance, Privacy & Security Policies and Procedures manual and have either read it or have had it read to me carefully. I understand all of its terms and conditions and agree to abide by them. I realize that failure to do so may result in disciplinary action or termination. I understand and agree that my employment may be terminated at-will, so that both Easter Seals and I remain free to choose to end our work relationship at any time. I also understand that Easter Seals remains free to change, revise, or eliminate any or all of the provisions stated in the manual,

including for reasons required by applicable law. I understand that nothing in this manual in any way creates an express or implied contract of employment between Easter Seals and me. I also understand that this manual is only intended to provide a better and more understandable working atmosphere and to ensure compliance with legal requirements, for so long as the employee/employer relationship exists.

_____ Date

_____ Employee's Signature

_____ *Employee's Printed Name*

_____ Date

_____ Representative's Signature