HIPAA Privacy and Security Policies and Procedures

Last Revised: July 11, 2022

Effective:
4/14/03

Former Amendments:
8/23/11; 7/1/15; 3/24/16; 4/18/19

Introduction

Imagine! is committed to protecting the privacy, security, confidentiality, integrity, and availability of Individually Identifiable Health Information (PHI) in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their associated regulations. All individuals representing Imagine! will take responsibility for safeguarding PHI to which they have access. Violation of provisions set forth in these policies and procedures may result in disciplinary action, which may include termination of employment.

Purpose

These Privacy and Security Policies are intended to comply with the requirements of the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), regulations under HIPAA, and any applicable State law that is more stringent than the HIPAA requirements. They are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA security, breach notification, and privacy regulations at 45 CFR Part 160 and Part 164.

These policies outline HIPAA rules and regulations with regard to the rights of persons applying for or receiving services, including their rights to notification and due process. The parent of a minor, acting on behalf of their child under the age of 18 years, as well as legal guardians and personal representatives are accorded the same rights if a court has awarded them the right to access or release the PHI of a person applying for or receiving services.

In the event of any conflict between a provision of these policies and more stringent State laws or requirements, the more stringent law or requirement shall control.

Enforcement

Any employee found to have violated these HIPAA policies and procedures may be subject to disciplinary action in accordance with applicable policies and procedures, up to and including termination of employment. Any vendor, subcontractor, or affiliate found to have violated these HIPAA policies and procedures may be subject to disciplinary action, up to and including termination of contract or affiliation.

Changes in Law

The Privacy Officer shall promptly change these HIPAA policies and procedures as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Privacy and Breach Notification Rules. The Security Officer shall promptly change security policies and procedures as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Security Rule, and to respond to environmental or operational changes. The changed policy or procedure shall be promptly documented and implemented. If the change materially affects the content of Imagine!'s Notice of Privacy Practices, the Privacy Officer shall promptly make the appropriate revisions to the Notice.

Note: These policies and procedures contain appropriate content as a result of the January 25, 2013 HIPAA/HITECH Act Final Omnibus Rule.

Questions Concerning HIPAA Compliance

If any member of Imagine!'s Workforce has a question concerning Imagine!'s privacy or breach notification policies, the HIPAA Privacy or Breach Notification Rules, or their application to any situation, he or she shall contact the Privacy Officer for guidance.

Either the Privacy Officer or the Security Officer may contact legal counsel for legal advice as he or she believes is necessary or desirable.

Disclaimer

It is the intention of Imagine! that these Privacy and Security Policies be used by its employees, and other members of its Workforce, in meeting their responsibilities to Imagine!. Violation of a policy can be the basis for discipline or termination of employment; however, because these Privacy and Security Policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy or procedure be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed by Imagine!, its employees, or its agents to another person.

Contents

Definitions – HIPAA Privacy and Security

These definitions are general definitions and not intended to provide complete or legal definitions of terms that are described in the HIPAA Privacy Rules or HITECH Act. In the event of a conflict, the definitions specified by HIPAA rules and regulations govern. Employees, subcontractors, interns, volunteers, providers or other persons affiliated with Imagine! shall consult with the Privacy or Security Officer if they have any questions.

Access: The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect Electronic PHI and to manage the conduct of the covered entity's Workforce in relation to the protection of that information. (Security)

Amend/Amendment: An amendment to PHI will always be in the form of information added to the existing PHI. This additional information may contain items that substantially change the initial PHI, make parts of the initial PHI more precise, or show some of the original PHI to be incorrect. However, the original PHI is never altered. Changes are indicated by the addition of the amended information.

Authentication: The corroboration that a person is the one claimed.

Authorization: A person served written statement of agreement to the use or disclosure of PHI to a third party.

Authorized Member of Imagine!'s Workforce: Means a member of Imagine!'s Workforce who has been authorized to take an action involved by: (a) his or her job description; (b) a protocol established by the Privacy Officer or Security Officer; or, (c) by the Privacy Officer or Security Officer.

Breach: The unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of PHI.

Business Associate: A person or organization that performs a function or an activity on behalf of Imagine! that involves the use or disclosure of PHI. A business associate might also be a person or entity that provides residential or day programs, community participation, therapy, support of persons served. Business associates may include persons or entities that provide legal, actuarial, accounting, billing, benefit management, claims processing or administration, utilization review, quality assurance, consulting, data aggregation, management, administrative, accreditation or financial services involving the use or disclosure of PHI.

Business Associate Agreement (BAA): A contract between a covered entity and a business associate, or between a business associate and its business associate subcontractor, that shall:

1. Establish the permitted and required uses and disclosures of PHI by the business associate.
2. Provide that the business associate shall use PHI only as permitted by the contract or as required by law, use appropriate safeguards, report any disclosures not permitted by the contract, make certain that agents to whom it provides PHI shall abide by the same restrictions and conditions, make PHI available to individuals and make its records available to U.S. Department of Health and Human Services (DHHS).
3. Authorize termination of the contract by the covered entity (or business associate if a business associate subcontractor is involved) if the covered entity (or business associate) determines that there has been a violation of the contract.
4. Meet the requirements for a Business Associate Agreements in all other respects pursuant to the HIPAA Privacy, Security, and Breach Notification Rules.

CMS: Centers for Medicare and Medicaid Services – The agency that regulates and enforces Federal Regulations for Medicare and Medicaid in Long Term Care and other healthcare entities.

Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

Consent: A document signed and dated by the individual or guardian/representative that a covered entity obtains prior to using or disclosing PHI to carry out treatment, payment or healthcare operations. Consent is not required under the privacy rule.

Court Order: An order issued from a competent court that requires a party to do or abstain from doing a specific act.

Covered Entity: A health plan, a healthcare clearinghouse, or a healthcare provider that is covered by the Privacy and Security Rules.

De-Identification: The process of converting Individually Identifiable Health Information into information that no longer reveals the identity of the person served.

De-identified Health Information: Health information that does not identify an individual and does not contain information that can identify or link the information to the individual to whom the information belongs.

Department Of Health And Human Services (DHHS): The US Department of Health and Human Services, of which the Office for Civil Rights is a part. This Federal agency is charged with the development, statement, implementation, and enforcement of the Privacy Rule.

Designated Record Set: A group of records maintained by or for Imagine! that is:

1. The case management records, medical records and billing records about persons served maintained by or for Imagine! or,

2. Used, in whole or in part, by or for Imagine! to make decisions about persons served. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for Imagine!.

Disaster Recovery Plan (DRP): The part of a Contingency Plan that documents the process to restore any loss of data and to recover computer systems if a disaster occurs (i.e., fire, vandalism, natural disaster or system failure). The document defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process to attain the stated disaster recovery goals.

Disclosure: The release, transfer, provision of access to or divulging in any other manner of PHI outside Imagine!. The two types of disclosure are:

1. ***Routine Disclosure:*** Customary disclosures of PHI that Imagine! discloses on a regular basis.
2. ***Non-Routine Disclosure:*** Disclosures of PHI that are not usually disclosed by Imagine!.

Electronic Media: Includes the following:

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

Electronic PHI (EPHI): Any PHI that is maintained or transmitted in an electronic media and may be accessed, transmitted or received electronically.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Financial Records: Admission, billing, and other financial information about a person served included as part of the designated record set.

Fundraising: An organized campaign by a private, nonprofit or charitable organization designed to reach out to certain segments of the population or certain identified populations in an effort to raise monies for their organization or for a specific project or purpose espoused by their organization.

Healthcare: 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.

Healthcare Operations: Any of the following activities of Imagine! to the extent that the activities are related to covered functions:

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 healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities;
3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and,
5. Business management and general administrative activities of Imagine!, including, but not limited to:
    a. Management activities relating to implementation of and compliance with the requirements of these policies and HIPAA Regulation;
    b. Person served service;
    c. Resolution of internal grievances;
    d. The sale, transfer, merger, or consolidation of or part of Imagine! with another covered entity, or an entity that following such activity shall become a covered entity and due diligence related to such activity; and,
    e. Consistent with the applicable requirements of the de-Identification of health information and creating de-identified health information or a limited data set, fundraising for the benefit of Imagine!, and marketing for which an individual Authorization is not required.

Healthcare Provider: An entity that provides healthcare, service or supplies related to the health of an individual, e.g., medical, dental, physical therapy, occupational therapy, speech therapy, behavioral health services or chiropractic clinics or hospitals.

Health Oversight Agency: An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory or an Indian tribe that is authorized by law to oversee the healthcare system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

HITECH Act: The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act is a Federal law that was designed to promote the adoption and meaningful use of health information technology and address the privacy and security concerns associated with the electronic transmission of health information. This definition is a general definition and is not intended to full describe the HITECH Act.

Individually Identifiable Health Information (IIHI): Any information, including demographic information, collected from an individual that:

1. Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and,
2. Relates to the past, present or future physical or mental health or condition of an individual; and,
    a. Identifies the individual; or,
    b. With respect to which there is reasonable basis to believe that the information can be used to identify the individual.

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

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

Limited Data Set (LDS): A data set that includes elements such as dates of application, termination, birth and death as well as geographic information such as the five digit zip code and the individual's state, county, city or precinct but still excludes the other 16 elements that "de-identify" information. In addition, this limited data set can only be used if a covered entity enters into a "data use agreement" with the data recipient similar to the agreements entered into between covered entities and their business associates.

Malicious Software: Software, for example, a virus, designed to damage or disrupt a system.

Marketing: 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. Face-to-face communications or those where only a gift of nominal value is provided are not considered marketing under the Privacy Rule. Marketing does not include the following:

1. Communications by a covered entity for the purpose of describing the entities participating in a healthcare provider network or healthcare 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.
2. Communications tailored to the circumstances of a particular individual if the communications are made by a healthcare provider to an individual as part of the treatment of the individual and for the purpose of furthering the treatment of that individual.
3. Communications by a healthcare provider or healthcare 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, healthcare providers or settings of care.

Master Record: The collection of documents, notes, forms, evaluations, assessments and other items which collectively document the services provided to an individual in any aspect of services delivered by Imagine! and the service provider network; individually identifiable data collected and used in documenting services rendered. The master record includes records of care used by case management while providing person served care services, for reviewing person served data, or documenting observations, actions or instructions. Imagine!'s master records includes documentation maintained in Imagine!'s electronic health record system, the electronically archived records stored in Imagine!'s Documents Management System as well as paper records, if applicable. Paper records are kept only for records that cannot be archived electronically (illegible scan or legal documents with seals) or for programs that have not yet fully transferred to Imagine!'s electronic Documents Management System. The master record consists of two parts:

1. The active record, which is defined as the designated record set and,
2. The administrative record, which is not part of the designated record set.

Minimum Necessary: The least amount of PHI needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of PHI it uses, discloses or requests to the minimum necessary to do the job.

Notice of Privacy Practices: A document required by HIPAA that provides the person served with information about their rights under the Privacy Rule and how Imagine! generally uses their PHI.

Office of Civil Rights: The Department of Health & Human Services' enforcement agency for the Privacy, Breach and Security Rules. OCR investigates complaints, enforces rights, and promulgates regulations, develops policy and provides technical assistance and public education to make certain understanding of and compliance with nondiscrimination and health information privacy laws including HIPAA. (www.hhs.gov/hipaa)

Opt Out: To make a choice to be excluded from services, procedures or practices. Person served rights under HIPAA include many situations where the person served may request to be excluded from a service, procedure or practice. In most cases, Imagine! shall comply or attempt to comply with the request to be excluded.

Password: Confidential authentication information composed of a string of characters.

Payment: The activities undertaken by a healthcare provider or payer to obtain reimbursement for the provision of care and services.

Person Served: Refers to persons applying, waiting for or receiving services from Imagine!.

Personal Representative: The term used in the Privacy Rule to indicate the person who has authority under law to act on behalf of a person served. For purposes of the Privacy Rule, Imagine! shall treat a personal representative as having the same rights as the person served unless there is a reasonable belief that the personal representative has subjected the person served to abuse or neglect, or treating the person as the personal representative could endanger the person served.

Physical Safeguards: Physical measures, policies and procedures to protect electronic information systems, equipment and their data and related buildings and equipment, from threats, natural and environmental hazards and unauthorized intrusion. They include restricting access to PHI, such as using locks and security cameras, retaining off-site computer backups, implementing and maintaining workstation security and data backup and storage.

Policy: A high-level overall plan embracing the general principles and aims of an organization.

Privacy Breach: A violation of one's responsibility to follow privacy policy and procedure that results in the PHI of a person served being accessed by unauthorized persons.

Privacy Officer: Imagine! employee who has been designated, pursuant to the Privacy Rule, with responsibility for ensuring Imagine!'s compliance with the Privacy Rule.

Privacy Rule: Refers to the regulation issued by the Department of Health and Human Services entitled Standards for Privacy of Individually Identifiable Health Information. The effective date for the Privacy Rule was April 14, 2001. Can be referenced as 45 CFR Part 160 and 45 CFR Part 164 and is amended from time to time. This definition is a general definition and is not intended to full describe the Privacy Rule.

Protected Health Information (PHI): Any health information maintained by Imagine! that is Individually Identifiable Health Information except (a) employment records held by Imagine! in its role as an employer; and (b) information regarding a person who has been deceased for more than fifty (50) years. PHI means any health information, including demographic information,

whether oral or recorded in any form or medium, including demographic information collected from an individual, that:

1. Is created or received by a health-care provider, health plan, employer 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 healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and,
    a. That identifies the individual; or,
    b. There is a reasonable basis to believe the information can be used to identify the individual.

All health information maintained by Imagine! is Individually Identifiable Health Information unless and until it is subject to De-Identification.

Psychotherapy Notes: Notes that are recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. Psychotherapy notes shall be kept separate from the rest of the master record of the person served. 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.

Qualified Protective Order: A legal command intended to protect a person or thing from an unfair or unjust action.

Order: A mandate, precept; a command or direction authoritatively given; a rule or regulation.

Re-Identification: The process of converting de-identified health information back to Individually Identifiable Health Information. Re-identified health information does reveal the identity of the person served and shall be treated as PHI under the Privacy Rule.

Research: A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalized knowledge.

Revoke: To cancel or withdraw an Authorization to release PHI.

Risk Analysis: The process of identifying, prioritizing and estimating an organization's exposure to risk arising from the operation of its information technology system to identify threats and vulnerability. Once identified, the risks can be mitigated by security controls (planned or already in place). Security risks can impact, among other things, the organization's operations and organizational assets (PHI), the agency's staff and persons served and third party entities doing business with the organization. Also known as a security assessment.

Risk Management: Management's identification, analyses and, when necessary, response to risks that might adversely affect realization of Imagine!'s business objectives in its capacity as a business associate of its clients.

Safeguarding: To make certain safekeeping of PHI for the person served.

Screen Saver: Any software program designed to, after a certain period of inactivity, display on a workstation monitor a random display of patterns, images, or to simply make the monitor blank so as to prevent an image from being burnt into the monitor.

Security or Security Measures: The administrative, physical and technical safeguards in an information system.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Security Officer: A position mandated by HIPAA Regulation. The responsibilities of this person are to oversee implementation of the requirements mandated by the Final Security regulation and any security requirements included in the other sections of the HIPAA regulation.

Security Rule: The Federal privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that created national standards to protect electronic medical records. (42 U.S.C. § 1320d, 45 C.F.R. parts 160 and 164, as amended)

Subcontractor: A person or entity who acts on behalf of Imagine!.

Subpoena: A process to cause a witness to appear and give testimony, commanding him/her to lay aside pretenses and excuses and appear before a court or magistrate therein named at a time therein mentioned to testify for the party named under a penalty thereof. There are two (2) kinds of subpoenas:

1. *Duces tecum:* A request for witnesses to appear and bring specified documents and other tangible items. The subpoena duces tecum requires the individual to appear in court with the requested documents, or simply turn over those documents to the court or to counsel requesting the documents.
2. *General subpoena (a.k.a. ad testificandum):* A command to appear in court at a certain time and place to give testimony regarding a certain matter, for example, to testify that the record was kept in the normal course of business.

Technical Safeguards: The technology and the policy and procedures for its use that protect electronic PHI and control access to it.

Treatment: The provision, coordination or management of healthcare and related services by Imagine!, including the coordination or management of services by Imagine! with a third party;

consultation with other providers relating to a person served; or the referral of a person served for services between Imagine! and another authorized care provider.

Treatment, Payment and Operations (TPO): The Privacy Rule allows sharing of information without the need for consent for purposes of treatment, payment and healthcare operations. Treatment includes use of person served information for providing continuing services. Payment includes sharing of information in order to bill for provision of services to the person served. Healthcare operations are certain administrative, financial, legal, and quality improvement activities that are necessary for Imagine! to run its business and to support the core functions of treatment and payment.

Use: With respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination or analysis of that information within Imagine!. (See also Disclosure)

User: A person or entity with authorized access to PHI.

Whistleblower: A person, usually an employee, who reveals wrongdoing within an organization to the public, government agencies or to those in positions of authority.

Workforce: Staff, volunteers, subcontractors, interns, and other persons whose conduct, in the performance of work for Imagine!, is under the direct control of Imagine!, whether or not they are paid. Members of the Workforce are not business associates. References in these Policies to Workforce members refers to Imagine!'s employees, subcontractors, interns and volunteers.

Designation of Privacy Officer and Security Officer

Designation of Privacy Officer

Imagine!'s Chief Executive Officer shall designate a Privacy Officer who shall be responsible for the development, updating and implementation of Imagine!'s privacy policies. The Privacy Officer may be the same individual who is designated as the Security Officer of Imagine!.

The Privacy Officer of Imagine! shall:

1. Oversee the development, implementation, maintenance, and revision of policies and procedures to protect confidential health information in accordance with Federal and State regulations. The Privacy Officer notifies the Executive Team of any policies, procedures, or implementation issues that need their review;
2. Perform periodic Privacy Rule focused risk assessments to identify issues that need attention;
3. Develop staff training on HIPAA policies, procedures, and practices;
4. Monitor and ensure that all Imagine! Workforce members receive HIPAA training;
5. Maintain an updated Notice of Privacy Practices that is distributed in accordance with these procedures;
6. Manage disclosures of information;
7. Responsible for any Breach Notification Rule requirements;
8. Respond to Requests for Amendments of PHI;
9. Investigate and respond to complaints regarding the confidentiality of information;
10. Provide additional information about matters covered by the Notice of Privacy Practices;
11. Update privacy forms and coordinate the placement of these forms throughout Imagine!.

Designation of Security Officer

Imagine!'s Chief Executive Officer shall designate a Security officer who shall be responsible for the development, updating and implementation of Imagine!'s security policies. The Security Officer may be the same individual who is designated as the Privacy Officer of Imagine!.

The Security Officer of Imagine! shall:

1. Oversee the development, implementation, maintenance, and revision of policies and procedures to protect confidential information in accordance with Federal and State regulations;
2. Assist with the development of staff training on HIPAA policies, procedures, and practices;
3. Oversee procedures designed to prevent, detect, contain, and correct security violations;
4. Maintain written or electronic copies of documentation related to communications, actions, activities, security measures or designations required by these policies and procedures or the Security Rule for a period of six (6) years from the date of its creation or the date when it last was in effect, whichever is later;
5. Develop a risk management plan that contains measures for:
    a. Conducting an accurate and thorough risk assessment of the potential risks and

vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by Imagine!;

b. Reducing the exposure to identified risks, including use of firewalls, anti-virus software, updated or new policies and procedures, or additional or advanced training;
c. Implement security measures sufficient to reduce the risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level; and,
d. If appropriate, the risk management plan shall be revised and improved based on results of periodic risk assessments.

Documentation of Privacy and Security Officers

Imagine!'s Chief Executive Officer shall maintain, or cause to be maintained, a written or electronic record of the designation of the Privacy Officer and of the Security Officer. Such record shall be maintained for six (6) years from the date of its creation or the date it is last in effect, whichever is later.

Training of Workforce

Imagine! provides HIPAA privacy and security training to Imagine! Workforce members who will come into contact with PHI while performing their job functions.

The Privacy and Security Officer, in concert with Human Resources staff, will establish separate privacy and security training courses.

All members of Imagine!'s Workforce shall be trained annually on Imagine!'s privacy and breach notification policies and procedures with respect to PHI as necessary and appropriate for the members of the Workforce to carry out their functions within Imagine!. Additional training will also occur in response to any risk assessment identifying the need for additional training.

Imagine! employees, subcontractors, interns, and volunteers shall be trained:

- Within thirty (30) days of employment at Imagine!;
- Within thirty (30) days after a material change in privacy policies becomes effective when their job duties are affected by the change;
- Within thirty (30) days of the Privacy or Security Officer determining they have disregarded privacy laws, policies or procedures.

The Privacy Officer, Security Officer, or their designee, will ensure the documentation of each training session and the names of Imagine! employees who completed the training. The supervisors of interns and volunteers will document their HIPAA training when it occurs. Documentation of the training for each member of the Workforce shall be kept in written or electronic form for six (6) years after the date of its creation or the date that person ceases to be a member of Imagine!'s Workforce, whichever is later.

In the event of a material change in Imagine! Privacy or Security policies or procedures, or in the HIPAA Privacy or Security Regulations, the Privacy and Security Officer shall work with Human Resources to retrain staff, interns and volunteers who would be affected by those changes. The additional training shall occur within thirty (30) days from the effective date of the new policies or regulations. The same requirements for enforcement and documentation of completion, as indicated above, shall apply.

Discipline for Non-Compliance of HIPAA Training

Human Resources shall implement the same procedures to discipline and hold Imagine! staff, interns, or volunteers accountable for completing HIPAA training, as with other trainings conditional for employment.

Training to Recognize and Respond to a Breach of Unsecured PHI

Imagine! employees, subcontractors, interns, and volunteers shall be trained to recognize and respond to a breach of unsecured PHI and to understand the consequences of a security breach. If an Imagine! employee, subcontractor, intern, or volunteer is involved in a privacy or security incident that was not the result of malicious or willful conduct, the Privacy or Security Officer (or

their designees) shall provide the offending individual with additional training regarding Imagine!'s privacy and security policies and procedures. The training shall focus on the areas directly related to the incident and shall be designated to prevent a recurrence of the incident.

In the event of a privacy or security incident, the Privacy or Security Officer may issue a training reminder to the Workforce member that focuses on the privacy and/or security issue involved in the incident, and how to avoid it in the future.

In order to safeguard ongoing privacy compliance and information security, the Privacy or Security Officer (or their designees) may provide periodic privacy or security reminders to Imagine! Workforce members. These reminders shall be provided on an as needed basis via presentations at staff meetings or through email and shall focus on practical privacy or security issues, such as handling passwords, dealing with email attachments, releasing information, etc.

Notice of Privacy Practices

Imagine! provides the Notice of Privacy Practices to persons applying for services, their parent (if a minor), legal guardian and personal representative at the time an application for services is being made. Persons served, their parent (if a minor), legal guardian and personal representative are also notified when the Notice of Privacy Practices changes. Imagine! requests that each person receiving a copy of the Notice of Privacy Practices at the time of application acknowledges their receipt of the Notice in writing.

The Notice of Privacy Practices shall comply with HIPAA rules and regulations. The Notice of Privacy Practices communicates:

1. The uses and disclosures of PHI that may be made by Imagine!;
2. The rights of a person with respect to his/her PHI; and,
3. Imagine! duties in safeguarding such PHI.

The Notice shall be written in plain language and shall be made available in languages understood by a substantial number of individuals served by Imagine!. Imagine! shall make certain the Notice in Spanish translation is available.

Imagine! staff shall provide a copy of the written Notice of Privacy Practices to persons served and to other persons upon request.

If the individual agrees, the Notice of Privacy Practices may be provided to that individual by e-mail in lieu of physical delivery.

The Privacy Officer shall post a copy of the Notice of Privacy Practices in clear and prominent location such as the entrance lobby at Imagine!'s various offices and facilities. A current version of the Imagine! Notice of Privacy Practices shall be maintained on its website.

Acknowledgement of Receipt of Notice of Privacy Practices

Imagine! intake staff shall provide the Notice of Privacy Practices to the person applying for services at the time of application. At the time the Notice of Privacy Practices is provided, Imagine! intake staff shall make a good faith effort to obtain the signature of the person applying for services, the parent of a minor, legal guardian or personal representative on the Acknowledgement of Receipt of Notice of Privacy Practices Form. The signed Acknowledgement of Receipt form shall be included in the individual's master record.

If the individual's acknowledgment cannot be obtained, the Imagine! staff member(s) who attempted to obtain it shall document their good faith efforts to obtain the acknowledgment and the reason why it was not obtained by completing the Documentation of Good Faith Effort to Obtain Written Acknowledgement of Receipt of Notice of Privacy Practices form. This document will be included in the individual's master record.

Revision of Notice of Privacy Practices

Whenever there is a material change to the uses or discloses, the individual's rights, Imagine!'s legal duties, or other privacy practices stated in the notice, the Privacy Officer will promptly revise the Notice of Privacy Practices. The revised Notice shall be made available on request and distributed.

Except when the material change is required by law, a material change to any term of the Notice of Privacy Practices shall not be implemented prior to the effective date of the Notice of Privacy Practices in which the material change is reflected.

A copy of each Notice of Privacy Practices used by Imagine! and of each written acknowledgment of receipt of the notice or documentation of good faith efforts to obtain such acknowledgment shall be maintained by Imagine! in written or electronic form for six (6) years after the date the notice was last in effect.

Changes to Privacy Practices Stated in Notice of Privacy Practices

When Imagine! changes a privacy practice that is stated in its Notice of Privacy Practices and makes corresponding changes to its policies, the following actions shall be taken:

1. The Privacy Officer shall ensure that these policies or procedures, as revised to reflect the change, complies with the HIPAA Privacy and Breach Notification Rules;

2. The Privacy Officer shall maintain a copy of each revised HIPAA policies and procedures and Notice of Privacy Practices for at least six (6) years from the date it was last in effect;

3. The Privacy Officer shall revise The Notice of Privacy Practices to state the changed practice and make the revised notice available. The changed practice may not be implemented prior to the effective date of the revised Notice of Privacy Practices except when required by law.

The change shall be effective only with respect to PHI created or received after the effective date of the revised Notice of Privacy Practices.

Changes to Privacy Practices Not Stated in Notice of Privacy Practices

Imagine! may change, at any time, a privacy practice that does not materially affect the content of its Notice of Privacy Practices, provided:

1. The policy or procedure involved, as revised, complies with the HIPAA Privacy and Breach Notification Rules; and,
2. Prior to the effective date of the change, the policy or practice, as revised, is documented by the Privacy Officer in written or electronic form for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

Designated Record Set

Confidential information and records, whether they are in paper or electronic format, that are used for the purpose of making decisions about a person served are considered part of the designated record set.

If records from other providers are used by Imagine! to make decisions related to the care and treatment of the person served, then these records are considered part of the designated record set for access by the Workforce member (if within the scope of their job duties). These records may include, but are not limited to, such documents as history and physical examination forms, discharge summaries and lab results from previous acute care hospitalizations, medical and billing records, payment, claims adjudication records, and any information used, in whole or in part, by or for Imagine! to make decisions about persons served. The designated record set will include electronic or paper-based records that meets this term's definition.

The designated record set is to be retained according to State and Federal regulations and following Imagine!'s Records Retention policy and procedures.

Program specific records, which may include active and historical designated records set documentation, are generally maintained by the programs in their administrative locations. Maintenance of privacy and security of these records is coordinated with the Privacy Officer and Security Officer.

Administrative records, which include investigative records, are not part of the Designated Record Set.

Minimum Necessary Use and Disclosures of PHI

When using or disclosing PHI, members of Imagine! Workforce shall make reasonable efforts to limit the amount of PHI used or disclosed to the minimum necessary. The following standards (the "Minimum Necessary Standard") apply to the use and disclosure of PHI:

1. Imagine! Workforce members shall only have access to the amount and type of PHI necessary to carry out their job duties, functions and responsibilities.
2. Imagine! limits access to, and use of, the PHI of persons served in accordance with its business associate agreements with vendors and subcontractors.
3. Imagine! Workforce members shall restrict their use, access and disclosure of PHI to the minimum necessary to achieve the purpose of the disclosure.

This Minimum Necessary Standard does not apply in the following situations:

1. When the PHI is for use by, or a disclosure to, a healthcare provider for purposes of providing treatment to the patient;
2. When the disclosure is to the person served, their parent (if a minor), legal guardian or legally authorized personal representative;
3. When the disclosure is pursuant to a valid Authorization requested through the person served or their parent (if a minor), legal guardian or legally authorized personal representative, in which case the disclosure shall be limited to the PHI specified in the Authorization;
4. When the disclosure is to the Secretary of the U.S. Department of Health and Human Services (Federal government);
5. When the law requires the disclosure; only PHI required to be disclosed by law shall be disclosed.

Minimum Necessary Standard When Requesting PHI

When requesting PHI from another entity, Imagine! shall limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are not on a routine or recurring basis, Imagine! shall evaluate the request to determine if the requirements of the Privacy Rule have been satisfied.

Safeguarding Verbal and Written PHI

All Imagine! employees, subcontractors, Business Associates, interns and volunteers are responsible for the privacy and security of PHI of persons receiving services. The Privacy Officer and Security Officer shall implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. They are responsible for periodically monitoring to ensure that uses and disclosure of PHI complies with applicable Federal, State and/or local law or regulation, and these policies and procedures.

Procedures for Safeguarding Verbal Use of PHI

Reasonable measures shall be taken so that unauthorized persons do not overhear conversations involving PHI. During face to face conversations, such measures may include:

1. Conducting meetings in a room with a door that closes, if possible;
2. Keeping voices to a moderate level;
3. At a meeting, having only staff and others involved in the care of the person served who have a "need to know";
4. Limiting the PHI discussed to the minimum amount necessary to accomplish the task of the meeting;
5. If in a public area, moving to a private or semi-private area within Imagine! and lowering the voice to minimize likelihood of inadvertent disclosure.

During telephone conversations where PHI is discussed, such measures may include:

1. Lowering the voice;
2. Requesting that unauthorized persons step away from the area, if possible;
3. Using a phone in a private area, or moving to a telephone in a more private area before continuing the conversation; and,
4. Limiting the PHI discussed to the minimum amount necessary to accomplish the purpose of the conversation.

Procedures for Safeguarding and Storing Written PHI

Hardcopy master records will be filed in a systematic manner in a Records area that safeguards the privacy and security of the information. The Business Systems Program Manager, or a designee, will monitor storage and security of such hardcopy master records.

Authorized staff shall review the hardcopy master record at a workstation within the secure Records area unless it is signed out. If removed from the Records area, the hardcopy master record will be signed out. Only authorized persons are allowed to sign out hardcopy master records. Hardcopy master records may not leave the building without the express approval of the Privacy Officer or her designee.

Hardcopy master records shall be returned to the Records area at the end of each work day. Exceptions may be made if there is a valid need to keep the record for a longer period of time.

Hardcopy master records shall not be left unattended in areas where unauthorized individuals could easily view the records.

Hardcopy "working" file contents shall be limited only to the essential information necessary for the Imagine! employee to complete their duties as assigned. When not in use, working files will be kept in a locked drawer at the employee's workstation.

Documents containing PHI shall not be easily accessible to visitors or unauthorized staff and shall be stored appropriately to reduce the potential for incidental use or disclosure.

Working documents containing PHI left on a workstation shall be turned face down or otherwise concealed from easy view before leaving work so that PHI is not readily observed by unauthorized individuals.

All trash that contains PHI must be placed in the designated, locked containers for shredding.

In the event that the confidentiality or security of a master record has been breached, the Privacy Officer shall be notified immediately.

Please see *Procedures for Transportation and Storage of PHI* for transporting and storing written PHI in that section of these policies and procedures.

Procedures for Safeguarding PHI when Using Printers, Copiers, or Scanners

A. Printers, copiers and scanners are located in areas not easily accessible to unauthorized persons.

B. Authorized Workforce members may view documents generated on printers, copiers or scanners. Access to such documents by unauthorized persons is prohibited by Federal law.

C. Documents containing PHI shall be promptly removed from the printer and/or copier/scanners and placed in an appropriate and secure location.

D. Periodically, designated administrative support staff will check printer/copier stations for unclaimed documents containing PHI and place them in a locked container to await shredding.

E. Documents containing PHI that shall be disposed of due to error in printing shall be destroyed by shredding or by placing the document in a locked container to await shredding.

Procedures for Transmitting PHI through Email or Fax

Imagine! staff, interns, subcontractors, and volunteers may communicate PHI via email or facsimile (fax) to persons served, their parent (if a minor), legal guardian, personal representatives or providers of service. Care shall be taken that the PHI transmitted in these instances is safeguarded from inappropriate use, disclosure or access.

Transmitting PHI through Email

A. Email users shall be set up with a unique identity complete with unique password and file access controls per Imagine!'s Procedure for Assigning Unique Identifier.
B. Email users may not intercept, disclose or assist in intercepting and disclosing email communications.
C. Whether the email is to Imagine! employees, subcontractors, interns or volunteers, or to persons external to Imagine!, the amount of PHI disclosed via email correspondence shall be limited to the minimum necessary to accurately communicate the needs or situation of the person served.
D. EPHI may be sent via email within Imagine!'s secured, internal network.
E. When sending EPHI outside of the Imagine! network, such as over the Internet, every effort shall be made to secure the confidentiality and privacy of the information.
    1. Imagine! email that contains EPHI that is sent or forwarded to an external email address shall be encrypted unless the conditions of number 4 below, are met.
    2. Users shall exercise extreme caution when forwarding messages. Sensitive information, including EPHI, shall not be forwarded to any party outside the agency without using the same security safeguards as specified above.
    3. Users shall verify the accuracy of the email address before sending any external email containing EPHI.
    4. Emails containing EPHI may only be sent unencrypted to a person served, or their guardian or personal representative, if the recipient requests to receiving PHI by unencrypted email by signing the "Request for Non Secure Communications form". This form must warn of the risks of unsecure email.
    5. Unencrypted email messages are not considered secure and private.
F. Employees, subcontractors, interns and volunteers shall immediately report any violations of this policy to their supervisor.
G. All external email containing EPHI shall automatically display a confidentiality statement.

Transmitting PHI through Fax

A. Received documents shall promptly be removed from the fax machine and, if necessary, forwarded to the appropriate recipient. To promote secure delivery, instructions on the cover page shall be followed.
B. Unless otherwise prohibited by State law, information transmitted via facsimile is acceptable as an original copy and may be included in the master record of the person served.

C. When sending a facsimile document that includes PHI, the PHI disclosed shall be the minimum necessary to meet the requestor's needs and/or communicate information about the needs or situation of a person served.
    1. Highly sensitive health information shall not be sent by fax (e.g., information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).
D. When sending a facsimile document that includes PHI, steps shall be taken to confirm that the fax transmission is sent to the appropriate destination. These include:
    1. Pre-programming and testing destination numbers to eliminate errors in transmission due to misdialing.
    2. Asking frequent recipients to notify Imagine! of a fax number change.
    3. Confirming the accuracy of the recipient's fax number before pressing the submit function.
E. When transmitting information, a cover page shall be attached to any facsimile document that includes PHI. The cover page shall include:
    1. Destination of the fax, including name, fax number and phone number;
    2. Name, fax number and phone number of the sender;
    3. Date;
    4. Number of pages transmitted; and,
    5. Confidentiality Statement
F. If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system shall be checked to obtain incorrect recipient's fax number. Fax a letter to the receiver and ask that the material be returned or destroyed. Notify the Imagine! Privacy Officer of misdirected fax.

Approval to Release PHI and Disclosure of PHI

When PHI is to be used or disclosed for purposes not covered by an established protocol in these policies and procedures, or for purposes other than the continuing care of persons receiving services (treatment), payment of services, or the coordination of day to day Imagine! operations (health care operations), Imagine! shall disclose PHI only as authorized by the Privacy Officer or his/her designee. In some instances, the Privacy Officer may need to track information that is disclosed.

Exceptions to Authorization Requirements

PHI may be disclosed by the Privacy Officer or his/her designee without an Authorization, pursuant to applicable policies herein, if the disclosure is:

1. For Imagine! treatment or continuation of services; payment activities, or the payment activities of the entity receiving the PHI; and, operations;
2. In limited circumstances, for the healthcare operations of another Covered Entity, if the other Covered Entity has or had a relationship with the person served;
3. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the Privacy Rule;
4. As required by other State or Federal law and as permitted under HIPAA rules and regulations;
5. An administrative request, subpoena or investigative demand. Imagine! may disclose the requested PHI if the administrative document itself or a separate written statement recites:
    a. The information sought is relevant to a lawful inquiry;
    b. The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry; and,
    c. De-identified information could not be used.
6. A request by a Public Officer, if the officer presents:
    a. A badge or other credential, such as a written statement of the authority under which the information is requested, for example, a copy of the law or regulation. If obtaining a written statement is impractical, an oral statement is sufficient; or,
    b. A request on government letterhead.
    c. If the person making the request is acting on behalf of a Public Officer, a written statement on government letterhead that the person is acting on behalf of a Public Officer. If other authority is presented, contact legal counsel for guidance before disclosure.
7. If PHI is disclosed to:
    a. Prevent or lessen a serious and imminent threat to the health or safety of a person or the public; or,
    b. Law enforcement authorities to identify or apprehend an individual.

PHI shall also not be used or disclosed in the absence of a valid written Authorization if the use or disclosure is:

    c. Of psychotherapy notes as defined by the Privacy Rule; or,
    d. For the purpose of marketing; or,

e. For the purpose of fundraising.

Uses and Disclosures to Carry Out Treatment, Payment, and Health Care Operations

Imagine! may use or disclose PHI, without an Authorization, as follows:

1. To the individual;
2. For its own treatment, payment, or health care operations;
3. For treatment activities of a health care provider;
4. To another entity covered by the Privacy Rule or a health care provider for the payment activities of the entity that receives the information;
5. To another entity covered by the Privacy Rule for health care operations of the entity that receives the information, if Imagine! and that other entity has or have had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to that relationship, and the disclosure is:
    a. For 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; patient safety activities (as defined in 42 CFR 3.20); 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.
    b. 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.
    c. For the purpose of health care fraud and abuse detection or compliance.
    d. To other participants in Imagine!'s Organized Health Care Delivery System (OHCDS) for any health care operations of that OHCDS.

Procedures for Disclosure Pursuant to an Authorization

Designated employees receive targeted training in reviewing and processing Authorizations and only these employees shall handle such requests on behalf of Imagine!. Other Imagine! staff members may not release PHI without the approval of the Privacy Officer, except in case of emergency (e.g. the person served faces risk of severe negative outcome if information is not shared immediately), or as a result of a specifically approved program area function.

When a written Authorization is required prior to disclosing PHI, members of Imagine!'s Workforce shall not disclose the PHI until a valid, written Authorization is received from the person served, their parent (if a minor), legal guardian, or personal representative.

If the request for disclosure is not accompanied by a written Authorization, the employee primarily serving the individual shall notify the requestor that Imagine! is unable to provide the

PHI requested. The requestor shall be supplied with a valid Authorization to Use or Disclose PHI form.

Imagine! employees shall make reasonable attempts to verify the identity and the authority of a person/entity making a request for the disclosure of PHI, if the identity or authority of such person is not known. Further, Imagine! employees shall request from the person/entity seeking disclosure of PHI such documentation, statement or representation, as may be required by the Privacy Rule, prior to a disclosure. Imagine! staff may rely on documentation, statements or representations that, on their face, meet the verification requirements, if the reliance is reasonable under the circumstances. If there are concerns as to the requirements, the Privacy Officer shall contact Imagine! legal counsel.

If the request for disclosure is accompanied by a written Authorization, the designated Imagine! employee shall review the Authorization to assure that it is valid.

If an Imagine! employee suspects an Authorization is invalid, the employee shall notify the Imagine! Privacy Officer. The Imagine! Privacy Officer will notify the requestor, in writing, of the deficiencies in the Authorization. No PHI shall be disclosed unless and until a valid Authorization is received.

If a person served needs interpretation or assistance in understanding the Authorization, they shall notify Imagine! staff for assistance.

Valid Authorizations shall be delivered to designated employees to process the disclosure of the requested PHI and then document the Authorization in the master record of the individual receiving services.

Requirements for Valid Authorization to Release PHI

An Authorization to Release PHI must be written in plain language and is valid when it contains all of the following elements:

1. A description of the specific information to be used or disclosed;
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom Imagine! may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the Authorization and does not, or elects not to, provide a statement of the purpose;
5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
6. A statement of the individual’s right to revoke the Authorization in writing;
7. A statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the Authorization by stating either:

   a. That the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the Authorization when the prohibition on conditioning of Authorizations applies; or,
   b. The consequences to the individual of a refusal to sign the Authorization when the Privacy Rule permits the entity to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain the Authorization.
8. A statement that information used or disclosed pursuant to the Authorization may be subject to redisclosure by the recipient and no longer be protected by the Privacy Rule;
9. Signature of the individual and date or if the Authorization is signed by a personal representative of the individual, a description of that personal representative's authority to act for the individual.

Defective Authorization for Release of PHI

An Authorization is defective if the document has any of the following defects:

1. The expiration date has passed;
2. The Authorization has not been filled out completely with respect to an element required to be included in the Authorization or the Authorization is missing a required element;
3. The Authorization is known by Imagine! to have been revoked;
4. If any material information in the Authorization is known by Imagine! to be false.

If any member of Imagine!'s Workforce believes an Authorization is defective for any reason, he or she shall promptly report that fact and the basis for his or her belief to the Privacy Officer.

Revocation of Authorization

The person served may revoke his/her Authorization at any time. The Authorization may be revoked verbally or in writing. If the person served, parent of a minor, legal guardian or personal representative informs Imagine! staff that he/she wants to revoke the Authorization, Imagine! employees, subcontractors, interns or volunteers shall obtain a copy of the original Authorization (hardcopy or printed electronic) and complete the designated area at the bottom of the form:

NOTE: This Authorization was revoked on (DATE)_____ Signature of Staff_____

Upon receipt of a written revocation, Imagine! may no longer use or disclose the PHI of the person served, pursuant to the Authorization.

Each printed or electronic revocation formally completed shall be filed in the master record.

The Privacy Officer will track and maintain a log of these requests.

Incidental Uses and Disclosures

A use or disclosure that is incidental to a use or disclosure that is otherwise permitted or required by these Privacy and Security Policies or the HIPAA Privacy Rule is permissible provided:

1. The applicable Minimum Necessary Standards are met;

2. Reasonable safeguards have been applied to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Requests for Master Record Copy or Portions of the Designated Record Set

With a few very limited exceptions, persons served or their personal representatives have the right to inspect and obtain a copy of their complete record in their designated record set (see *Designated Record Set* in these policies and procedures for definitions). Persons served who want to inspect their records or request a complete copy of their records must submit their request in writing to Imagine!'s Privacy Officer. Persons served or their personal representatives do not have the right to access PHI that is not part of a designated record set because the information is not used to make decisions about individuals.

The request shall state specifically what personal health information the individual in services, their parent (if a minor), legal guardian or personal representative wishes to inspect or receive a copy of. The request shall state the form of access and copy desired, such as in hardcopy or electronic format.

Upon receipt of a request for a copy of a complete record, the Privacy Officer will review the contents of the record prior to releasing the copy to the requestor. The Privacy Officer will remove any components of the copy that Imagine! is authorized to restrict access to.

Under certain limited circumstances, Imagine! may deny a person's request for access to all or a portion of the PHI requested. In some of these circumstances, a person has the right to have a denial reviewed by a licensed health professional.

Unreviewable grounds for denial include:

1. Psychotherapy notes;
2. Information compiled in anticipation of, or use in, a civil, criminal or administrative action or proceeding;
3. If such information is protected by more stringent disclosure statues such as alcohol or substance abuse information or HIV status and HIPAA Rules and Regulations do not require disclosure or are preempted;
4. Information gathered in the process of an investigation as requited by rule and statute, in response to allegations of mistreatment, abuse, neglect, and exploitation, and other incidents defined as critical by regulatory agencies.
5. The requested PHI was obtained by someone other than Imagine! (e.g. a family member of the person served) under a promise a confidentiality and providing access to the information would be reasonably likely to reveal the source of the information.
6. An inmate requests a copy of their PHI held by a correctional institution and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate, or other inmates, or the safety of correctional officers, employees, or other persons at the institution or responsible for transporting the inmate. However, in these cases, an inmate retains the right to inspect their PHI.

Reviewable grounds for denial include (as determined by a licensed health care professional in the exercise of professional judgment):

1. The access is reasonably likely to endanger the life or physical safety of the person served or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g. concerns that the individual will not be able to understand the information or may be upset by it).
2. The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
3. The access to a personal representative of the person served that requests such access is reasonably likely to cause substantial harm to the person served or another person.

See *Procedures for Denying Access to PHI by Persons Receiving Services* in these policies and procedures.

The Imagine! Privacy Officer will fulfill record copy requests within thirty (30) calendar days after receiving the request. If the request is granted, in whole or in part, the Privacy Officer will inform the requestor of the acceptance of their request and provide access and copies.

If a request is denied, the Privacy Officer will inform the requestor of the basis for the denial, how they may have the denial reviewed, and how the requestor may appeal.

Imagine! will provide one copy of the requested information at no charge. Additional copies will be provided at a reasonable fee per copied page, plus mailing costs, if it is requested that the information be mailed.

Responding to Specific Types of Disclosures

Media: No PHI shall be released to the news media or commercial organizations without the written Authorization of the person served or his/her personal representative. In the event of a communications emergency, refer to Imagine!'s *Communicating with the Media during a Crisis* plan.

Telephone Requests: Staff receiving requests for PHI via the telephone shall make reasonable efforts to identify and verify that the requesting party is entitled to receive such information (for example, calling the professional contact information of the person requesting information to verify their official capacity).

Disclosures to Individuals Involved in the Care of A Person Served

Imagine! may disclose PHI to a family member, other relative, close friend, or any other individual identified by the person served without a written Authorization:

1. That is directly relevant to that individual's involvement in the care, or payment for care, of the person served; or,

2. To notify such individual of the location, general condition or death of a person served, and
3. In the case of an un-emancipated minor fifteen years of age or older who consents to treatment, with or without the consent of a parent or legal guardian, Imagine!, with or without the consent of the minor, may advise the parent or legal guardian of that minor of the services given or needed.

If the disclosure is sought by individuals involved in the care of a person served and it is relevant to the requesting party's involvement in the care, Imagine! may rely on reasonable professional judgment in verifying the identity and authority of the individual seeking disclosure.

Imagine! staff, interns, and volunteers shall take reasonable steps to confirm the identify of a family member or friend of the person served. Imagine! is permitted to rely on the circumstances as confirmation of involvement in care. For example, the fact that a person lives at home with family is sufficient confirmation of the family's involvement in the care of the person served.

Prior to a permitted disclosure, if the person served is present for, or otherwise available, then Imagine! staff, interns and volunteers may use or disclose PHI if they:

1. Obtain the agreement of the person served;
2. Provide the person served with an opportunity to object to the disclosure, and the person served does not express an objection (the opportunity to object and the response may be done orally); or,
3. Based on the exercise of professional judgment, reasonably infer from the circumstances that the person served does not object to the disclosure.

If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, a member of Imagine!'s Workforce may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or needed for notification purposes.

Imagine! staff will document the incapacity reason or emergency circumstance of the person served and why there was a determination that the disclosure was in that person's best interest.

Disclosures for Disaster Relief

Imagine! may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, *e.g.*, the Red Cross, for the purpose of coordinating with such entities the uses and disclosures permitted by "Notification of Location, Condition, or Death".

Use and Disclosures about Victims of Abuse, Neglect, or Domestic Violence.

Imagine! may disclose PHI about an individual that a Workforce member reasonably believes to be a victim of abuse, neglect, or domestic violence to law enforcement or a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence:

1. To the extent the disclosure is required by law and is limited to the relevant requirements of that law; or,
2. To the extent the disclosure is expressly authorized or required by statute or regulation.

If a member of Imagine!'s Workforce makes such a disclosure, the person served or their legal representative shall be promptly notified that such a report has been or will be made, except if:

1. A member of Imagine!'s Workforce, in the exercise of professional judgment, believes informing the person served would place the individual at risk of serious harm; or,
2. The individual being notified is a personal representative of the person served and there is a reasonable belief that the person representative is responsible for the abused, neglect, or other injury, and that informing the personal representative would not be in the best interests of the person served.

Disclosures for Judicial and Administrative Proceedings.

Any member of Imagine!'s Workforce who receives an order of a court, administrative tribunal, or a subpoena, a discovery request, or other lawful process, must promptly deliver the document to the Privacy Officer. The Privacy Officer will oversee and approve of the disclosure. Imagine! will disclose PHI in the course of any judicial or administrative proceeding:

1. In response to an order of a court or administrative tribunal, only the PHI expressly authorized by the order; or,
2. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
    A. Imagine! receives satisfactory assurances from the party seeking the information that reasonable efforts have been made by that party to ensure that the PHI of the person served has been given notice of the request, per the requirements below; or,
        i. The party requesting the information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
        ii. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the person served a chance to raise an objection to the court or administrative tribunal; and,
        iii. The time for the individual to raise objections to the court or administrative tribunal has elapsed and no objections were filed or all objections that were filed were resolved by the court and the disclosures being sought are consistent with that resolution.
    B. Imagine! receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by that party to secure a qualified protected order that meets the requirements below:

1. A qualified protected order has been sought if Imagine! receives from the requesting party a written statement and accompanying documentation demonstrating that:
    i. The parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or,
    ii. The party seeking the PHI has requested a qualified protected order from that court or administrative tribunal.
2. A qualified protected order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
    i. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the information was requested; and,
    ii. Requires the return to Imagine! or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Responding to a Subpoena

Employees, subcontractors and others associated with Imagine! may be served with a subpoena or shall receive a letter from a lawyer or a less formal request for information, testimony or documents. Similarly, employees, subcontractors and others associated with Imagine! may receive notification, or field questions or requests for information and documents, from Federal, State, or local authorities regarding an investigation. Imagine! shall respond to the request in a manner that appropriately addresses the request, while observing the advice of counsel, the requirements of HIPAA, the needs for confidentiality for persons served and the applicability of any other standards, statutes, court orders or policies.

A. Employees, subcontractors, interns, volunteers and others associated with Imagine! who are served with a formal or informal request for information, testimony or documents relating to any person served by Imagine!, or to Imagine! itself, shall promptly advise their supervisor, the Privacy Officer and the Chief Executive Officer (CEO).
    1. The CEO or Privacy Officer will coordinate responding to the request and provide direction to staff on their response.
B. Employees, subcontractors, interns, volunteers and others associated with Imagine! who receive notification, or field questions, from Federal, State, or local authorities regarding an investigation shall promptly advise their supervisor, the Privacy Officer and the Chief Executive Officer (CEO).
    1. The CEO or Privacy Officer will coordinate responding to the request and provide direction to staff on their response.

The CEO or Privacy Officer may seek the advice of counsel before responding to any subpoenas, court orders or investigatory requests for information.

Disclosures for Law Enforcement Purposes

An authorized member of Imagine!'s Workforce may disclose PHI for a law enforcement purpose to a law enforcement official:

1. As required by law, including mandatory reporting law;
2. In compliance with and as limited by relevant requirements of:
    a. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
    b. A grand jury subpoena; or,
    c. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that the information sought is relevant and material to a legitimate law enforcement inquiry, is specific and limited in scope in light of the purpose for which the information is sought, and de-identified information could not reasonably be used;

Limited Information for Identification and Location Purposes

An authorized member of Imagine!'s Workforce may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that only the following information is provided:

i. Name and address;
ii. Date and place of birth;
iii. Social security number;
iv. ABO blood type and rh factor;
v. Type of injury;
vi. Date and time of treatment;
vii. Date and time of death, if applicable; and,
viii. A description of distinguishing physical characteristics, including height, weight, gender, hair, eye color, race, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Victims of a Crime

An authorized member of Imagine!'s Workforce may disclose PHI in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, if:

i. The person served agrees to the disclosure, except for in instances of suspected mistreatment, abuse, neglect, or exploitation where disclosure is mandatory under law;
ii. Imagine! is unable to obtain the agreement of the person served because of incapacity or other emergency circumstance, provided that:
    a. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

b. The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and,
c. The disclosure is in the best interests of the person served as determined by the Imagine! Workforce member's professional judgment.

Decedents

Imagine! may disclose PHI about a person who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if Imagine! has a suspicion that such death may have resulted from criminal conduct.

Crime on the Premises

Imagine! may disclose PHI to a law enforcement official that he or she believes in good faith constitutes evidence of criminal conduct that occurred on Imagine! property.

Reporting Crime in Emergencies

If Imagine! is providing emergency health care in response to a medical emergency, other than on Imagine! property, an authorized member of Imagine!'s Workforce may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

1. The commission and nature of a crime;
2. The location of such crime or of the victim(s) of such crime; and,
3. The identity, description, and location of the perpetrator of the crime.

Uses and Disclosures for Public Health Activities

Imagine! may use and disclose PHI for the public health activities and purposes described below:

a. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, and the conduct of public health surveillance, public health investigations, and public health interventions;
b. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
c. To a school about an individual who is a student or a prospective student if the PHI disclosed is limited to proof of immunization and the school is required by law to have such proof of immunization in order to admit the student and the parent/guardian consents to such disclosure;
d. A person subject to the jurisdiction of the United States Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated products or activities. Such purposes include:
    i. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
    ii. To track FDA-regulated products;
    iii. To enable product recalls, repairs, or replacements; or,
    iv. To conduct post-marketing surveillance.

e. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease, if Imagine! or a public health authority is authorized by law to notify such person.

When Imagine! is required by any of these situations to inform the person served of a use or disclosure permitted by this section, or when the person served agrees to a use or disclosure permitted by this section, Imagine!'s information and the individual's agreement may be given orally. However, if given orally, the Imagine! Privacy Officer will document the giving of this information or the agreement by recording it in an Accounting of Disclosures for the person served.

Use and Disclosures About Decedents

Any member of Imagine!'s Workforce who receives a request, or proposes, to use or disclose PHI to a coroner, medical examiner, or funeral director must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will oversee the use or disclosure for compliance.

Coroners and Medical Examiners

With the oversight of the Privacy Officer, an authorized member of Imagine!'s Workforce may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

Funeral Directors

With the oversight of the Privacy Officer, an authorized member of Imagine!'s Workforce may disclose PHI to funeral directors consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, Imagine! may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

Uses and Disclosures for Cadaveric Organ, Eye, or Tissue Donation

Any member of Imagine!'s Workforce who receives a request, or proposes, to use or disclose PHI for purposes of cadaveric organ, eye or tissue donation must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance. An authorized member of Imagine!'s Workforce may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

Uses and Disclosures for Research Purposes

Any member of Imagine!'s Workforce who receives a request, or proposes, to use or disclose PHI for research purposes must promptly deliver the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance. With the oversight of the Privacy Officer, an authorized member of Imagine!'s Workforce may use or disclose PHI for research, regardless of the source of funding for the research, provided that:

1. Imagine! obtains documentation that an alteration to, or waiver, in whole or in part, of the individual Authorization required by these Privacy and Security Policies has been approved by either:
    a. An Institutional Review Board (IRB) or,
    b. A privacy board that meets the requirements of the HIPAA Privacy Rule (45 CFR §164.512(i)(1)(i)(B)).
2. Imagine! obtains from the researcher representations that:
    a. Use or disclosure is ought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
    b. No PHI will be removed from Imagine! by the researcher in the course of the review; and,
    c. The PHI for which use or access is sought is necessary for the research purposes.
3. Imagine! obtains from the researcher that:
    a. Representation that the use or disclosure is sought solely for research on the PHI of decedents;
    b. Documentation, at the request of Imagine!, of the death of such individuals; and,
    c. Representation that the PHI for which use or access is sought is necessary for the research purposes.

Use and Disclosures to Avert a Serious Threat to Health or Safety

Any member of Imagine!'s Workforce who receives a request, or proposes, to use or disclose PHI to avert a serious threat to health or safety must promptly deliver the request to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will oversee the use or disclosure for compliance. With the oversight of the Privacy Officer, an authorized member of Imagine!'s Workforce may use or disclose PHI if that person, in good faith, believes the disclosure meets either of the following:

1. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;
    a. A use or disclosure of this type above may not be made if the information is learned in the course of treatment, counseling, or therapy to address the propensity of the individual to commit the crime or through a request by the individual to initiate or be referred for treatment, counseling, or therapy.
2. Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that Imagine! reasonably believes may have caused serious physical harm to the victim or where it appears from all circumstances that the individual has escaped from a correctional institution or from lawful custody.

Use and Disclosures for Health Oversight Activities

With the oversight of the Privacy Officer, an authorized member of Imagine!'s Workforce may disclose PHI to a health oversight agency, e.g., state department of health, CMS, for oversight

activities authorized by law, including: audits, civil, administrative, or criminal investigations; inspections, licensure or disciplinary actions; civil, administrative, or criminal proceedings or other actions; or, other activities necessary for appropriate oversight of:

1. The health care system;
2. Government benefit programs for which health information is relevant to beneficiary eligibility;
3. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or,
4. Entities subject to civil rights laws for which health information is necessary for determining compliance.

Use and Disclosures for Specialized Government Functions

Any member of Imagine!'s Workforce who receives a request, or proposes, to use or disclose PHI for purposes of a specialized government function must promptly deliver the request to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance. Specialized government functions include:

1. Military and veterans activities;
2. Foreign military personnel;
3. National security and intelligence agencies;
4. Protective services for the President and others;
5. Correctional institutions and other law enforcement custodial situations:
    a. An authorized member of Imagine!'s Workforce may use or disclose PHI about an inmate or individual, if the correctional institution or such law enforcement official represents that such PHI is necessary for:
        i. The provision of health care to such individuals;
        ii. The health and safety of the person served, other inmates, or the officers or employees at the correctional institution;
        iii. The safety of law enforcement on the premises of the correctional institution;
        iv. The administration and maintenance of the safety, security and good order of the correctional institution.

Disclosures for Worker's Compensation

Unless the use or disclosure has previously been approved by the Privacy Officer, a member of Imagine!'s Workforce who receives a request, or proposes, to disclose PHI to comply with laws relating to workers compensation or other similar programs, must promptly deliver the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance.

Disclosures to the Secretary of Health and Human Services

Any member of Imagine!'s Workforce who receives a request, or proposes, to disclose PHI information to the Secretary of Health and Human Services must promptly deliver the request to

the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the disclosure for compliance.

Imagine! will permit access by the Secretary of Health and Human Services during normal business hours to its facilities, books, records, accounts and other sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable requirements of HIPAA. If the Secretary of Health and Human Services determines that exigent circumstances exist, such as when documents may be hidden or destroyed, Imagine! will permit access by the Secretary of Health and Human Services at any time and without notice.

If any information required of Imagine! under this section is in the exclusive possession of any other agency, institution, or person and that other agency, institution or person fails or refuses to furnish the information, the Privacy Officer will so certify and set forth what efforts Imagine! has made to obtain the information.

Disclosures by Whistleblowers

A member of Imagine!'s Workforce or a business associate may disclose PHI and de-identified PHI as permitted by HIPAA rule and regulations in accordance with these policies, provided that:

1. The Workforce member or business associate believes in good faith that Imagine! has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by Imagine! potentially endangers one or more persons served or supported by Imagine!, workers, or the public; and,
2. The disclosure is to:
    a. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Imagine! or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Imagine!; or,
    b. An attorney retained by or on behalf of the Workforce member or business associate for the purpose of determining the legal options of the Workforce member or business associate with regard to the reported conduct. Disclosure to a non-Business Associate retained attorney would have to be de-identified PHI.

The disclosure does not need to be approved by the Privacy Officer before it is made.

Disclosures by Workforce Members Who are Victims of a Crime

A Workforce member who is the victim of a criminal act may disclose PHI to a law enforcement official, provided that:

1. The PHI disclosed is about the suspected perpetrator of the criminal act; and,
2. The PHI disclosed is limited to the following information:
    a. Name and address;
    b. Date and place of birth;

c. Social security number;
d. ABO blood type and Rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and,
h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

The disclosure does not need to be approved by the Privacy Officer before it is made.

Disclosures to Business Associates

Authorized members of Imagine!'s Workforce may disclose PHI to a business associate and may allow a business associate to create, receive, maintain, or transmit PHI on Imagine!'s behalf, if Imagine! has a written contract with the business associate that meets the requirements of the HIPAA Privacy Rule. However, such a written contract will not be required from a business associate that is a subcontractor of a business associate. PHI disclosed shall be limited to the minimum necessary for the services provided by the business associate.

Uses and Disclosures for Marketing

Imagine! obtains the written Authorization of a person served, their parent (if a minor), legal guardian or personal representative prior to using PHI and/or a photograph of a person served in its marketing or communication materials.

The Privacy Rule defines marketing as a communication and/or disclosure of PHI that encourages an individual to use or purchase a product or service, except under the following conditions:

1. Communications made directly by Imagine! to describe the services it provides;
2. Communications made for care or treatment of the individual;
3. Communications for case management or care coordination for the person served, the parent of a minor, legal guardian or personal representative;
4. Communications to direct or recommend alternative treatments, therapies, and care providers or settings of care; and,
5. Face to face communications made by Imagine! representatives to an individual.

A member of Imagine!'s Workforce may not use or disclose PHI for marketing without an Authorization that meets the applicable requirements of this section. If the marketing involves financial remuneration to Imagine! from a third party, the Authorization must state that such remuneration is involved. Any use of PHI for marketing without an Authorization must be approved in advance by the Privacy Officer.

Imagine! staff shall obtain a valid, completed Authorization to Use or Disclose Protected Health Information form prior to using or disclosing PHI for purposes that meet the HIPAA definition of marketing and do not qualify for any of the exceptions listed in items 1-5 above.

1. If direct or indirect remuneration to Imagine! from a third party is involved, the Authorization shall state the nature of such third party remuneration.
2. Imagine! shall make reasonable efforts to verify that persons served who decide to opt out of any use of their PHI is documented appropriately and honored by Imagine! staff or its business associates.

No Authorization is required in the following situations:

1. When communications are directed at an entire population (not to a targeted individual) that promote health or services in a general manner and do not endorse a specific product or service.
2. When PHI is not disclosed in a marketing communication (such as a newspaper advertisement).

In the event a planned marketing activity involves payment to Imagine! (e.g., cash, referral, gifts, etc.), anti-kickback, inducement, self-referral and general fraud and abuse statutes and regulations may apply. These shall be considered prior to implementation of the marketing activity.

Uses and Disclosures for Fundraising

An authorized member of Imagine!'s Workforce may use or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without an Authorization:

a. Demographic information relating to a person served;
b. Dates of health care provided to a person served;
c. Department of service information;
d. Treating physician;
e. Outcome information; and,
f. Health insurance status.

Any use of PHI for the purpose of raising funds for Imagine!'s benefit without an Authorization must be approved in advance by the Privacy Officer.

Fundraising Requirements

Imagine! will not use or disclose PHI for fundraising purposes unless a statement is included in its Notice of Privacy Practices stating that Imagine! may contact the individual to raise funds for Imagine! and the individual has a right to opt out of receiving such communications.

1. Right to Opt Out: With each fundraising communication sent to an individual, Imagine! will provide the individual with a clear opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive any further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.
2. No Conditioning of Treatment or Payment: Imagine! will not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

3. Cessation of Fundraising Communications to an Individual: Imagine! will not make fundraising communications to an individual where the individual has elected not to receive such communications.
4. Right to Opt In: With the Privacy Officer's approval, Imagine! may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

Sale of Protected Health Information

Imagine! will obtain an Authorization for any disclosure of PHI for which the disclosure is for direct or indirect payment from or on behalf of the recipient of the PHI. Such Authorization will state that the disclosure will result in payment to Imagine!.

This does not apply, however, to disclosures of PHI:

1. For research purposes where the only payment received by Imagine! is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;
2. For the sale, transfer, merger, or consolidation of all or part of Imagine!;
3. To or by a business associate for activities that the business associate undertakes on behalf of Imagine! and the only payment provided is by Imagine! to the business associate for the performance of such activities;
4. Permitted by and in accordance with the applicable requirements of the HIPAA Privacy Rule, where the only payment received by Imagine! a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by law.

Restrictions to Permitted Uses and Disclosures of Protected Health Information

The person served, their parent (if a minor), legal guardian or personal representative are notified of their right to request restrictions on the use and disclosure of their PHI in Imagine!'s Notice of Privacy Practices. Specifically, the person served may request restrictions on:

1. The use or disclosure of PHI for treatment, payment, or healthcare operations; or,
2. The disclosures to family/friends/others involved in care and notification purposes.

A restriction agreed to by Imagine! is not effective to prevent uses or disclosures when the use or disclosure does not require an Authorization or a requirement for an opportunity to agree or object to the use or disclosure.

Requesting Restrictions on Use and Disclosure of PHI

Persons served, their parent (if a minor), legal guardian or personal representative shall make their request in writing. The Privacy Officer or his/her designee shall provide a Request to Restrict Use and Disclosure of PHI form to the individual asking to make a restriction.

The Privacy Officer manages requests for restrictions. A request for restriction shall not be reviewed until the Request to Restrict Use and Disclosure of PHI form is completed and signed by the person served or their representative. The Privacy Officer shall review the request in consultation with Imagine! staff providing coordination of care to the person served in order to determine the feasibility of the request. Imagine! shall give primary consideration to the need for access to PHI for service and payment purposes in making its determination.

If Imagine! agrees to the requested restriction, the Privacy Officer shall document the restriction on the Request to Restrict Use and Disclosure of PHI form, provide the individual making a request with a copy, forward the copy for archiving, and document the restriction on the electronic health record system. The Privacy Officer shall also notify the appropriate Imagine! employees, subcontractors, interns or volunteers of the restriction.

Exceptions to Accepted Restrictions

Imagine! staff shall abide by the accepted restriction with the following exceptions:

1. Imagine! may use the restricted PHI, or may disclose such information to an authorized provider, if the person served is in need of emergency services. In this case, Imagine! staff shall release the information, but ask the emergency provider not to further use or disclose the PHI of the person served.
2. Imagine! may disclose the information to the individual who requested the restriction.
3. Imagine! may use and disclose the PHI when statutorily required to use and disclose the information under the Privacy Rule.

Declining a Request for Restriction on Use and Disclosure of PHI

If Imagine! declines the request for restriction, the Privacy Officer shall complete the "Facility Response" section of the Request to Restrict Use and Disclosure of Protected Health Information

form and provide a copy to the individual making the request. The Request and documentation associated with the request shall be placed in the master record of the person served.

Terminating a Restriction on Use and Disclosure of PHI

If the person served, their parent (if minor), legal guardian, or personal representative wishes to terminate the accepted restriction, they may do so in writing or verbally. If verbally terminated, Imagine! staff shall document the verbal agreement in the master record of the person served and the restriction on the electronic health record shall be removed.

The Privacy Officer shall notify the appropriate program and/or care coordination staff of the termination of the restriction and document the termination of the restriction on the Request to Restrict Use and Disclosure of Protected Health Information form, provide the person served with a copy and maintain the documentation in the master record of the person served.

Terminating the Restriction without Person's Agreement

There may be situations that occur in which Imagine! wishes to terminate the restriction without the agreement of the person served, their parent (if minor), legal guardian, or personal representative when permitted by HIPAA rule and regulation. The Privacy Officer will communicate that the restriction is being terminated.

a. If by mail: The notification shall be sent via certified mail, return receipt requested. Imagine! shall maintain a copy of the notification and of the return receipt with the Request to Restrict Use and Disclosure of Protected Health Information form. Imagine! shall not terminate the restriction until it receives confirmation that the person served has have received the notification.
b. If in person: It is preferable to have the appropriate individual (person served, their parent [if minor], legal guardian, or personal representative) sign and date a notification of termination of a restriction. However, it shall be acceptable to document that the person(s) listed above were notified on the Request to Restrict Use and Disclosure of Protected Health Information form.
c. If by telephone: This action shall be documented on the Request to Restrict Use and Disclosure of Protected Health Information form. In addition, an email, or alternatively, a letter shall be sent as well. Letters shall be sent via certified mail, return receipt requested. The termination shall be effective as of the date the appropriate individual listed above is informed by telephone.
d. If by email: This action shall be documented on the Request to Restrict Use and Disclosure of Protected Health Information form. The message shall be sent via encrypted email, to a verified email account to the appropriate person. The termination shall be effective as of the date of the email.

Such termination is only effective with respect to PHI created or received after Imagine! has informed the person served, the parent (if minor), legal guardian, or personal representative that the restriction is being terminated. Imagine! shall continue to abide by the restriction with

respect to any PHI created or received before it informed the person(s) listed above about the termination of the restriction.

Communication and Access to Protected Health Information by Persons Receiving Services

Persons served, their parent (if a minor), legal guardian or personal representative have the right to request communication about their PHI in a variety of ways, such as through phone calls, emails, or in writing as well as the right to direct where PHI is to be sent. They also have the right to inspect and obtain a copy of PHI in the designated record set, except for information compiled in reasonable anticipation of, or for, use in a civil, criminal or administrative action or proceeding.

Requests for Alternate Communication Methods

When a person served notifies Imagine! staff of their preferred method of communication, or requests that Imagine! communicate with him or his/her personal representative by some alternate means, Imagine! shall promptly provide the person served with a copy of a Request for Communications by Alternative Means form. A request shall not be evaluated until this request form is completed and signed by the person served or personal representative. Reasonable requests shall be honored by Imagine! staff.

The Privacy Officer shall review the completed Request for Communications by Alternative Means form to determine if it is a reasonable request. The Privacy Officer shall not require an explanation for the request and shall generally accommodate a request determined to be reasonable.

The Privacy Officer shall complete the response section of the Request for Communications by Alternative Means form to inform the person served of Imagine!'s decision.

Procedures for Access to PHI by Persons Receiving Services

A person served, parent of a minor, legal guardian or personal representative is notified of their right to access PHI in Imagine!'s Notice of Privacy Practices. The Notice of Privacy Practices is given to the person served upon application to Imagine!.

A person served, parent of a minor, legal guardian, or personal representative has the right to inspect the designated record set (see *Designated Record Set* for definitions) except for components of the record that are inaccessible per HIPAA rule and regulation (see *Requests for Master Record Copy or Portions of the Designated Record Set* for definitions). Their request shall be communicated in writing to the attention of the Privacy Officer.

1. The Privacy Officer or his/her designee shall manage the viewing of the designated record set and determine whether the requestor is considered a legal representative based on State law (e.g., guardian, conservator, durable power of attorney).

2. The Privacy Officer or his/her designee shall verify the identity of the requester before he/she is allowed access to the record (e.g., driver's license, identification card, other legal ID).

The Privacy Officer or his/her designee shall set up a meeting within 24 hours as required by law. If the requestor cannot accommodate a meeting within the 24 hour time frame, the review shall be set up at a mutually agreed upon time.

1. If possible, program or case management staff shall be in attendance during the meeting, to answer questions, prevent the record from being altered and to prevent documents from being removed or destroyed.
2. The person served or their legal representative shall be allowed to review and read the record without intervention from the staff present.
3. If the PHI is stored off-site, Imagine! is allowed thirty (30) days to fulfill the request. If the request cannot be processed within the allowed thirty (30) days, Imagine! may have a onetime extension of an additional thirty (30) days. A written statement of the reasons for the delay shall be provided and the date by which Imagine! shall complete its action on the request will be stated.

When a person served, parent of a minor, legal guardian, or personal representative requests a copy of the PHI in the designated record set, they shall communicate this request in writing per the Requests for Master Record Copy procedures in this document and direct it to the attention of the Privacy Officer.

A reasonable cost-based fee may be charged for the paper copies provided. The cost per page may not exceed the State statute for copying costs. One (1) free copy of the designated record set shall be made available to the person served or his/her legal representative.

If a <u>former</u> person served, parent of a minor, legal guardian, or personal representative requests to view or review PHI, Imagine! shall respond to the request within thirty (30) days.

1. If the PHI is stored off-site, or cannot be processed within the allowed thirty (30) days, Imagine! may have a onetime extension of thirty (30) days, provided that a written statement of the reasons for the delay are provided and the date by which Imagine! shall complete its action on the request is stated.
2. The Privacy Officer shall provide the PHI in the form or format requested. If the PHI is not accessible in the format requested, a readable hard copy or a format acceptable to Imagine! and the person making the request shall be provided. A reasonable cost-based fee may be charged for the paper copies provided. The cost per page may not exceed the State statute for copying costs.

Procedures for Denying Access to PHI by Persons Receiving Services

Imagine!'s Privacy Officer will provide a timely, written denial to the person served, parent of a minor, legal guardian, or personal representative. The denial will be written in plain language and contain:

1. The basis for the denial.
2. If applicable, a statement of the individual's review rights, including a description of how the individual may complain to Imagine! or to the Secretary of the Office of Civil Rights.
3. If Imagine! does not maintain the PHI that is the subject of the request for access, and Imagine! knows where the requested information is maintained, a statement informing the requestor where to direct the request for access.
4. Imagine! may deny the request if the PHI is not contained in its designated record set.

Person served, the parent of a minor, legal guardian, or personal representative have the right to request a review of the denial. If a denial review request is received, the following steps shall be taken:

1. Imagine!'s Security Officer or CEO shall promptly review the denial.
2. The request may also be reviewed by a qualified individual who was not directly involved in the denial, if necessary.
3. Imagine! shall promptly provide written notice of the results of the review and based on the review, take any necessary steps required.

Imagine! may deny the request for access to the PHI of a person served without a right to review if:

1. Psychotherapy notes;
2. Information compiled in anticipation of, or use in, a civil, criminal or administrative action or proceeding;
3. If such information is protected by more stringent disclosure statues such as alcohol or substance abuse information or HIV status and HIPAA Rules and Regulations do not require disclosure or are preempted;
4. Information gathered in the process of an investigation as requited by rule and statute, in response to allegations of mistreatment, abuse, neglect, and exploitation, and other incidents defined as critical by regulatory agencies.
5. The requested PHI was obtained by someone other than Imagine! (e.g. a family member of the person served) under a promise a confidentiality and providing access to the information would be reasonably likely to reveal the source of the information.
6. An inmate requests a copy of their PHI held by a correctional institution and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate, or other inmates, or the safety of correctional officers, employees, or other persons at the institution or responsible for transporting the inmate. However, in these cases, an inmate retains the right to inspect their PHI.

Reviewable grounds for denial include (as determined by a licensed health care professional in the exercise of professional judgement):

1. The access is reasonably likely to endanger the life or physical safety of the person served or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g. concerns that the individual will not be able to understand the information or may be upset by it).

2. The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
3. The access to a personal representative of the person served that requests such access is reasonably likely to cause substantial harm to the person served or another person.

Amendment of Protected Health Information

Individuals receiving services from Imagine!, their parent (if a minor), legal guardian or personal representative shall be notified of the right to amend his or her PHI in the Notice of Privacy Practices.

Procedures for Evaluating and Responding to a Request for Amendment of PHI

The Privacy Officer shall process all requests for amendment of PHI.

Upon receiving an inquiry from a person served, the parent of a minor, legal guardian or personal representative regarding the right to amend his/her PHI, the Privacy Officer shall provide a copy of an Amendment of Protected Health Information form. A request for amendment shall not be evaluated until the request form is completed and signed by the person served, the parent of a minor, legal guardian or personal representative.

The Privacy Officer shall act on the request for amendment no later than 60 days after receipt of the request.

1. If the amendment is accepted, the Privacy Officer or his/her designee will add the requested amended information to the original content and then inform the person served, the parent of a minor, legal guardian or personal representative within 60 days of the written request.
2. If the amendment is denied, Imagine! will notify the person served, the parent of a minor, legal guardian or personal representative in writing of the denial within 60 days of the written request.
3. If Imagine! is unable to act on the request for amendment within 60 days of receipt of the request, it may have one extension of no more than 30 days. The Privacy Officer will notify the person served, the parent of a minor, legal guardian or personal representative in writing of the extension, the reason for the extension and the date by which action shall be taken.

Procedures for Accepting a Request for Amendment of PHI

If the Privacy Officer, in consultation with the appropriate department director and/or staff, determines that the request for amendment shall be accepted, in whole or in part, the Privacy Officer shall:

1. Place a copy of the amendment in the records of the person served, or provide a reference to the location of the amendment within the body of the master record.
2. The person served or the parent of a minor, legal guardian or personal representative may indicate providers or entities with whom the amendment shall be shared (as identified on the original Amendment of PHI form.
3. This notification shall occur within a reasonable period of time.

The Privacy Officer shall also identify other persons, including business associates, which he/she knows have the PHI and that may have relied on, or could foreseeably rely on, such information to the detriment of the person served. The Privacy Officer shall determine whether the person

served, the parent of a minor, legal guardian or personal representative wishes for Imagine! to notify such other persons or organizations of the amendment.

1. If the person served, the parent of a minor, legal guardian or personal representative wishes for Imagine! to notify these individuals, the Privacy Officer shall obtain a signed Authorization to Release PHI form.
2. This notification shall occur within a reasonable period of time.

Procedures for Denying a Request for Amendment of PHI

Imagine! may deny the request for amendment in whole or in part if:

1. The PHI was not created by Imagine!. An exception may be granted if the person served, the parent of a minor, legal guardian or personal representative provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the requested amendment and it is apparent that the amendment is warranted. (Note: This shall rarely be the case.) Every other avenue shall be explored before an amendment is made to information that was not created by Imagine!.
2. The PHI is not part of the designated record set.
3. The PHI would not be available for inspection under the HIPAA Privacy Rule.
4. The PHI that is subject to the request for amendment is accurate and complete.

If the Privacy Officer, in consultation with the appropriate department director and/or staff, determines that the request for amendment shall be denied in whole or in part, the Privacy Officer shall provide the person served, the parent of a minor, legal guardian or personal representative with a timely amendment denial letter. The denial shall be written in plain language and shall contain:

1. The basis for the denial;
2. A statement that the person served, the parent of a minor, legal guardian or personal representative has a right to submit a written statement disagreeing with the denial and an explanation of how to file such a statement;
3. A statement that, if the person served, the parent of a minor, legal guardian or personal representative does not submit a statement of disagreement, they may request that Imagine! includes the request for amendment and the denial with any future disclosures of the PHI; and,
4. A description of how the person served, the parent of a minor, legal guardian or personal representative may file a complaint with Imagine! or to the Secretary of the U.S. Department of Health and Human Services. The description shall include the name or title and telephone number of the contact person for complaints.

If the person served, the parent of a minor, legal guardian or personal representative submits a written statement of disagreement, Imagine! may prepare a written rebuttal to the statement. Imagine! shall provide a copy of the written rebuttal to the person served, the parent of a minor, legal guardian or personal representative who submitted the statement within a reasonable period of time.

The following documentation shall be appended (or otherwise linked) to the PHI that is the subject of the disputed amendment:

1. The person served, the parent of a minor, legal guardian or personal representative's Amendment of PHI form;
2. Imagine!'s amendment denial letter;
3. The person served, the parent of a minor, legal guardian or personal representative's statement of disagreement, if any; and,
4. Imagine!'s rebuttal, if any.

If the person served, the parent of a minor, legal guardian or personal representative submitted a statement of disagreement, Imagine! shall disclose that statement of agreement, Imagine!s amendment denial letter and Imagine!'s rebuttal or an accurate summary of such information with future disclosures of the PHI to which the disagreement relates.

If the person served, the parent of a minor, legal guardian or personal representative did not submit a statement of disagreement, and if the person served, the parent of a minor, legal guardian or personal representative has requested that Imagine! provide the Amendment of PHI form and the amendment denial letter with any future disclosures, Imagine! shall include these documents (or an accurate summary of that information) with future disclosures of the PHI to which the disagreement relates.

Procedures if Imagine! Receives a Notice of Amendment from another Entity or Provider

Any member of Imagine!'s Workforce who is informed by another provider, health plan or a healthcare clearinghouse of an amendment to an individual's PHI shall promptly inform the Privacy Officer of the amendment. The Privacy Officer shall make the amendment to the designated record set.

1. Amendments to the designated record set shall be filed with that portion of the PHI to be amended.
2. Amendments that cannot be physically placed near the original PHI shall be filed in an appropriate location. A reference to the location of the amendment shall be added near the original information location.

Accounting of Disclosures of Protected Health Information

Persons served, their parent (if a minor), legal guardian or personal representative have the right to receive an accounting of the disclosures of their PHI maintained in their designated record set.

Procedures for Accounting of Disclosures of PHI

Upon receiving an inquiry about disclosures of PHI, the Privacy Officer shall provide the person served, the parent of a minor, legal guardian or personal representative with a copy of a Request for an Accounting of Disclosures of PHI form.

1. Requests are not evaluated until the form is completed and signed by the person served, the parent of a minor, legal guardian or personal representative.
2. The Privacy Officer shall review and process the request.

The written accounting of disclosures is provided to the requestor using a format created and maintained by Privacy Officer.

1. The accounting shall include disclosures during the period specified by the person served, the parent of a minor, legal guardian or personal representative in the request. The specified period may be up to six years prior to the date of the request. Disclosures made on or before April 13, 2003 shall not be included in the accounting.
2. The Privacy Officer shall include known disclosures made by its Business Associates, if aware of any such disclosures that are required to be included in an accounting of disclosures.
3. The Privacy Officer shall exclude those disclosures that qualify as an exception.
4. For each disclosure, the accounting shall include:
    a. The date the request for disclosure was received and when disclosure was made;
    b. The name of provider or entity requesting disclosure and, if known, the address of such person or entity;
    c. A brief description of the PHI that was disclosed; and,
    d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
5. If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, the Privacy Officer may provide:
    a. The first disclosure during the accounting period;
    b. The frequency, or number of disclosures made during the accounting period;
    c. The date of the last such disclosure during the accounting period.

The Privacy Officer shall provide the written accounting of disclosures no later than 60 days after receipt of the request. If Imagine! is unable to meet the 60-day time frame, Imagine! may extend the time once by no more than 30 days as long as the individual is provided with a written statement of the reasons for the delay and the date by which Imagine! shall provide the accounting.

Imagine! provides the first accounting of disclosures within a 12-month period without charge. However, Imagine! may impose a reasonable, cost-based fee for each subsequent request for an

accounting by the same party within the 12-month period, provided Imagine! has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.

Imagine! shall document and retain for six (6) years from the date of the accounting for records:

1. The information required to be included in the accounting; and,
2. The written accounting provided to the requesting party.

Procedures Regarding the Exceptions to the Accounting of Disclosures

Accounting of disclosure does not include disclosures:

1. Necessary to carry out treatment, payment, and healthcare operations;
2. To the person served, the parent of a minor, legal guardian or personal representative for whom the PHI was created or obtained;
3. Pursuant to a signed Authorization by the person served, the parent of a minor, legal guardian or personal representative;
4. To persons involved in the care of the person served;
5. For national security or intelligence purposes;
6. To a correctional institution;
7. Temporarily suspended by a law enforcement official or health oversight agency (exception applies only during the period of suspension as long as the agency or official provides Imagine! with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities);
8. That are incidental;
9. As part of a Limited Data Set; and,
10. That occurred on or prior to April 13, 2003.

HIPAA Privacy Complaints

Any concerned individual has the right to file a formal complaint concerning privacy issues without fear or reprisal. Such issues could include, but are not limited to, allegations that:

- PHI was used/disclosed inappropriately;
- Access or amendment rights were wrongfully denied;
- Imagine!'s Notice of Privacy Practices does not reflect current practices accurately.

Imagine! uses the Notice of Privacy Practices form to notify persons receiving services, parent(s) of a minor, legal guardians or their personal representative of their right to complain to Imagine!, or the US Department of Health and Human Services, about privacy issues.

Individuals who have concerns or complaints about Imagine!'s privacy and breach notification policies and procedures, its compliance with those policies and procedures, or the requirements of the HIPAA Privacy and Breach Notification Rules shall direct their concerns or complaints to the Privacy Officer by telephone, fax, mail, email, or in person. The person making the complaint may also put their complaint in writing through Imagine!'s EthicsPoint system. The Privacy Officer will document all privacy issue complaints in a designated log.

The Privacy Officer will investigate the complaint and respond to the individual in writing concerning his or her findings and what action, if any, Imagine! will take in response to the complaint. Written documentation of each complaint and its disposition will be kept in written or electronic form for six (6) years after the date of its creation or the date when it was last in effect, whichever is later.

Imagine!'s Workforce members may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against the person served, the parent of a minor, legal guardian or personal representatives or any other person filing a complaint.

De-Identification of Health Information

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not Individually Identifiable Health Information. There are important uses to de-identified PHI. Imagine! may use de-identified health information to report on company-wide demographic information, quality of service initiatives, cost efficiencies, and other topics or areas of interest directly related to the work of the organization.

Requirements for De-Identification

Before any member of Imagine's Workforce treats any information as being de-identified, the information must be submitted to the Privacy or Security Officer. Whether or not health information has been de-identified will be determined by the Privacy or Security Officer.

The Privacy or Security Officer may find that health information has been de-identified only if one of the following two conditions are met:

Condition One: Statistical and Scientific Principles

A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable applies such principles and determines that the risk is very small that the information could be used to identify the consumer. The methods and results of the analysis shall be documented.

Condition Two: Removal of Identifiers

The following identifiers of the individual or of relatives, employers, or household members of the individual are removed and Imagine! does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information:

1. Names;
2. All geographic subdivisions smaller than a State, including street addresses, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and he initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;

7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images;
18. Any other unique identifying number, characteristic, or code.

Requirements for Re-Identification of PHI

During the process of de-identifying PHI, the Privacy or Security Officer, or consultants performing statistical de-identification, shall assign a code that allows the information to be re-identified by Imagine! as long as the code is not derived from or related to information about the person served, and is not otherwise capable of being translated so as to identify the person served. The code or other means of record identification shall not be used or disclosed for any other purpose and the mechanism for re-identification shall not be disclosed.

Whether or not information shall be coded for re-identification and be re-identified shall be determined by the Privacy Officer. If information is re-identified, the Privacy or Security Officer shall oversee the process of doing so.

Business Associates

Some providers that contract with Imagine! may be required to sign a Business Associate (BA) Agreement in which they supply assurances that they will create, receive, use, safeguard, disclose and transmit the PHI of persons receiving services within HIPAA Privacy and Security regulations and as permitted by the BA Agreement. See **Business Associate** for who Imagine!'s business associates are.

A. Imagine! shall follow established procedures regarding contract review, revision and approval to verify that the contract is in compliance with State and Federal law, to include any HIPAA contract addendums.
B. The Chief Financial Officer (CFO) and Privacy/Security Officer shall determine whether a BA Agreement is necessary for specific entities. Common examples of entities needing a BA Agreement are:
    1. A CPA firm whose accounting services involve access to PHI;
    2. An attorney who reviews PHI to assist in a case or any other matter that requires the disclosure of PHI to the attorney; and,
    3. Consultants or vendors who may see PHI in the course of completing their duties for Imagine!.
C. If a BA Agreement is necessary and the other party provides its own BA Agreement, the CFO and Privacy/Security Officer shall review the Agreement to assure it meets requirements of the Privacy and Security Rule.
D. If a BA Agreement is necessary, and the other party does not provide the Agreement, the CFO or Privacy/Security Officer shall submit Imagine!'s BA Agreement for approval by the other party.
E. If the BA refuses to sign the Agreement, the Privacy Rule prohibits Imagine! from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of Imagine!, Imagine! shall not contract with the BA.
F. The original signed contract and contract addendum containing BA language shall be maintained by Imagine!.
G. The CFO and Privacy/Security Officer shall amend BA Agreements when changes occur to HIPAA rules, regulations and standards.

Procedures for Breach of a BA Agreement and Sanctions

If Imagine! staff learns of a breach or violation of a BA requirement by a BA, it shall be reported to the CFO or a Privacy/Security Officer. The Privacy/Security Officer shall determine whether reasonable steps can be taken to cure the breach. The BA is required to take whatever reasonable steps can be taken to cure the breach and prevent further breaches of PHI in the future.

If reasonable steps to cure the BA's violations are unsuccessful, or if the BA refuses to take necessary steps to cure the breach or prevent further breaches of PHI, Imagine! may:

1. Terminate the contract or arrangement; or
2. If termination is not feasible, report the violation to the Secretary of the U.S. Department of Health and Human Services.

When a contract with a BA is being terminated, the BA is obligated to return or destroy any PHI that was shared with the BA as a result of its contract with Imagine!.

The Privacy/Security Officer shall assist with contacting the BA regarding the BA's obligations to return or destroy PHI that originated from Imagine!. If return or destruction is not feasible, the BA is obligated to maintain the PHI that originated from Imagine! in accordance with HIPAA standards, rules and regulations.

The contract and contract addendum shall be retained for no less than six years after the contract was last in effect.

Determining Whether a Breach of PHI Occurred

This section addresses Imagine!'s Breach Notification Rule Requirements. An acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Privacy or Security Officer or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and,
4. The extent to which the risk to the PHI has been mitigated.

The risk assessment will also examine the three exceptions of a definition of a breach:

1. Unintentional acquisition, access, or use of PHI by a Workforce member or person acting under the authority of Imagine! or Imagine! business associate and such acquisition, access, or use was made in good faith and within the scope of authority;
2. Inadvertent disclosure of PHI by a person authorized to access PHI to another person authorized to access PHI at Imagine!, a member of the OHCDS, or an Imagine! business associate;
3. Imagine! or Imagine!'s business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Procedures for Breach Notification

Imagine! maintains an open-door policy regarding compliance with HIPAA. Employees, subcontractors, interns and volunteers are encouraged to speak with the Privacy/Security Officer or other appropriate individual regarding any concerns they may have with Imagine!'s HIPAA policies and procedures or initiatives designed to maintain and enhance privacy and security controls. There shall be no retaliation against employees, subcontractors, interns or volunteers who, in good faith, report any activities he or she believes is a breach of HIPAA. Although not guaranteed (depending on the circumstances) anonymity shall be maintained whenever possible. Imagine! may impose lesser sanctions, when it determines it is appropriate, when a Workforce member is responsible for a breach, and reports the breach; and/or that more severe sanctions may be imposed for a Workforce member who is responsible for a breach, but fails to report it, under appropriate circumstances.

Employees, subcontractors, interns or volunteers who believe that unauthorized access, use or disclosure of PHI has occurred shall immediately report the circumstances of the suspected breach to their supervisor and the Privacy Officer (or, in the absence of the Privacy Officer, reports may be made to the Security Officer) within forty-eight (48) hours after knowledge of the incident. The report of a potential breach shall include the following information, to the extent available:

1. A brief description of what happened, including the date of the potential breach and the date the potential breach was discovered;

2. Who used the PHI without appropriate permission or Authorization and/or to whom the information was disclosed without permission or Authorization;
3. A description of the types of and amount of unsecured PHI involved in the breach;
4. Whether the PHI was secured by encryption, destruction, or other means;
5. Whether any intermediate steps were taken to mitigate an impermissible use or disclosure;
6. Whether the PHI that was disclosed was returned prior to being accessed for an improper purpose; and,
7. If the PHI was provided to Imagine! under a Business Associate Agreement.

Following a report of a concern of impermissible use or disclosure of PHI, the Privacy Officer, or her designee, will complete a risk assessment to determine the probability level that the PHI has been compromised by the impermissible use or disclosure. The conclusion of the risk assessment will be documented, along with any actions needed, such as a notification letter, in the Imagine! HIPAA Incident Log. It is expected that members of Imagine!'s Workforce will cooperate in the investigation and assessment.

Failure to report a suspected breach to the Privacy or Security Officer may result in disciplinary action against employees, subcontractors, interns or volunteers.

Timeline of Notification

HIPAA's breach notification rule requires notification to affected individuals, the Secretary of USHHS, and in certain cases, the media, without unreasonable delay and within sixty (60) calendar days following the discovery of a breach under Federal and or State HIPAA rule guidelines. The discovery of a breach includes the first date it shall have been known by exercising reasonable diligence.

Content of Notification

The Privacy Officer will be responsible for writing and sending the Breach Notification letters to affected individuals. The notification shall be written in plain language and include to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps individuals shall take to protect themselves from potential harm resulting from the breach;
4. A brief description of what Imagine! is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
5. Contract procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site, or postal address.

Generally, the notice shall avoid including any sensitive material, such as a social security number or credit card number.

Reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by Imagine! and as may be necessary to ensure effective communication with individuals with disabilities.

Methods of Breach Notification

Written Notice

The notification to affected individuals shall be by mail to the individual at the last known address of the individual. The notification may be provided in one or more mailings as information is available.

If Imagine! knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by mail to either the next of kin or the personal representative is permitted. It may be provided in one or more mailings as information is available.

Substitute Notice

If there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice, which is reasonably calculated to reach the individual, will be used, including contacting the next of kin or personal representative. If Imagine! has insufficient or out-of-date contact information for 10 or more persons served, Imagine! shall post the notice on the home page of Imagine!'s website for at least 90 days or provide the notice to a major print or broadcast media where the affected persons served most likely reside. Imagine! shall include a toll-free number that remains active for at least 90 days where persons served can learn if their information was involved in the breach.

Additional Notice in Urgent Situations

If the Privacy Officer deems the situation to require urgency because of possible imminent misuse of unsecured PHI, Imagine! may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice stated above.

Notification to the Media

If a breach of unsecured PHI involves more than five hundred (500) residents of a State or other jurisdiction, Imagine! shall notify prominent media outlets serving that State or jurisdiction of the breach. This notice will be provided without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the breach.

Notification to the US Secretary of Health and Human Services

Following discovery of a breach, the Privacy Officer shall notify the Secretary of Health and Human Services as stated below.

1. If the breach involves five hundred (500) or more individuals, with one exception, Imagine! will provide the Secretary of Health and Human Services with notice of the breach at the same time as its notice to the affected individuals. The notice will include the same information that is provided to affected individuals and will be provided to the US Secretary of Health and Human Services in the manner specified on the Health and Human Services Web site. The exception is when there is a law enforcement delay pursuant the "Law Enforcement Delay" of this section.

2. If the breach involves less than five hundred (500) individuals, the Privacy Officer will maintain a log or other documentation of such breaches and, no later than sixty (60) days after the end of each calendar year, provide the Secretary of Health and Human Services with notice of breaches discovered during the preceding calendar year in the manner specified on the US Department of Health and Human Services Web site. This log will be kept for six years.

Notification from a Business Associate

When notification is received from a business associate of Imagine! of its discovery of a breach of unsecured PHI, the Privacy Officer shall give notice to affected individuals in accordance with these polices. However, if the agreement between Imagine! and the business associate permits, the Privacy Officer may require the business associate to give such notice.

Law Enforcement Delay

If a law enforcement official states to Imagine! that a notification, notice, or posting required by the "Breach Notification" section of these policies and procedures would impede a criminal investigation or cause damage to national security, the Privacy Officer shall:

1. If the statement of the law enforcement official is in writing and specifies how long of a delay is required, delay the notification, notice, or posting for the time period specified in the writing; or,
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily but no longer than 30 days from the date of the statement, unless a written statement as described in subparagraph 1, above, is submitted during that time.

Any member of Imagine!'s Workforce who is contacted by a law enforcement official in this regard shall immediately refer the official to the Privacy Officer.

Procedures for Investigation of a Reported Breach of PHI

The Privacy/Security Officer shall respond promptly to any security and/or privacy incident. The Privacy Officer and/or Security Officer shall determine if there is a concern regarding a possible violation of HIPAA or Imagine!'s policies or procedures related to HIPAA. If the Privacy/Security Officer determines there is a concern, he/she shall notify the CEO. If the Privacy Officer, Security Officer, or CEO determines an investigation is needed, it shall begin promptly. The Privacy Officer will determine who will conduct the investigation.

If, at the conclusion of the investigation, it is found that a violation of Imagine!'s policy or procedure has occurred, the Privacy Officer will notify the CEO. The Privacy Officer or CEO, in consultation with the Director of Human Resources, will determine what disciplinary actions will be taken. The disciplinary action report documenting the violation shall be placed in the employee's electronic or hard copy personnel file. Documentation of findings and final actions from the investigation shall be maintained as a part of Imagine!'s Privacy records and retained

for six (6) years. The Privacy/Security Officer shall take or direct appropriate action to address the issues identified through the investigatory process.
The Privacy Officer will determine whether any external notifications are required and, if so, the specifics of the required notification pursuant to these policies and procedures and Federal and or State HIPAA rule guidelines.

Prohibition on Intimidating or Retaliatory Acts

Imagine! shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against:

1. Any individual for exercising a right or participating in a process provided for in this policy or in the privacy or security regulations under HIPAA;
2. Any individual who:
    a. Files a complaint with the U.S. Secretary of the Department of Health and Human Services as permitted by the privacy or security regulations;
    b. Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing conducted by a government enforcement agency; or,
    c. Opposes any act or practice made unlawful by the privacy or security regulations under HIPAA, provided that the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the privacy or security regulations under HIPAA or this policy.

Any individual who believes that a form of retaliation or intimidation is occurring or has occurred shall report the incident to the Privacy Officer. The Privacy Officer shall treat such a report as a complaint and investigate it accordingly.

Access, Use or Disclosures That Do Not Constitute a HIPAA Violation or Breach

The procedures outlined in this section do not apply when an individual exercises his/her right to:

1. File a complaint with the Office for Civil Rights, U.S. Department of Health and Human Services pursuant to the HIPAA regulations;
2. Oppose any act made unlawful by the Privacy or Security rules; provided the individual has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy and Security rules;
3. Disclose PHI as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity provided the individual in good faith believes Imagine! has acted unlawfully; or,
4. The individual is the victim of a crime and discloses PHI to a Law Enforcement Officer, provided that the PHI is about a suspected perpetrator of the criminal act and is limited to the information allowed under Federal Law.

Sanctions

Any member of Imagine!'s Workforce who fails to comply with Imagine!'s Privacy and Security Policies and procedures or the requirements of the HIPAA Privacy, Breach Notification and Security Rules shall be subject to sanctions imposed through Imagine!'s discipline and discharge policies. Employees, subcontractors, interns or volunteers shall report coworkers who violate HIPAA Privacy and Security Rules to the Privacy or Security Officer. The Privacy Officer shall cause written documentation of the sanctions that are applied, if any, to be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later.

Procedures for Determining Sanctions for Employees, Subcontractors, Interns, and Volunteers

The sanctions imposed depends on a variety of factors, including, but not limited to, the severity of the violation, whether it was intentional or unintentional, and whether the violation indicates a pattern of improper use, disclosure, or release of PHI.

The degree of discipline may range from a verbal warning up to and including termination of the employment or the relationship with Imagine!. The following levels of violating severity shall be utilized in recommending the disciplinary action and/or corrective action taken:

Level 1: An individual inadvertently or mistakenly accesses PHI that he/she had no need to know in order to carry out his/her responsibilities Imagine!, or carelessly accesses or discloses information to which he/she has authorized access. Examples of violations include, but are not limited to, the following:

a. Leaving PHI in a public area;
b. Mistakenly sending emails or faxes containing PHI to the wrong recipient;
c. Discussing PHI in public areas where it can be overhead;
d. Leaving a computer accessible and unattended with unsecured PHI;
e. Loss of an unencrypted electronic device containing unsecured PHI;
f. Improperly disposes of PHI in violation of Imagine! policy; or
g. Failing to report that his/her password has been potentially compromised (e.g., has responded to email spam and given out their password).

Level 2: An individual intentionally accesses, uses and/or discloses PHI without appropriate Authorization. Examples of violations include, but are not limited to, the following:

a. Intentional, unauthorized access to their own, their friend's, relative's, coworker's, public personality's or other individual's PHI (including searching for an address or phone number);
b. Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual a user name and password to access electronic PHI;
c. Disclosing consumer condition, status or other PHI obtained as an employee, subcontractor, intern or volunteer to a co-worker who does not have a legitimate need to know;

d. Obtaining PHI under false pretenses;
e. Failure to properly verify the identity of individuals requesting PHI which results in unauthorized disclosure, access or use of PHI;
f. Failure to promptly report any violation of Imagine!'s privacy or security policy or procedure to the Privacy or Security Officer;
g. Logging into Imagine! information systems and allowing another individual to access PHI;
h. Connects devices to the network and/or uploads software without having received authority from IT; or
i. Second occurrence of any Level 1 violation (it does not have to be the same offense).

Level 3: An individual intentionally uses, accesses and/or discloses PHI without any Authorization for personal or financial gain; causes physical or emotional harm to another person; or causes reputational or financial harm to Imagine!. Examples of violations include, but are not limited to, the following:

a. Unauthorized intentional disclosure and/or delivery of PHI to anyone;
b. Intentionally assisting another individual to gain unauthorized access to PHI cause harm. This includes, but is not limited to, giving another individual your unique user name and password to access electronic PHI;
c. Accessing or using PHI for personal gain (i.e., lawsuit, marital dispute, custody dispute);
d. Disclosing PHI for financial or other personal gain;
e. Uses, accesses or discloses PHI that results in personal, financial or reputational harm or embarrassment to the person served; or
f. Second occurrence of any Level 2 violation (it does not have to be the same offense), a Level 1 and Level 2 violation, or multiple occurrences of any Level 1 violation.

Procedures for Determining Sanctions for Business Associates

Any level of breach by the business associate and/or its staff or agents shall be addressed by Imagine! in accordance with the terms of the BA Agreement currently in effect at the time of the breach.

Prior to Imagine! disclosing any EPHI information to a business associate or allowing a business associate to create or receive EPHI on its behalf, Imagine! will obtain assurances from the business associate that the business associate will appropriately safeguard the EPHI disclosed to it or that it creates or receives on Imagine!'s behalf. The satisfactory assurance shall be through a written contract with the business associate that contains at least the provisions required by the Privacy and Security Rules.

However, if the business associate is required by law to perform a function or activity on behalf of Imagine! or to provide a service described in the HIPAA Privacy Rule's definition of a business associate to Imaigne!, Imagine! may disclose EPHI to the business associate to the extent

necessary to comply with the legal mandate without meeting the requirements for business associates, provided:

1. Imagine! attempts in good faith to obtain satisfactory assurances, as stated above; and,
2. If that attempt fails, the CFO documents the attempt and the reasons that the assurances cannot be obtained.

Any contract of Imagine! where the other party, or one of the other parties, may be a business associate shall be submitted to the Privacy Officer, Security Officer, and/or CFO for review for compliance with these Privacy and Security Policies and the HIPAA Privacy Rule prior to being signed on behalf of Imagine!.

Transportation and Storage of PHI

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI in any form. All PHI in paper or electronic form must be transported and stored in a secure manner to safeguard it against improper disclosure or loss. PHI will be transported and stored outside secure networks sites and servers only when necessary. Only the minimum amount of PHI necessary to accomplish a task shall be transported.

Procedures for Transportation and Storage of PHI

If it is necessary to transport physical PHI or EPHI in a vehicle, the following precautions will be applied:

1. Employees, subcontractors, interns or volunteers who transport PHI must be aware of the possibility of that vehicle accidents can occur which could provide unauthorized access to items within the vehicle. In addition, vehicles can be inappropriately accessed for the purpose of theft of the contents of the vehicle. In such circumstances PHI could be accessed by unauthorized individuals. Precautions must be taken to prevent or minimize the possibility that PHI will be compromised.
2. Physical PHI transported in a vehicle must be kept in a locked container, or if not available, a briefcase or bag that closes with a zipper, hiding the contents from plain view.
    1. The locked container, briefcase or bag shall be placed in the trunk or another part of the vehicle that is not visible from outside the vehicle. Hard drives will expand and then fail if left in temperatures above 95 degrees. While it is recommended to put documents in the trunk, it is advised that computers/tablets be placed under a seat in the car for short periods during hot weather; and,
    a. If the vehicle does not have a trunk, the locked container, briefcase or bag shall be out of plain sight in the backseat of the vehicle.
    b. PHI shall not be left in an unattended vehicle, except when necessary, and not for any unreasonable length of time.
    c. PHI shall not be left in a vehicle overnight.
3. Employees, subcontractors, interns or volunteers shall only transport the minimum necessary to perform their job duties.

If it is necessary to store physical PHI or EPHI in a location outside a secure location such as an employee's home office, the PHI must be placed in a secure, locked file cabinet or other locked container. Every effort shall be made to keep PHI secured from access by family members and others.

If PHI is lost or stolen, or improperly accessed by others, the employee, subcontractor, intern or volunteer shall notify the Privacy Officer and file a police report if the improper access involved theft.

Employees, subcontractors, interns or volunteers who violate this policy are subject to disciplinary action up to and including termination of employment or contractual relationship.

Violations must be reported by the employee, subcontractor, intern or volunteer's immediate supervisor as soon as possible regardless of whether PHI has been compromised.

Maintenance of Psychotherapy Notes

Hardcopies of psychotherapy notes created by Imagine! Behavioral Health Services shall be maintained by the mental health professional who prepared the notes in a locked file in his or her office. These notes may be archived electronically in a secure document management system with restricted access to employees of the Imagine! Behavioral Health Services department but must at all times remain segregated from any other record; and the use and disclosure must be restricted as required under 45 CFR 164.508 (a)(2). Access by employees who are not the originator of the psychotherapy note is severely limited under HIPAA.

Upon termination of the mental health professional's employment or contract, any psychotherapy notes maintained by him/her shall be destroyed or transferred to a permanent file.

Limited Data Set

Imagine! may use or disclose a limited data set if Imagine! enters into a "data use agreement" with the limited data set recipient. Prior to Imagine! using or disclosing any PHI as part of a "limited data set," both the limited data set and the data use agreement must be approved by the Privacy Officer. A limited data set may be used and disclosed only for the purposes of research, public health, or health care operations. Imagine! may use PHI to create a limited data set or disclose PHI to a business associate of Imagine! for that purpose, whether or not the limited data set is to be used by Imagine!.

A "limited data set" is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

a. Names;
b. Postal address information, other than town or city, State, and zip code;
c. Telephone numbers;
d. Fax numbers;
e. Electronic mail addresses;
f. Social security numbers;
g. Medical record numbers;
h. Health plan beneficiary numbers;
i. Account numbers;
j. Certificate/license numbers;
k. Vehicle identifiers and serial numbers, including license plate numbers;
l. Device identifiers and serial numbers;
m. Web Universal Resources Locators (URLs);
n. Internet Protocol (IP) address numbers;
o. Biometric identifiers, including finger and voice prints; and
p. Full face photographic images and any comparable images.

Data Use Agreement

A data use agreement between Imagine! and the limited data set recipient must:

1. Establish the permitted uses and disclosures of the limited data set by the recipient. The data use agreement may not authorize the recipient to use or further disclose the information in a manner that would violate the requirements of these policies or the HIPAA Privacy Rule if done by Imagine!;
2. Establish who is permitted to use or receive the limited data set; and,
3. Provide that the limited data set recipient will:
    a. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    c. Report to Imagine! any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

d. Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and,
e. Not identify the information or contact the individuals.

If Imagine! knows of a pattern or practice of the recipient that constitutes a material breach or violation of the data use agreement, Imagine! will take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful:

1. Discontinue disclosure of PHI to the recipient; and,
2. Report the problem to the Secretary of Health and Human Services.

Policies for the Security of Electronic Protected Health Information (EPHI)

Imagine! implements procedures to protect electronic protected health information (EPHI) and for controlling access to EPHI. The Security Officer shall oversee and be responsible for implementing procedures designed to prevent, detect, contain, and correct any security violations.

Administrative Safeguards

Security Risk Analysis

The Security Officer shall periodically perform a thorough and accurate security risk analysis to assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by Imagine!. The analysis shall be documented in written or electronic form and maintained for six (6) years from the date it was created or superseded by a newer analysis, whichever is later.

Security Measures

The Security Officer shall implement security measures appropriate to reduce the risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level. These measures shall be documented in written or electronic form and maintained for six (6) years from the date it was created or superseded by a newer analysis, whichever is later.

Sanction Policy

Any member of Imagine!'s Workforce who fails to comply with Imagine!'s security policies and procedures or the requirements of the HIPAA Security Rule shall be subject to sanctions imposed through Imagine!'s discipline and discharge policies.

Information Systems Activity Review

The Security Officer shall verify that hardware, software, or procedural mechanisms are implemented in order to record and examine activity in Imagine!'s information systems that contain or use EPHI. See Procedure for Audit Controls.

Workforce Security and Access

Imagine! will ensure the supervision of its workforce. Imagine! shall implement procedures to ensure all members of its Workforce have appropriate access to EPHI. Furthermore, Imagine! shall implement procedures to ensure that Workforce members who are not authorized to access EPHI are unable to do so. See Procedure for Information Access Establishment and Modification.

Security Incident

Employees, subcontractors, interns or volunteers who believe that unauthorized access, use or disclosure of EPHI has occurred shall immediately report the circumstances of the suspected breach to their supervisor and the Security or Privacy Officer. Staff shall also report if they detect evidence that a security incident may be imminent. Imagine! staff shall report any suspected breach of unsecured EPHI to the Security or Privacy Officer as soon as possible, within 48 hours

after knowledge of the incident. See the Incident Response and Reporting Procedures for Imagine!'s response to security incidents.

Business Associates

Refer to page 64, Business Associates, for Business Associate agreement guidelines.

Physical Safeguards

Imagine! implements procedures for the use of physical safeguards designed to protect its information systems and facilities from unauthorized entry, natural disasters, and environmental hazards.

Procedures for Safeguarding PHI when Using Portable Devices and Media

A. Workforce members shall limit the use of assigned portable computers and tablet devices or any Imagine! provided resource or device that contains or can access client EPHI, to Imagine! staff only.
    1. Imagine! issued portable devices shall have appropriate password, security, and encryption programs installed upon them. Any EPHI that is accessed from a portable device shall have adequate disk encryption as approved by the Privacy/Security Officers.
    2. Workforce members shall avoid accessing EPHI where it might be seen by persons without a legitimate need to know.
    3. Smart Phone users shall be sure to close connections to email and other systems/portals that contain PHI immediately when they are finished using the system/portal.
    4. If necessary, the Security Officer, or his/her or her designee, provides Workforce members with accessories to protect their portable computers and tablets, and requires use of these devices.

B. Workforce members shall only log in to systems and portals for which they have authority and properly obtained valid access credentials.

C. Workforce members shall not store EPHI on flash drives (thumb drives) or other removable media or memory devices unless absolutely necessary and only on devices approved by the Security Officer. When using removable media or memory devices is absolutely necessary, employees, interns or volunteers shall:
    1. Ensure that the flash/thumb drive is encrypted.
    2. When not in use, keep the flash/thumb drive on their person or securely stored.
    3. Not leave an external drive or other removable media or memory device attached to a computer. (Many removable drives and media devices are lost because their owners transferred a file to the device for a presentation and then forgot the flash drive at the end of the presentation.)
    4. Not store older documents on removable media; they shall be archived to Imagine!'s network. Removable media shall contain what is needed in the immediate future.

D. The Security Officer (or his/her designee) maintains a current list of Imagine! issued portable computer and tablet users, assigned equipment serial numbers and software. Imagine! holds the portable computer or tablet user responsible and accountable for the safety and security of the assigned equipment and information.

E. Workforce members shall secure Imagine! issued portable computers and tablets when equipment is left unattended in offices and meeting rooms.

F. Privacy and security training shall emphasize that flash drives and other removable media and memory devices such as PDAs and Smart Phones are easy to lose or misplace and that if the drive, media or device contains EPHI, its loss or misplacement can create a serious data breach issue.

G. The Security Officer shall perform loss investigations on stolen equipment.

Procedures for Safeguarding PHI when Using Mobile Devices

A Mobile Device includes cellular telephones, watches and tablets. Mobile devices that are used to access company data must comply with Imagine!'s *Bring Your Own Device Policy and Procedures*. Reference that policy and procedures for security safeguards and expectations.

Workforce members shall not transmit any EPHI over text message to persons served, their parents or legal representatives, or other Imagine! co-workers unless the *Request for Non Secure Communications* is completed by the person served, their parents or legal representatives.

A. Imagine! allows its employees to use mobile device cameras to take pictures of documents containing PHI as an alternative to scanning or making a copy. Pictures of documents containing PHI must be promptly sent via secure email and deleted from the mobile device. Phones set up to automatically back up certain files (e.g. photos) to cloud services shall be disengaged.
B. Workforce members are permitted to exchange text messages with persons served and their parents or personal representatives to confirm appointments or other communications that do not include EPHI. The use of initials to reference persons served is required when text messaging or using unsecure email.

Procedures for Tracking Computer Hardware Assets

Imagine!'s IT department will maintain an inventory database of hardware assets. This will be updated in real-time as new hardware is placed into service and old hardware is removed from service. When necessary, a physical inventory of department's assets will be done to maintain database accuracy.

Technical Safeguards

Procedure for Terminating an Employee's Access Upon Separation from Imagine!

Purpose: The purpose of this procedure is to ensure that when a member of Imagine!'s workforce is terminated, for any reason whatsoever, that his or her ability to access electronic protected health information is terminated.

Responsible Party: The Human Resources Director or designee shall be responsible for ensuring these procedures are followed when a member of Imagine!'s workforce is terminated for any reason whatsoever.

I. Recovery of Items

When an individual's employment with Imagine! ends, the Human Resources Director or designee shall collect from the employee all keys, bus passes, computers, electronic keys (fobs), cell phones and any other company issued equipment. This shall be verified by using the exit interview checklist.

In the event items are not recoverable, appropriate action will be taken to render them inoperable. This could include changing physical locks, deactivating electronic keys and key cards and remote wiping cellular phones.

II. Remove Computer Access

Additionally, the employee's supervisor or Human Resources Department shall inform an Information Technology systems administrator or designee that the employee no longer works at Imagine! and that all accounts for that employee should be closed. The Information Technology systems administrator or designee will remove all accounts for the former employee within eight (8) hours of notification. For any accounts to which the employee had passwords that cannot be closed, Information Technology systems administrator or designee shall change the passwords immediately.

Revised: 7/2008, 3/2015, 10/2018

Procedure for Authorizing Employee Access to Electronic Protected Health Information

Purpose: The purpose of this procedure is to ensure that Imagine!'s employees are only authorized to access the minimum amount of electronic protected health information necessary for them to perform their job duties.

Responsible Party: Imagine!'s Security Officer is responsible for ensuring that this procedure is followed.

I. Authorizing Employee Access to EPHI

Every employee who has a need to access EPHI in order to perform his duties as an employee of Imagine! must first be authorized to access EPHI by their supervisor or department director. The Information Technology Director or Systems Administrator shall ensure that each employee's access to EPHI is the minimum necessary to perform his duties.

When authorizing access to EPHI, Information Technology Director or Systems Administrator shall refer to the job descriptions and informational needs that Imagine! created as part of its Privacy Rule Compliance. The Security Officer shall determine which information described therein is Electronic Protected Health Information. The employee's supervisor or department director shall then authorize the employee to access that EPHI.

See also the Procedure for Information Access Establishment and modification.

Revised: 1/2014

Procedure for Information Access Establishment and Modification

Purpose: The purpose of this procedure is to ensure that after an employee of Imagine! is granted access to electronic protected health information, the authorized level of access is implemented and that, as employees' duties and responsibilities change, their level of access is appropriately modified.

I. Access Establishment

After the Security Officer determines the minimum necessary EPHI that an employee needs to access to perform her job, the Security Officer shall notify Information Technology Director or designee of the authorized access.

The Information Technology Director or designee, or department director or designee shall then establish the employee's access to that EPHI on Imagine!'s information systems. Access shall be established by instituting the appropriate accounts and account permissions on Imagine!'s information systems.

II. Access Modification

When an employee changes positions within Imagine!, or for some other reason his or her needs for access to EPHI change, the employee's supervisor or department director shall notify the Information Technology Director or designee. Information Technology Director or designee, or department director or designee shall then review the employee's needs for EPHI and revise the employee's authorization accordingly. The employee's previously established access will also be modified as necessary at this time.

III. Access Revocation

When an employee leaves the employ of Imagine!, for any reason whatsoever, the employee's supervisor, department director or human resources department shall notify the Information Technology Director or designee. The Information Technology Director or designee shall immediately revoke the employee's authorization to access EPHI. In the case of information systems where the employee's supervisor or department director manages access to systems containing EPHI, they shall immediately revoke the employee's authorization to access EPHI in those systems. Revoking employee's access includes immediately removing all accounts and other points of access that the employee used. In the case of any publicly known passwords, those passwords shall be changed immediately as well.

If the termination of the employee is suspected to lead to litigation, the Information Technology Director or designee will place the employee's email account on litigation hold, change and record the user's active directory password and only remove the users

account when the Human Resources department instructs the Information Technology department to do so.

IV. Application Access Matrix

Application access shall be governed by the Application Access Matrix. While there will be circumstances of individual deviations from this matrix, the Security Officer, Information Technology Director or designee shall make the determination as to when those deviations are appropriate and ensure they are applied accordingly.

Revised: 7/2007, 3/2011, 8/2017, 10/2018

Procedure for Security Awareness and Training

Purpose: The purpose of this procedure is to ensure that members of Imagine!'s workforce receive appropriate training regarding Imagine!'s security policies and procedures.

Responsible Party: The Security Officer is responsible for ensuring that Imagine!'s workforce members are trained in accordance with these policies and procedures.

I. Security Training Responsibility

The Security Officer shall be responsible for designing and implementing Imagine!'s training program. The Security Officer and Human Resources Director or designee shall be responsible for training members of Imagine!'s workforce in conformance with the following Security Training Procedures.

II. Training Timeframes

a. Initial Training

The Security Officer shall ensure that all workforce members receive security training prior to April 20, 2005.

b. New Employees

The Human Resources Director or designee shall ensure that all new workforce members receive security training within thirty (30) days of hire date.

c. Training in the Event of a Material Policy or Procedure Change

In the event of a material change in Imagine!'s Security Policies or in the HIPAA Security Regulations, the Security Officer shall ensure that the affected members of Imagine!'s workforce receive training on these changes. This additional training shall occur within thirty (30) days from the date of the change and no later than the effective date of the new Policies or Regulations

III. Training Goals

Imagine!'s security training shall be designed to make each member of the workforce aware of the need for information security and his role in maintaining information security. The training shall familiarize each member of the workforce with the requirements of the HIPAA Security Rule and Imagine!'s Security Policies and Procedures.

IV. Remedial Training

If a member of Imagine!'s workforce has been involved in a security incident that was not the result of malicious or willful conduct, the Security or Privacy Officer shall provide the

offending individual with additional training regarding Imagine!'s Security Policies and Procedures. This training will focus on the areas directly related to the incident and shall be designed to prevent a recurrence of the incident.

V. Training Reminders

In order to ensure ongoing compliance and information security, the Information Technology Director or designee shall provide security reminders to members of Imagine!'s workforce. These reminders shall be provided on an as needed basis. These reminders will be provided by e-mail for all employees with an account and interoffice memorandum to be posted at work sites with employees who do not have an e-mail account. These reminders will focus on practical security issues, such as handling passwords, dealing with e-mail attachments, etc.

In the event of a security incident, the Security Officer shall issue a training reminder to all members of Imagine!'s workforce that focuses on the security issue involved in the incident and how to avoid it in the future. If the Security or Privacy Officer becomes aware of recurring security lapses, the Executive Director or Information Technology Director shall issue a reminder to all members of Imagine!'s workforce regarding the lapse and the appropriate way to handle the issue in light of Imagine!'s policies and procedures.

Revised: 10/2011, 10/2018

Procedure for Protection Against Malicious Software

Purpose: The purpose of this procedure is to ensure that Imagine!'s information systems are protected against malicious software. Ultimate responsibility for compliance with all listed procedures is the responsibility of the Security Officer.

I. Anti Virus Software

The Information Technology department shall ensure that all Imagine! workstations that can access EPHI have an Antivirus software installed. This software shall be configured to automatically scan all local disks, and any other files downloaded onto the workstation or any electronic media connected to the workstation and detect and remove any malicious software. The Information Technology department shall ensure that this software is regularly updated, has the most current virus definitions, and has the most current patches installed.

II. Internet Firewall

The Information Technology Director or designee shall ensure that Imagine! has a firewall program or appliance installed between the Internet and its local area network. This firewall shall be configured to allow members of Imagine!'s workforce to use the Internet in conformance with Imagine!'s polices and procedures on Internet usage, but should prevent unauthorized access to Imagine!'s network from the Internet. The exact configuration of the firewall will be determined by the Information Technology Director or designee.

III. E-mail Security Appliance

The Information Technology Director or designee shall ensure that Imagine! has a security program or appliance installed between the Internet and its internal e-mail server. This program or appliance will filter all incoming and outgoing e-mail messages for SPAM content, forbidden attachments and scan all messages and attachments for viruses.

IV. Other Procedures

Downloaded software

All software downloaded from non-Imagine! sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the

Internet, and a considerable amount of its information is outdated or inaccurate.

Reporting

Any employee that believes he/she has intentionally or inadvertently downloaded or otherwise caused malicious software to be installed or saved to their workstation or any shared network drive must notify the Information Systems department immediately.

Revised: 3/2008, 6/2018

Procedure for Log-In Monitoring

Purpose: This procedure is designed to ensure that monitoring of log-in records for applications and networks used by members of Imagine!'s workforce is done to the best possible extent.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

I. Log-In Monitoring

The Security Officer shall designate members of the Information Technology staff to assist in application of this procedure. Any information system or application used by members of Imagine!'s workforce that contains EPHI and allows for the tracking of log-in history shall be reviewed by a designated member of the Information Technology department. In addition to applications, the log-in records of the network directory tree shall also be reviewed.

In the event the Information Technology department discovers a discrepancy, the employee discovering the discrepancy shall notify the Security Officer who shall then take steps in accordance with Security Incident Responses Procedures.

The period of this review shall be as needed or at least every three months.

Revised: 8/2010, 10/2018

Procedure for Password Management

Purpose: This procedure is designed to ensure that passwords used by members of Imagine!'s workforce to authenticate themselves on Imagine!'s information systems are maintained in a manner that reduces the risk of unauthorized entry into Imagine!'s information systems.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

I. Password Requirements

Imagine!'s information systems shall use passwords to authenticate individual users. Information systems include individual applications that contain EPHI and access to the network directory tree. Each user will be assigned or create a unique password. A password must be at least ten characters long and contain characters from three of the following four character types; uppercase letters, lowercase letters, numbers or symbols. The Information Technology Director or Systems Administrator shall configure Imagine!'s information systems to only accept passwords that meet the above criteria.

The Information Technology department shall assign each user a password when the User's account is created. This will be a temporary password and the user will be instructed to change it when logging in for the first time. The Information Technology department shall provide the password to the user by voice mail, interoffice memo or in person. The user shall be allowed to modify or change their password at any time.

II. Password Expiration and Renewal

A User's password is valid for 182 days from the date of creation. After that time, the user shall choose or be assigned (depending on the information system in question), a new password. The Information Technology department shall configure Imagine!'s workstations to stop accepting a password after it has been in use for 182 days. The Information Technology department shall configure the system to notify the user that their password will be expiring. The user shall be responsible for creating a new password that conforms to Imagine!'s password policies.

If a user is denied access to the system, because the user failed to create a new password during the user's grace log-in period, the user shall notify the Information Technology department who will then verify the user's access should remain active, reactivate the user's access, and assign the user a new password.

After a user's password expires, the user shall choose a new password. This password should meet Imagine!'s procedures governing password management.

All information systems that have the capability of notifying the user a password change is necessary will be configured to do so. For systems that do not have this feature, the Information Technology department will send out a reminder to employees that a password change is needed.

III. Safeguarding Passwords

Users shall not write passwords down anywhere around their workstations. Users shall not share passwords with other users.

Users should never disclose their passwords in an e-mail, neither should anyone providing technological support for Imagine! requesting a member of Imagine!'s workforce disclose a password over email.

Revised: 7/2010, 1/2014, 7/2015, 3/2018

Procedure for Incident Response and Reporting

Purpose: The goal of this procedure is to ensure that Imagine! responds to security incidents in an appropriate manner.

Responsible Party: Imagine!'s Security Officer is responsible for ensuring that members of Imagine!'s workforce follow these procedures.

I. Preparation

A. The Security Officer shall ensure that the security of Imagine!'s information systems is maintained at a reasonable and appropriate level. This shall be handled by following Imagine!'s procedures for evaluating the security of its information systems outlined in Imagine!'s HIPAA Privacy and Security Policies and Procedures.

B. Because training is important to ensure that procedures are followed, the Security Officer shall ensure that Imagine!'s security training program includes training employees on how to report and respond to a security incident.

II. Detection

A. The Information Technology Director or designee shall be the central point of contact for incident reporting. When a member of Imagine!'s workforce determines that a security incident has occurred, or detects evidence that a security incident may be imminent, that person shall notify the Information Technology Director or designee. The person notified shall then implement Imagine!'s Security Incident Response Procedures.

B. The Security Officer shall be contacted by cell phone if an incident should occur when response personnel are not regularly in the office.

III. Analysis

A. Upon detection of a security incident, the Security Officer shall immediately begin efforts to determine the nature, scope, and source of the incident. The Security Officer shall also endeavor to determine the potential harm from the incident including information at risk and the level of risk presented.

IV. Containment

A. The Security Officer shall work with department directors, managers and pertinent personnel to determine parameters for containment. These parameters shall be used by the Information Technology department to determine when to begin containment procedures. Once the Security Officer has determined the nature and scope of the incident, this information shall be used, in conjunction with the containment parameters, to determine an appropriate containment strategy and when that strategy should be implemented.

B. Once the Security Officer determines that containment shall begin, the Information Technology department shall immediately take steps to isolate those systems that have been affected or compromised by the incident from the rest of Imagine!'s information systems.

C. The affected or compromised systems shall remain isolated until the incident is resolved.

V. Eradication

Upon the identification of a security incident, the Information Technology department shall begin eradication procedures as soon as possible.

VI. Recovery

A. After the Security Officer is certain that the security incident has been resolved, the Information Technology department shall investigate whether EPHI was lost or altered as during the incident. If the Information Technology department determines that EPHI was lost or damaged, the Information Technology department shall determine the extent of loss or alteration to EPHI and shall restore lost or damaged information according to Imagine!'s procedures for Data Recovery.

B. In the event the Security Officer determines that electronic protected health information was disclosed during the incident, the Security Officer shall ensure that the information regarding the disclosure is recorded according to Imagine!'s polices and procedures for documenting disclosures for which Imagine! must account to the individual.

C. The Security Officer shall take steps to mitigate the harm from the security incident by following Imagine!'s mitigation procedures.

1. The Security Officer shall document the occurrence of the security incident. This documentation shall include, date of the incident, extent of the incident, duration of the incident, response to the incident, and any other pertinent information that he or she determines is necessary for future reference or any reporting require.

VII. Reassessment

Following the aftermath of an incident, the Security Officer or designee will reassess the risks and vulnerabilities associated with the incident with special attention given to the systems or processes involved. Based on this assessment, a determination will be made if changes are necessary to IT systems or staff training to minimize the risk of a reoccurrence for the same reasons.

Revised: 3/2008, 8/2011, 10/2018

Incident Response Planning Checklist

I. Personnel Qualifications

- Are information technology issues handled internally or externally?

Internal IT capability:

- Are IT issues handled by an individual or department?
- In either case, does your organization's information technology department respond to all incidents or are some incidents handled externally?
- Does the department feel that they have a sufficient level of technical understanding to adequately respond to security incidents?
- Does the department feel that they have the resources, including time, available to adequately respond to security incidents?

External IT Capability:

- Are IT issues handled by a contractor or through your vendor?
- If through an external contractor, discuss with your IT consultant whether they can provide an incident response capability.
- If your IT issues are handled by your vendors, it is unlikely they can provide a comprehensive incident response capability. If not, you will either need to find an employee or employees to handle incident response, or begin researching IT contractors. You might try talking to your vendors and to any trade associations in order to obtain recommendations.

II. Preparation

- Part of your preparation will be documented in your training procedures re: educating the employees.
- Part of your preparation will involve your ongoing evaluation of your Security Policies and Procedures.
- Part of your preparation will involve your decision regarding how to handle security incident response-in house/out of house.

A. In house response

- Response personnel need to keep their technical skills sharp. Your procedures and policies will need to include training for these individuals. Part of this will be practicing responses part will be attending seminars so that they keep old skill sharp and learn new skills as technologies change.

This is similar to the ongoing training that nurses and professionals are required to undergo.

B. Out sourced response

- Depending upon the terms of your outsourcing agreement, you may retain responsibility for such things as keeping software and virus definitions up-to-date, evaluating and improving security, training, etc. Be certain that your contract clearly delineates responsibilities.

- If you are outsourcing incident response, you will need a business associate agreement that includes the security rule provisions.

- When evaluating security contractors, inquire about their technical expertise and ongoing training. You would keep your employees sharp, so you should make sure your contractor does the same.

III. Centralized Communications

Reporting

- Regardless of whether incident responses are handled internally or externally, you will need a means for members of your workforce to report incidents. This means you will need an on-site point of contact.

- Do you have a current point of contact for IT issues, i.e., a help desk (or IT person)?

- Do you need a twenty-four hour response capability? In other words, do employees usually work after hours? Is your help desk available twenty-four hours a day?

- If you have a help desk/person, it might be simplest to make them the response point of contact. This makes it easier for employees to report incidents.

- If your help desk personnel are not also your response personnel, you will need to have clear procedures for the help desk to use to contact the response personnel.

- If your response capabilities are handled by a contractor, be sure that your agreement clearly states how they are to be contacted when an incident happens—phone numbers, central contact personnel, etc. You will likely have a central point of contact for your employees. Response time is obviously critical, but it is more practical to have the help desk or your internal support staff handled contacting the incident response team. You may be able to contract with them for help desk-type support, but most likely, they will be there to provide the

additional response capabilities while you will handle regular administration and support internally.

IV. Disseminating Information Back to Personnel

- Are all employees on the office network? Do all employees have e-mail?
- If yes, the response team can most easily update the members of your workforce via e-mail.
- If not, what method does your organization currently use to distribute information to the entire workforce? This method can be adopted for your response team.
- Again, when you are outsourcing your incident response, be sure the agreement states how they will notify your organization of the progress of the incident and the response. Will they have a capability to notify everyone or will you also have a central point of contact who will receive updates from them and then update your organization. The latter seems like a better option.

V. Detection and Analysis

- Incidents will be detected a number of different ways. For example, an employee may detect an incident because a virus infects her computer. The person who has responsibility for reviewing audit logs may detect evidence of an unauthorized intrusion in one of the logs.
- If you hire a contractor to provide incident response capabilities, they will likely be able to provide incident detection services as well. Because some companies are managed security companies, they can provide network security services. These services would put them in a position to detect incidents as well. You should discuss with your contractor whether they will be an "on call" response or be able to detect and respond without a call or if there are some things they will detect, but others you will need to notify them about. In the latter case, it may be simple to always call, rather than trying to distinguish between types of events.
- It is important that all employees understand who to contact. For employees outside of the IT department, it may not be important to understand that concept of a security incident as much as they understand to report viruses or unauthorized access.
- The person/department/contractor who is handling incident response will be primarily responsible for analysis as well. Analysis is where the response personnel determine the nature and scope of the incident. This allows them to determine an appropriate response.

VI. Containment

- The main decision here is whether to immediately contain an incident or allow it to continue in order to develop additional evidence about the incident.

- That decision will usually be based upon the perceived threat from the incident. Obviously, if an incident poses the threat of major harm, containment should begin immediately.

- One way to approach this is to set parameters in advance as to what acceptable risks are. These parameters should be set in consultation with the departments that depend upon the information in question. These parameters are especially important if incident response is handled externally. The contractor should always respond to you.

- The actual containment strategies will vary depending upon the nature of the incident. The response personnel or IT personnel will need to decide upon the actual methodologies.

VII. Eradication

- Again, this stage will be the primary responsibility of the response personnel. Methods and strategies will differ from incident to incident.

- One example of eradication is running a disinfectant program on a computer that has a virus.

- Obviously, the provider will prefer to have the incident eliminated as soon as possible.

VII. Recovery

- Once the source of the incident has been eliminated, who will be responsible for recovery?

- Who is responsible for backing up EPHI? Do you have an outside contractor who performs your backups or do staff members handle this? If it is an outside contractor, are they responsible for restoring data? What responsibilities, if any do you have in conjunction with the contractor?

- The covered entity may be responsible for Recovery. If so, I recommend simply making it clear in your Incident Response procedures that recovery should be handled according to Security Rule Recovery procedures.

Revised: 10/2011, 10/2018

Contingency Plan Procedure

Purpose: This procedure is designed to ensure that Imagine! has implemented policies and procedures to ensure the availability of EPHI in the event of any emergencies that may damage systems containing EPHI. These emergencies include, but are not limited to; systems crashes, virus attacks, hardware failures, fires, natural disasters and malicious attacks on Imagine! property.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

1. Data Backup Plan

Backups of critical network data will be done on a daily basis. Snapshots of server operating systems will be done monthly. Current backups will be maintained at all times. This is to ensure against data loss.

Data storage will be maintained on as well as off-site. In the case of removable media, storage will be in the fireproof safe located in the server room. Off-site storage will be with an approved cloud storage provider.

There will be complete backups done on a nightly basis, and there will be random backups performed during the workday. The random backups will mainly be done by special request, i.e. accounting department before closing quarters, specific database backups done before database updates, etc.

2. Data Recovery Plan

A. Do Network Operating Systems need to be re-installed?

If servers require reinstallation of operating systems please make sure either the Information Technology Director or System Administrator performs the task. These tasks require very specific methods of installation. If there is no one available you may contact any of the people on the EMERGENCY CONTACT List that will be located inside the cover of the Backup Log for assistance.

B. Do only data files need to be restored?

1. If the data or file can be recovered from the network shadow copies that are done throughout the day then this is the most convenient method of restoration.
2. If the data or file cannot be recovered via shadow copies, they can be restored from the local backup system and nightly backups.
3. If the data or file cannot be recovered via shadow copies, and the local system copy is not appropriate, they can be restored from the off-site cloud storage.

3. Emergency Mode Operation Plan

Definition

"Emergency Mode" will be any interruption in normal business operations which disrupts the availability of EPHI to the extent that consumer health and safety is in jeopardy.

In-House Emergencies

Any disruptions that can be managed without having to relocate from the current central offices at 1400 Dixon Ave. and 1665 Coal Creek Dr. will be considered in-house emergencies. These include, but are not limited to; power outages, hardware failures, software failure or corruption and virus intrusions. Since preparation for all foreseeable emergencies would be too exhausting, general systems will be put in place to ensure any incident can be mitigated in the most efficient way possible. Some preparations include:

- UPS power backup for critical systems
- Following the Data Backup procedures
- Ensuring replacement hardware is available
- Ensuring original installation disks are available for applications and operating systems

In the event the emergency exceeds the capacity of the Information Technology department expertise, outside technical assistance will be brought in to mitigate the emergency.

Relocation Emergencies

Disruptions that cannot be managed without having to relocate from the current central offices at 1400 Dixon Ave. and 1665 Coal Creek Dr. will be considered relocation emergencies. These would include any natural disaster, fire or other incident that made the occupation of the central office impossible for any length of time. Any situation that could not guarantee the security and access of EPHI would also be considered a relocation emergency. All data should be recoverable to at least the previous nights backup. If new hardware is required due to total or partial loss of needed systems, purchase of the fastest possible replacement should occur as soon as possible. Any systems that can be relocated should be.

Locations that will be utilized in the event relocation is necessary are, in order of priority:

1. A suitable group home with enough room for business office operations. Currently the basement of the Bob and Judy Charles Group Home in Boulder.
2. Basement of the Charles Family Group Home in Longmont
3. Rental property in the Boulder/Lafayette area
4. Available office space at the Developmental Disabilities Resource Center in Lakewood

If habitation of the central office locations cannot occur for some time, a suitable rental location that can house as many departments as possible should be sought out. It may be necessary to find several locations for different departments.

Revised: 11/2007, 3/2010, 1/2014, 3/2018

Procedure for Facility Access Controls

Purpose: This procedure is designed to ensure that the physical security of all Imagine! facilities is maintained.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

1. Facility Security Plan

Physical access to Imagine!'s central office and any other office will be controlled by the issuance of keys or electronic key fobs to outside doors. The Executive Assistant or designee will govern issuance of physical keys. The Information Technology Director or designee will govern the issuance of electronic key fobs. In the case of the central offices, employees will receive a key fob. Other employees as needed may be issued physical keys. In the case of any satellite office, the department director or manager overseeing that location shall identify the appropriate personnel who need access and issue keys as needed. The issuing entity will document all keys issued.

All external doors to facilities are to be kept locked during business hours unless employees inside the location can monitor them. All external doors are to be locked after business hours.

In the case of residential properties that serve clients, issuance of keys will be governed by the department director or supervisor of that location. Since these locations are home to individuals we serve, staff will lock the premises whenever deemed necessary by their specific situation.

2. Access Control and Validation

Facility access control for employees is done by issuance of only the keys needed to perform their assigned duties. Visitors to any facility shall be escorted by an employee that has appropriate access to the areas the visitor needs to visit.

Revised: 3/2008, 6/2018

Procedure for Workstation Use

Purpose: The purpose of this procedure is to ensure that the confidentiality, integrity, and availability of electronic protected health information by describing the appropriate use of all workstations that contain or that can access Imagine!'s electronic protected health information.

Responsible Party: Imagine!'s Security Officer is responsible for ensuring that members of Imagine!'s workforce follow these procedures.

GENERALLY

Members of Imagine!'s workforce should use any desktop, laptop, tablet or other hardware capable of running applications, herein referred to as workstations, that access protected health information in compliance with these policies and procedures.

ENFORCEMENT

Violation of these Workstation Use policies shall be punished according to the Sanctioning policy outlined in Imagine!'s *HIPAA Privacy and Security Policies and Procedures.*

POLICIES

Members of Imagine!'s workforce should use their workstations to access only the electronic protected health information which they have been authorized to access and to which they have been granted access. Furthermore, members of Imagine!'s workforce should only use their workstations to perform job related tasks.

Location

When placing a workstation or monitor in an office, the member of Imagine!'s workforce should place the monitor so that it cannot be viewed from a vantage point outside of an employee's office. Preferably, the monitor should be placed in a position where only the employee can view it. Workforce members should consider factors such as location of windows and doors and sightlines from these points.

E-Mail

1. **Company property**

   As a productivity enhancement tool, Imagine! encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Imagine!, and are not the property of users of the electronic communications services.

2. **Authorized usage**

   Imagine! electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as it does not consume more than a trivial amount of resources, interfere with staff productivity or preempt any business activity.

Users are forbidden from using Imagine! electronic communications systems for private business activities. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

3. Default privileges

Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. For example, end users must not be able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of the IT department has been obtained.

4. User separation

These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user-IDs and associated passwords to isolate the communications of different users. All Imagine! staff and authorized contractors have unique usernames and passwords to access the e-mail system.

5. User accountability

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms.

6. No default protection

Employees are reminded that Imagine! electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. Any email sent outside of the Imagine! domain and containing PHI must be sent encrypted, unless the *Request for Non Secure Communications* form is completed.

7. Respecting privacy rights

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. Imagine! is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

The computers and computer accounts given to users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the computer system.

8. No guaranteed message privacy

   Imagine! cannot guarantee that electronic communications will be private. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allow authorized IT department employees to access and review all materials users create, store, send, or receive on the computer or through the Internet or any other computer network. Personal information could and may be deleted.

   Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Furthermore, others can access electronic communications in accordance with this policy.

9. Regular message monitoring

   It is the policy of Imagine! NOT to regularly monitor the content of electronic communications. However, Imagine! has the right, but not the duty, to monitor any or all aspects of its computer system, including, but not limited to, e-mail sent and received by users. The content of electronic communications and the usage of electronic communications systems may be monitored to support operational, maintenance, auditing, security, and investigative activities. Users understand that Imagine! may use automated software to monitor material created, stored, sent or received on its computer network.

10. Statistical data

    Consistent with generally accepted business practice, Imagine! collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, IT staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

11. Incidental disclosure

    It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels (department director, executive director, etc.).

12. Message forwarding

    Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Imagine! sensitive information must

not be forwarded to any party outside the company without the prior approval of a department director or executive director.

13. Purging electronic messages

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. Unless directed to the contrary by your supervisor, inactive e-mail should be discarded after 30 days. Imagine!'s email policy will automatically delete messages from the inbox, sent and deleted folders after six months. If Imagine! is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the executive director or designated representative has communicated that it is legal to do so.

Internet Use

1. Introduction

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes Imagine!'s official policy regarding Internet security. It applies to all users (employees, contractors, temporaries, etc.) who use the Internet with Imagine! computing or networking resources, as well as those who represent themselves as being connected in one way or another with Imagine!. All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the IT director.

2. Downloaded software

All software downloaded from non-Imagine! sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

3. Information protection

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, Imagine! confidential, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. Most web sites will use a secure, encrypted page when the user is expected to submit sensitive information. The user should ensure that the website they are accessing uses transport layer security (TLS) or secure sockets layer (SSL) as an encryption protocol.

Imagine! documentation and all other types of internal information must not be sold or otherwise transferred to any non-Imagine! party for any purposes other than business purposes expressly authorized by management.

4. Resource usage

   Imagine! management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not company, time. Likewise, games, news groups, and other non-business activities must be performed in such a manner so as not to affect productivity.

5. Public representations

   Staff may indicate their affiliation with Imagine! in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address. In either case, whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of Imagine!.

   Staff must not publicly disclose internal Imagine! information via the Internet that may adversely affect the company's customer relations or public image unless the approval of the department director or executive director has first been obtained.

6. Access control

   All users wishing to establish a connection with Imagine! computers via the Internet must authenticate themselves at a firewall before gaining access to the internal network. This authentication process must be done via a virtual private network system approved by the IT director.

   Unless the prior approval of the IT director or designated staff has been obtained, staff may not establish Internet or other external network connections that could allow non-Imagine! users to gain access to company systems and information. These connections include the establishment of multi-computer file systems, virtual private network, Internet home pages, FTP servers, and the like.

7. Employee responsibilities

   Imagine! is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even

innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk.

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as bulletin boards, newsgroups, or chat groups) or displayed on or stored in Imagine!'s computers. Users viewing or receiving this kind of material should immediately report the incident to their supervisors.

Hosting a Website from a Workstation

Members of Imagine!'s workforce shall not create websites that are either hosted by Imagine!'s computers or accessed through Imagine!'s network.

Settings and Administration

The Information Technology department shall ensure that each workstation requires a username and password to gain access. For workstations that are shared by members of Imagine!'s workforce, each individual user shall have a unique username and password.

Saving Files

Members of Imagine!'s workforce shall not save files containing EPHI to an unencrypted workstation drive. If an encrypted local drive is not available, all files shall be saved to an appropriate directory on the main file server or approved Internet storage site.

Virus Protection

The Information Technology department shall ensure that each workstation has a software program installed designed to intercept, detect, and remove any malicious software. The Information Technology department shall also ensure that the software has all patches installed and has the most recent virus definitions.

Revised: 3/2008, 10/2018

Procedures for Ensuring Workstation Security

Purpose: This procedure is designed to ensure the physical security of all Imagine! workstations that contain or that can access electronic protected health information.

GENERALLY

Imagine! shall implement the following Physical safeguards for all workstations that can access EPHI.

ENFORCEMENT

Violation of these Procedures for Ensuring Workstation Security shall be punished according to the Sanctioning policy outlined in Imagine!'s *HIPAA Privacy and Security Policies and Procedures.*

OFFICE SECURITY

Whenever possible, members of Imagine!'s workforce shall lock their office doors when they leave their offices for extended periods of time and when they leave at the end of each workday.

COMPUTER SECURITY

Monitor Placement

Employees shall ensure that each workstation monitor is placed in a manner that prevents unauthorized persons from viewing the monitor while the workstation is being used by a member of Imagine!'s workforce.

Server Room

Only members of Imagine!'s workforce who are authorized to access the main server shall be allowed into the server room. At the end of each business day and during any period where the room is unattended, Information Technology personnel shall ensure the door that provides access to that room is locked. The server shall not be left unattended if the room is unlocked.

Revised: 11/2007, 1/2014, 3/2018

Procedure for Disposal of Computer Hardware and Other Electronic or Physical Media Which Contains or Contained EPHI

Purpose: The purpose of this procedure is to ensure the confidentiality of Imagine!'s electronic protected health information is maintained even when computer hardware or storage media are discarded. Electronic protected health information shall be removed from computer hardware and other electronic media in the following manners:

I. Computer and Other Hardware

Erase Hard Drive and Re-install software

The Information Technology Director or designated staff shall ensure that all computer hardware containing electronic protected health information is erased or otherwise physically destroyed and made unreadable. In the case of erasure, a method that overwrites the existing data of the hard drive in multiple passes, such as DoD 5220.22-M, must be used. In the case of computer hardware that is being donated to clients, etc., the Information Technology Director or designee shall then reinstall any operating system or other software that is was originally installed on the computer's hard drive or any other software that was purchased by Imagine! which Imagine! is donating along with the computer.

II. Other Electronic Media

A. Disposing of external hard drives, floppy disks, USB thumb drives, and other removable magnetic storage media

Any magnetic storage media that contained EPHI and is to be discarded shall be brought to the Information Technology department for disposal. Before this media is discarded, in accordance with local, state and federal regulations regarding the disposal of electronic devices and media, said media will be subject to bulk magnetic erasing, physical destruction or a multi-pass data wipe method such as DoD 5220.22-M.

B. Disposing of DVDS, CDS and Other Forms of Optical Storage

In some situations, Imagine! stores electronic protected health information to optical media. Any optical media that contained EPHI and is to be discarded shall be brought to the Information Technology department for disposal. When Imagine! determines it is appropriate to dispose of this media, the Information Technology Director or designee shall ensure that the discs are rendered physically unusable prior to disposal.

III. Physical Media

Destruction and Retention of Paper Documents

All paper documents that need to be disposed of shall be shredded or placed in a secure container until such time it can be collected and shredded. Paper documents shall be retained according to Imagine!'s Document Retention Policy.

Revised: 10/2009, 2/2014, 6/2018

Procedure for Removal of EPHI from Electronic Media Being Reused

Purpose: The purpose of this procedure is to ensure that electronic protected health information is removed from reusable media, before that media is returned to circulation after being used by a member of Imagine!'s workforce.

Electronic protected health information shall be removed from re-usable electronic media prior to being recirculated by using an approved software that completely re-writes the data on the re-usable media.

Failure to follow these procedures will result in the offending workforce member being sanctioned pursuant to policies for sanctioning a violation Imagine!'s Security Policies and Procedures. Additionally, attempts to recover information from reusable media not placed on the media by the workforce member attempting the recovery will result in that workforce member being sanctioned pursuant to Imagine!'s policies for sanctioning a violation of its Security Policies and Procedures.

Revised: 1/2014, 1/2017

Technical Safeguards

Procedure for Assigning Unique Identifier incident response

Purpose: The purpose of this procedure is to ensure that each member of Imagine!'s workforce who uses Imagine!'s information systems has a unique identifier for logging into those systems.

Responsible Party: Imagine!'s Security Officer is responsible for ensuring that members of Imagine!'s workforce follow these procedures.

Creating and Assigning Unique Identifier

The Information Technology Director or Systems Administrator shall be responsible for creating for each user a unique identifying name upon the user being authorized to access Imagine!'s information systems. The unique identifying name or number shall be derived from first initial of users first name combined with user's last name.

The Information Technology Director or Systems Administrator shall also be responsible for creating accounts and taking any necessary action to assign the user name created for the user to the user. This shall include such actions as creating accounts on the appropriate servers, creating an account on the workstation the user has been assigned, and any other action necessary to ensure that the user is identified by his/her unique user identification in all of Imagine!'s information systems.

For new accounts, The Information Technology Director or Systems Administrator shall then provide the employee with appropriate levels of access, by following Imagine!'s procedures for Authorizing Access to Electronic Protected Health Information.

For systems where user access is maintained by other departments, those departments will follow this procedure for the creating and maintenance of user accounts on those systems.

Any deviations from these procedures due to identifiers that were established before the effective date of these policies and procedures will be tolerated. Additionally, any information system that does not support adherence to these procedures will be tolerated but must be documented. Documentation should include what specification the systems supports and how unique identifiers will be determined on that system.

Notice to Responsible Employee

The department director or designee responsible for the supervision of the new employee or the Human Resources department shall be responsible for notifying the Information Technology Director or Systems Administrator that a new employee has been hired and that they need a unique user identification.

Revised: 1/2008, 7/2010, 1/2014, 8/2016, 3/2018

Emergency Access Procedure

Purpose: This procedure is designed to ensure that Imagine! has implemented policies and procedures to ensure the availability of EPHI in the event of any emergencies that may damage systems containing EPHI. These emergencies include, but are not limited to; systems crashes, virus attacks, hardware failures, fires, natural disasters and malicious attacks on Imagine! property.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

1. In-House Emergency Access

Any disruptions that can be managed without having to relocate from the current central offices at 1400 Dixon Ave. and 1665 Coal Creek Dr. will be considered in-house emergencies. These include, but are not limited to; power outages, hardware failures, software failure or corruption and virus intrusions. Personnel and equipment from one central office may be relocated to the other should one office become uninhabitable. Since definition of all foreseeable emergencies would be too exhausting, general systems will be put in place to ensure any incident can be mitigated in the most efficient way possible. Some preparations include:

- UPS power backup for critical systems
- Following the Data Backup procedures
- Ensuring replacement hardware is available
- Ensuring original installation media is available for applications and operating systems

In the event the emergency exceeds the capacity of the Information Technology department expertise, outside technical assistance will be brought in to mitigate the emergency.

2. Relocation Emergency Access

Any disruptions that cannot be managed without having to relocate from both central offices will be considered relocation emergencies. These would include any natural disaster, fire or other incident that made the occupation of the central offices impossible for any length of time. Any situation that could not guarantee the security and access of EPHI would also be considered a relocation emergency.

All data should be recoverable to at least the previous nights backup. If new hardware is required due to total or partial loss of needed systems, purchase of the fastest possible replacement should occur as soon as possible. Any systems that have hardware warranty replacement should be ordered immediately. Any systems that can be relocated should be.

Locations that will be utilized in the event relocation is necessary are, in order of priority:

1) A suitable group home with enough room for business office operations. Currently the basement of the Bob and Judy Charles Group Home. The Charles Family Group Home is an alternate as well as the Foothills group home.
2) Rental property in the Boulder/Lafayette area
3) Available office space at the Developmental Disabilities Resource Center

If habitation of the central office locations cannot occur for some time, a suitable rental location that can house as many departments as possible should be sought out. It may be necessary to find several locations for different departments.

Revised: 3/2009, 2/2015, 6/2018

Procedure for Automatic Logoff

Purpose: The purpose of this procedure is to ensure that a workstation that is left unattended either terminates any open session or takes some other step to ensure it cannot become an avenue for unauthorized access to electronic protected health information.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

1. The Information Technology department shall ensure that software which provides access to electronic protected health information, and has the ability to terminate a session after a maximum of thirty (30) minutes of inactivity, will be configured to do so.

2. The Information Technology department shall ensure that all workstations have some form of screen saver software or user lock out. Additionally, the Information Technology department shall ensure that the screen saver or lock out is configured to activate after ten (10) minutes. The Information Technology department shall also ensure that the screen saver or lock out requires a password to deactivate.

Revised: 1/2014, 11/2017

Procedure for Audit Controls

Purpose: This procedure is designed to ensure that monitoring of audit logs and records for Imagine!'s information systems used by members of Imagine!'s workforce is done to the best possible extent.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

1. Firewall Error Logs

The Security Officer shall designate members of the Information Technology staff to assist in application of this procedure. Review of the latest error logs as recorded by the internal and external firewall appliances or software will take place on a monthly basis and as needed in response to any security incident.

2. SPAM Server Error and Quarantine Logs

The Security Officer shall designate members of the Information Technology staff to assist in application of this procedure. Review of the latest error logs as recorded by the e-mail filtering appliance or software will take place on a monthly basis. This will include review of the quarantine reports to identify any possible internal threats as well as error logs generated by the e-mail system.

3. Network Switching Hardware Logs

The Security Officer shall designate members of the Information Technology staff to assist in application of this procedure. Review of the latest error logs as recorded by the internal network switching hardware shall take place on a monthly basis.

4. Security Incident Logs

The Security Officer shall designate members of the Information Technology staff to assist in application of this procedure. Review of any logs indicating abnormal or possible security issues generated by other systems not mentioned above, such as Anti-Virus monitoring. Review of these will be on as as-needed basis as the security incidents are being detected.

Revised: 1/2014, 3/2018

Procedure for Authenticating Electronic Protected Health Information (Transmission)

Purpose: The purpose of this procedure is to provide a means to verify that electronic protected health information was not altered without authorization during transmission.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

Imagine! has determined, based upon its technical capabilities, size, and budget, that a dedicated technological authentication solution is not reasonable in its environment. Any emails sent to outside organizations will be sent encrypted, unless the *Request for Non Secure Communications* form is completed. All applications accessed over the internet will use SSL or TLS protocol.

Whenever an employee believes that a piece of electronic protected health information has been altered in an unauthorized manner, that employee shall immediately compare the electronic protected health information contained on Imagine!'s information systems to the information contained in the individual's file.

In the event that the employee determines, based upon this comparison, that the electronic protected health information has been altered, he or she shall immediately notify the Security Officer that the information has been altered. The Security Officer shall then follow Imagine!'s Incident Response and Reporting Procedure. The employee should not amend the electronic protected health information, but should allow the Security Officer to determine when it is appropriate to correct the information.

Furthermore, the employee should resend the information, but should use a different mode of transmission. If the need for the information is time sensitive, the employee should attempt to fax the paper copies of the information using Imagine!'s procedures for faxing protected health information.

Revised: 7/2010, 1/2014, 8/2016, 3/2018

Procedure for Authentication, Person

Purpose: The purpose of this procedure is to provide a means to verify that an individual who attempts to access Imagine!'s information systems by using an assigned identifier is person to whom the identifier was assigned.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

Password Authentication

Authentication shall be provided by the use of a password. Each employee will be assigned a password at the time they are granted access to Imagine!'s information systems.

The password assigned to each employee shall conform to the requirements of Imagine!'s Password Management Procedure. This shall include the length of time the password shall be valid, the composition of the password, and the assignment of a new password at the expiration of the old password.

Biometric Authentication

The Information Technology department shall be responsible for implementing a biometric authentication system in areas where deemed necessary. Biometric authentication can be used for both workstation access and application access. Each employee shall be authenticated based upon a unique physical feature.

Imagine! has settled upon fingerprint recognition for biometric authentication. This will take the form of a fingerprint reader positioned at the workstation accepting this authentication. The Information Technology department shall be responsible for configuring the workstations using this solution.

The Information Technology department shall also be responsible for configuring the biometric device to work with each employee. Each employee shall have his or her right or left index finger or thumb scanned as necessary for use with the biometric device. The Security Officer shall be responsible for scheduling the scans in manner designed to ensure the biometric device is working by July 1, 2005, where applicable.

Revised: 1/2014

Procedure for Authentication, EPHI

Purpose: The purpose of this procedure is to provide a means to verify that an individual who attempts to access Imagine!'s information systems by using an assigned identifier is person to whom the identifier was assigned.

Responsible Party: The Security Officer shall be responsible for ensuring that this procedure is followed by members of Imagine!'s workforce.

Password Authentication

Authentication shall be provided by the use of a password. Each employee will be assigned a password at the time they are granted access to Imagine!'s information systems.

The password assigned to each employee shall conform to the requirements of Imagine!'s Password Management Procedure. This shall include the length of time the password shall be valid, the composition of the password, and the assignment of a new password at the expiration of the old password.

Revised: 1/2014

Appendix A

I) ADMINISTRATIVE SECURITY POLICIES

A. Workforce Security *[45 CFR §164.308(a)(3)(i)]*

1. Authorization/Supervision of Workforce *[45 CFR §164.308(a)(3)(ii)(A)]*

The Procedure for Information Access Establishment and Modifications establishes physical safeguards which are sufficient to protect and secure PHI and EPHI from persons not authorized to access it. These measures are seen as sufficient enough to protect EPHI under this specification.

2. Workforce Member Clearance *[45 CFR §164.308(a)(3)(ii)(B)]*

Imagine! feels this specification is necessary to implement. Given the population we serve and employee's access to sensitive EPHI, the risk of not ensuring qualified members of the workforce is too great to not address.

3. Workforce Member Termination Procedures *[45 CFR §164.308(a)(3)(ii)(C)]*

Imagine! will implement this specification in order to be aligned with the current exit procedure used by the Human Resources department.

B. Information Access Management *[45 CFR §164.308(a)(4)]*

1. Access Authorization *[45 CFR. §164.308(a)(4)(ii)(B)]*

Imagine! currently operates several applications that utilize EPHI. For this reason, it is necessary to restrict employee access to these applications based on job description. This is also in alignment with the "minimum necessary" requirements of the privacy policy. This specification is necessary to implement.

2. Access Establishment and Modification *[45 CFR §164.308(a)(4)(ii)(C)]*

Imagine! currently operates several applications that utilize EPHI. For this reason, it is necessary to restrict employee access to these applications based on job description. This is also in alignment with the "minimum necessary" requirements of the privacy policy. This specification is necessary to implement.

C. Security Awareness and Training *[45 CFR §164.308(a)(5)]*

1. Security Reminders *[45 CFR §164.308(a)(5)(ii)(A)]*

Imagine! has determined that implementation of this standard is necessary due to our geographically dispersed workforce. Imagine! also possesses the infrastructure to make this a simple and cost effective standard to implement.

2. Protection Against Malicious Software *[45 CFR §164.308(a)(5)(ii)(B)]*

Imagine! has determined that implementation of this standard is necessary due to our high reliance on the Internet and e-mail communication. Imagine! also possesses the infrastructure to make this possible and cost effective to implement.

3. Log-in monitoring *[45 CFR §164.308(a)(5)(ii)(C)]*

Imagine! has determined that implementation of this standard is necessary. Currently, all applications used by Imagine! do not offer log-in monitoring. These applications are largely legacy systems due for eventual upgrade or replacement. It is therefore unreasonable to alter them so they would provide log-in monitoring. Monitoring will be done on all applications that provide this feature and on the network directory tree level. Individual workstation monitoring will not be done as EPHI

should not be stored on standalone workstations and the network monitoring will be able to provide clues to security breaches. As new applications are installed, log-in monitoring of those applications will occur to the extent that the application provides.

4. Password Management *[45 CFR §164.308(a)(5)(ii)(D)]*

Imagine! has determined that implementation of this standard is necessary. Given the number of applications used by Imagine!'s workforce and their reliance on Internet technology, the risk to EPHI is high. All of Imagine!'s applications containing EPHI require a password to obtain access so implementation of this standard does not represent a substantial additional financial burden.

D. Contingency Plan *[45 CFR §164.308(a)(7)]*

1. Testing and Revising the Contingency Plan *[45 CFR. §164.308(a)(7)(ii)(D)]*

Imagine! has determined that implementation of this standard is necessary. Given the scope of the systems supported and high risk of unavailability of EPHI, it is reasonable to implement this standard by partial testing and simulations. The additional cost of staff time to do the required testing and revising is not prohibitive.

2. Applications and Data Criticality Analysis *[45 CFR §164.308(a)(7)(ii)(E)]*

Imagine! has several applications that are critical to its business operations and availability of EPHI. A formal analysis of these systems and data is not necessary as the risk assessment identifies these areas of criticality. Imagine! will not implement this standard.

Other procedures in this standard ensure the recoverability and survivability of critical information systems in case of an emergency. All EPHI data is recoverable under these procedures and therefore it is not necessary to identify critical versus non-critical systems as they pertain to the contingency plan.

II) PHYSICAL SAFEGUARDS *[45 CFR §164.310]*

A. [Facility / Location] Access Controls *[45 CFR §164.310(a)]*

1. Contingency Operations *[45 CFR §164.310(a)(2)(i)]*

Imagine! has determined that full implementation of this standard is not necessary. Facility access during a contingency will take one of two forms; central office sites are still secure and accessible, or central office sites are not secure and operations have been relocated. In the event of the former, current access and security policies will continue to protect access to EPHI. In the event of the later, emergency access to hot or non-hot sites will be established based upon the same rules as were in place at the central offices. Imagine!'s Contingency Plan Procedure as well as it's Data Backup, Data Recovery and Emergency Mode Operation Plans are sufficient to govern contingency operations. A separate policy on contingency access would be redundant and unnecessary.

2. Facility Security Plan *[45 CFR §164.310(a)(2)(ii)]*

Imagine! has determined that implementation of this standard is necessary. Due to the high risk of compromise of EPHI, it is reasonable to implement this specification at all facilities managed by Imagine! that contain systems with EPHI. Current access procedures are in place that make the implementation of this specification cost efficient.

3. Access Control and Validation Procedures [45 CFR §164.310(a)(2)(iii)]

Imagine! has determined that implementation of this standard is necessary. Due to the high risk of compromise of EPHI, it is reasonable to implement this specification at all facilities managed by Imagine! that contain systems with EPHI. Current access procedures are in place that make the implementation of this specification cost efficient.

4. Maintenance Records *[45 CFR §164.310(a)(2)(iv)]*

Imagine! has determined that full implementation of this standard is not necessary. Facility access for maintenance purposes is controlled by the employee requesting the maintenance. Access to sensitive areas is controlled and workstations and applications are secure. It is unlikely that maintenance personnel would know what applications contained EPHI and even more unlikely they would know how to access this information. Equipment likely to be worked on by external maintenance personnel does not need to be tracked as any equipment containing EPHI would not

be leaving the facility. Given the risk to EPHI is low, Imagine!'s normal procedures for the maintaining of repair records and work orders will be sufficient under the circumstances.

B. Device and Media Controls *[45 CFR §164.310(d)]*

1. Accountability *[45 CFR §164.310(d)(2)(iii)]*

Imagine! has determined that this specification is not reasonable in its work environment. Based on our assessment, Imagine! will implement the following as an equivalent alternative measure.

Imagine! will maintain a database containing identifying features of all server, workstation, laptop and mobile computing devices purchased by Imagine! and used in the access of EPHI. This database should contain at a minimum the serial or asset tag number, model number, purchase date, issue date and the user it's assigned to. It is the responsibility of the Information Technology Director or designee to ensure this data is up-to-date and accurate.

Tracking and inventory of every type of electronic media that is likely to contain EPHI would present an unnecessary burden on the Information Technology department as well as Imagine! employees to report and track every possible device. This burden would not be cost effective given the information that would be tracked and the fact that the risk to EPHI would not be substantially lowered.

2. Data Backup and Storage *[45 CFR §164.310(d)(2)(iv)]*

Imagine! has determined that this specification is not reasonable in its work environment. Since hardware containing EPHI is largely server computers, Imagine! will rely upon the retrievable exact copies created as part of its routine backup. In the event of loss of electronic protected health information due to a move of equipment, Imagine! will restore the lost information from Imagine!'s regularly performed backup. Loss of information on any other system besides a server machine does not represent a threat to the availability of EPHI. Based on this assessment, Imagine! has determined it is reasonable to implement an equivalent alternative measure, the details of which are covered in the procedures for regular data backups.

II) TECHNICAL SAFEGUARDS *[45 CFR §164.312]*

A. Access Control *[45 CFR §164.312(a)]*

1. Automatic Logoff *[45 CFR §164.312(a)(2)(iii)]*

Imagine! has determined that this specification is not reasonable in its work environment. Based on our assessment, Imagine! will implement the following as an equivalent alternative measure.

Given that some applications that access EPHI do not have the features of automatic logoff and some of these are legacy systems which would require they be altered, some at considerable expense, Imagine! cannot fully implement this standard.

A suitable alternative will be to have the automatic screen saver feature of the workstation enabled and set to engage after ten (10) minutes of inactivity. In addition, a password would be required to de-activate the screen saver and begin using the station.

2. Encryption and Decryption *[45 CFR §164.312(a)(2)(iv)]*

Imagine! has determined that this specification is not reasonable in its work environment. At this time, several legacy systems containing EPHI are being phased out for more secure systems. Of the remaining systems, the most commonly used access EPHI through secure SSL Internet browser links or applications which utilize a SQL server database backend.

Threats to SQL databases are determined to be low, as is the possibility of obtaining EPHI by intercepting SSL Internet transmissions. Procedures require that any email containing PHI that are destined for non-Imagine! domains are sent via encryption.

All laptop computers will have disk based encryption.

Risks due to desktop systems not being encrypted are low. However, desktop systems will be encrypted at the disk level whenever appropriate.

B. Integrity of Electronic Protected Health Information *[45 CFR §164.312(c)]*

1. Mechanism to Authenticate Electronic Protected Health Information *[45 CFR §164.312(c)(2)]*

Imagine! has determined that this specification is not reasonable in its work environment. Based on our assessment, Imagine! will implement the following as an equivalent alternative measure.

Authentication shall be provided by the use of a password. Each employee will be assigned a password at the time they are granted access to Imagine!'s information systems. The password assigned to each employee shall conform to the requirements of Imagine!'s Password Policy and Procedure. This shall include the length of time the password shall be valid, the composition of the password, and the assignment of a new password at the expiration of the old password.

Imagine! currently has no application accessing EPHI that utilizes technical authentication of information. Implementing this specification would be unreasonably expensive as it would mean replacing current information systems. Risk to EPHI is low when all workstation and authentication safeguards are taken into account.

C. Transmission Security *[45 CFR §164.312(e)]*

1. Integrity Controls *[45 CFR §164.312(e)(2)(i)]*

Imagine! has determined, based upon its technical capabilities, size, and budget, that a technological authentication solution is not reasonable in its environment. Instead, Imagine! has decided that an equivalent alternative measure is reasonable and appropriate.

Since transmission of EPHI takes several forms from e-mail to Internet, implementation of a system to verify integrity of all transmitted EPHI would be too costly.

2. Encryption *[45 CR. §164.312(e)(2)(ii)]*

Imagine! has determined that a partial implementation of this specification is reasonable in its work environment. Because of the dispersed nature of our workforce, any employees with a laptop computer will use an encryption technology that ensures any PHI on the device is

secure. For desktop computers that do not leave Imagine! facilities, encryption is not required. It needs to be noted that most applications used are browser based and PHI is not stored in local databases on computers.

Revised: 1/2008, 7/2010, 1/2014, 8/2016, 3/2018

Appendix B – HIPAA Forms

The following pages contain current authorized forms to fulfill specific functions and tasks related to an individual's PHI. Both English and Spanish versions are enclosed. Members of Imagine!'s Workforce shall only use these form versions to complete their duties as assigned.

1. Authorization to Release Information
2. Authorization to Release Information (Spanish)
3. Photo and Video Release
4. Acknowledgement of Receipt of Notice of Privacy Practices
5. Acknowledgement of Receipt of Notice of Privacy Practices (Spanish)
6. Documentation of Good Faith Effort to Obtain Written Acknowledgement of Receipt of Notice of Privacy Practices
7. Documentation of Good Faith Effort to Obtain Written Acknowledgement of Receipt of Notice of Privacy Practices (Spanish)
8. Request for Communications by Alternative Means
9. Request for Communications by Alternative Means (Spanish)
10. Request for Amendment of Protected Health Information
11. Request for Accounting of Disclosures
12. Request for Accounting of Disclosures (Spanish)
13. Request to Restriction on Uses or Disclosures
14. Request for Non Secure Communications
15. Request for Non Secure Communications (Spanish)
16. Records Retention Policy
17. Bring Your Own Device

Authorization to Release Information

To allow a THIRD PARTY to have access to Protected Health Information
Revised: 7/8/2022

CLIENT INFORMATION:

Client Name (required): _____ Date of Birth: _____

Social Security or Medicaid #:_____ Phone Number: _____

Address, City, State, Zip: _____

Imagine! is authorized to disclose my Protected Health Information as specified below to the following person or organization at the Client's request for the purpose of fulfilling the Client's request, or for the following purpose(s):

_____

Name:_____ Phone Number: _____

Organization: _____

Address, City, State, Zip: _____

This authorization for release of information covers the period of healthcare from:

☐ _____ to _____ OR ☐ all past, present, and future periods.

INFORMATION TO BE PROVIDED:

- ☐ All healthcare records, meaning every page in my record, including all categories of records listed below.
- ☐ All employment, personnel or wage records including vocational and supported employment
- ☐ Oral communication, conversations with or without client and other parties, regarding evaluation or treatment
- ☐ All pharmacy/prescription records including NDC numbers and drug information handouts/monographs.
- ☐ All medical and mental health records and assessments (Including diagnosis and medications prescribed)
- ☐ All billing records including all statements, insurance claim forms, itemized bills, and records of billing to third party payers and
- ☐ Other _____

This authorization will automatically expire 1 year from the date signed below unless I request an expiration date sooner. Expiration date: _____ (expiration date not to exceed one year from signature date).

I understand the following: I may revoke this authorization at any time, except to the extent that action has already been taken to comply with it, by notifying Imagine! in writing. Information disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and is no longer protected by the HIPAA Privacy Rule. Imagine! will still provide services and seek payment for services provided, whether or not I sign this authorization. Imagine! may charge for copies of records.

Client or Representative signature: _____ **Date:** _____

If by Representative, the Representative's authority to act: _____
Client must sign if over 18 and without legal guardian. Parent, Legal Guardian, Power of Attorney or equivalent may sign on behalf of adult or minor child.

This Authorization was REVOKED on: (Date)_____ Staff Signature: _____

Modificado: Febrero de 2019

Autorización para Divulgar Información

Información de la persona recibiendo servicios de Imagine!:	Información de la persona dando consentimiento a esta divulgación
Nombre:	Nombre:
Teléfono/Correo electrónico:	Teléfono/Correo electrónico:
Fax:	Fax:
Fecha de Nacimiento:	Role: ☐ Si mismo ☐ Padre/Guardián/Representante personal

Tipo de Divulgación:	Para el propósito de:
☐Divulgar a ☐Obtener de ☐Intercambiar con	☐ Continuar cuidado/tratamiento ☐ Admisión/Evaluación ☐ Solicitud del individuo ☐Otro:

Autorizo:		
☐Imagine!	☐ACL	☐Abogado/ Policía:
☐ Proveedor de Servicio:		☐Escuela:
☐Medico:		☐Otro:

Para Divulgar información a:			Dirección, Teléfono y Numero de Fax
☐Proveedor de Servicio	☐Médico	☐Otro	
☐Escuela	☐Abogado/ Policía		
☐Proveedor de Servicio	☐Médico	☐Otro	
☐Escuela	☐Abogado/ Policía		
☐Proveedor de Servicio	☐Médico	☐Otro	
☐Escuela	☐Abogado/ Policía		

Para recibir información de:			Dirección, Teléfono y Numero de Fax
☐Proveedor de Servicio	☐Médico	☐Otro	
☐Escuela	☐Abogado/ Policía		
☐Proveedor de Servicio	☐Médico	☐Otro	
☐Escuela	☐Abogado/ Policía		
☐Proveedor de Servicio	☐Médico	☐Otro	
☐Escuela	☐Abogado/ Policía		

Tipo de Archivos/información Pedido:						
☐ Referencia/Admisión	☐ Descarga	☐ Medico	☐ Notas del Caso	☐ Notas de psicoterapia	☐ Archivos Escolares	☐ Servicios residenciales
☐ Plan de Servicios/IFSP	☐ Evaluación de desarrollo	☐ Salud de Conducta	☐Vista/Audición	☐ Archivos de terapias: física, ocupacional, habla	☐ Otro:	

Rango de fecha de los Archivos:		
Desde:_____	**Hasta:**_____	☐Archivo entero

Esta autorización se vence _____ (*la fecha de vencimiento no puede ser después de un año de la fecha cuando se firmó)* **Yo entiendo lo siguiente:** Esta autorización se vence automáticamente 1 año desde la fecha que sea firmada a menos que yo pida una fecha antes. Yo puedo **revocar** esta autorización a cualquier momento, excepto que ya sea cumplido por medio de notificar a Imagine! por escrito. Información revelada de acuerdo con la autorización puede ser revelada otra vez por el receptor y ya no será protegido por el reglamento de privacidad de HIPAA. Imagine! Todavía va a proveer servicios y buscaremos pago de los servicios proveídos, aunque yo firme esta autorización o no. Imagine! puede cobrar por copias de los archivos.

_____ _____

Firma de la persona dando consentimiento | Fecha | Nombre Escrito

Autorización fue REVOCADA: (Fecha)_____ **Firma:**_____

Imagine! Specific Photo and Video Release

Revised November 8, 2017

I give my permission to Imagine! Innovations to reprint and use specific photographs, videos, or other recorded media and information about

_____

Print Individual's Name

as described here:

The image/information will be used for Imagine! promotional/publicity activities designed to further the agency's mission in the community. This may include Imagine! newsletters/brochures/reports, newspapers/publications, television, on display in Imagine! buildings, on Imagine! websites, and on social media sites such as Facebook, Twitter, and blogs.

Use the section below to describe the specific manner in which the image/information will be published:

Imagine! employee newsletter, Facebook, Twitter, Instagram, YouTube, Imagine! blogs, and print copy in Imagine! administrative buildings.

This permission is consistent with protections provided by rules for the Colorado Division for Intellectual and Developmental Disabilities at 2 CCR 503-1. I understand that I may refuse to sign this authorization, and that my refusal to sign will not affect my (my dependent's) determination of eligibility to receive services nor opportunity to receive services if deemed eligible. If I cancel my permission, no additional copies of marketing literature will be printed after that date and already printed copies may be used until that literature is replaced.

_____ _____

Signature of individual/guardian **Date signed**

_____ _____

Printed name of individual/guardian **Relationship to person in services**

Imagine! will use this information to acknowledge, recognize, and promote the many contributions individuals with intellectual and developmental disabilities are bringing to their communities every day. All images will be used with respect and dignity. If an individual or guardian does not believe a picture to respectful or dignified, s/he may ask for the image to be removed.

Name of Imagine! Staff Soliciting Release: _____

Imagine!
1400 Dixon Ave., Lafayette, CO 80026
Phone: (303) 665-7789 • Fax: (303) 604-5431
www.imaginecolorado.org

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

Effective: September 2013
Revised: August 1, 2017

This is to acknowledge my receipt of Imagine!'s Notice of Privacy Practices (effective September 23, 2013).

_____
Printed Name of Person Receiving Imagine! Services

_____
Individual's Address

_____
Signature of Individual or Personal Representative **Date**

_____
Name of Personal Representative of Legal Guardian

_____
Description of Legal Guardian's/Personal Representative's Authority to act for the Individual (if applicable)

Please return this form to:

Rebecca Novinger
Privacy Officer
1400 Dixon Avenue
Lafayette, CO 80026

RECONOCIMIENTO DE RECIBO DE AVISO DE PRACTICAS DE PRIVACIDAD

Efectivo: Septiembre de 2013
Enmendado: 1 de Agosto de 2017

Esto es para confirmar que recibí el Aviso de Prácticas de Privacidad de Imagine! (efectivo el 23 de septiembre de 2013)

_____

Nombre de la Persona Recibiendo Servicios de Imagine! (en letra de molde)

_____

Dirección del Individuo

_____

Firma del Individuo o del Representante Personal Fecha

_____

Nombre del Representante Personal o Tutor Legal

_____

Descripción de la Autoridad del Representante Personal/Tutor Legal para Actuar para el Individuo (si aplica)

Por favor regrese esta forma a:
Rebecca Novinger
Privacy Officer
1400 Dixon Avenue
Lafayette, CO 80026

Documentation of Good Faith Efforts to Obtain Written Acknowledgment of Receipt of Notice of Privacy Practices

Name of Individual: _____

Effort to Obtain Written Acknowledgment of Notice of Privacy Practices:

_____

_____

_____

_____

_____

_____

Reason Why the Written Acknowledgment Was Not Obtained:

_____

_____

_____

_____

_____

_____ _____

Date Signature of Authorized Imagine! Staff

Documentación de Esfuerzos de Buena Fe para Obtener Reconocimiento Escrito de Haber Recibido el Aviso de Practicas de Privacidad

Nombre del Individuo: _____

Esfuerzos para Obtener Reconocimiento Escrito de Haber Recibido el Aviso de Practicas de Privacidad:

_____

_____

_____

_____

_____

_____

Razón porque el Reconocimiento Escrito no fue Obtenido:

_____

_____

_____

_____

_____

_____ _____

Fecha Firma del Empleado Autorizado de Imagine!

Request for Communications by Alternative Means

Effective: January 1, 2019

Information about Individual Receiving Services from Imagine!:
Full Name:
Address:
Phone/Email:
DOB:

I, _____ hereby request that the following alternative means of communication be used with the Protected Health Information of the person identified above.

Alternative Means of Communication
Please describe how you'd like your protected health information communicated to you:

Information about Person Completing This Request:
Full Name:
Address:
Phone/Email:
Role (choose one): ☐ Self ☐ Parent/Guardian/Personal Representative

_____ _____

Signature of Person Making Request Date

_____

Printed Name of Person Making Request

For Internal Use Only:

☐ Request Accepted

Return a copy of this form to the individual. Forward original for records archiving.

☐ Request Denied and reason:_____

Return a copy of this form to the individual. Forward original for records archiving.

_____ _____

Privacy Officer Signature Date

Solicitud de medios de comunicación alternativa

Efectivo: Enero 1, 2019

Información personal de la persona quien recibe servicios en Imagine!:
Nombre completo:
Dirección:
Telfono/Correo electrónico:
Fecha de Nacimiento:

Yo, _____ por la presente solicito, que se utilicen los siguientes medios alternativos de comunicación con la información sanitaria protegida de la persona identificada anteriormente.

Medios alternativos de comunicación:
Por favor describa cómo desea que le comuniquen su información médica protegida:

Información acerca de la persona quien completa la solicitud:
Nombre completo:
Dirección:
Telefono/Correo electrónico:
Rol (seleccione uno): ☐Yo ☐Padre/Guardian/Representante personal

_____ _____

Firma de quien realiza la solicitud Fecha

_____

Nombre de quien realiza la solicitud

Para uso interno solamente:

☐Acepto la solicitud

Devuelva una copia de este formulario a la persona. Reenviar original para archivo de registros.

☐No acepto la solicitud, por qué?: _____

Devuelva una copia de este formulario a la persona. Reenviar original para archivo de registros.

_____ _____

Firma del Oficial de Privacidad Fecha

Request for Amendment of Protected Health Information

Complete and email this form to rnovinger@imaginecolorado.org or mail to 1400 Dixon St. Lafayette, CO 80026

Revised: August 1, 2017

Name of Person Receiving Services from Imagine!			
Date of Birth		**Today's Date**	
Name of Person Completing this Form		**Relationship to Person Receiving Imagine! Services**	☐ Self ☐ Parent/Guardian/Personal Representative
Please describe the information in the record that is inaccurate or incomplete.			
Please explain how you'd like this information changed (amended).			
Would you like the changes (amendments) sent to anyone else who received the information in the past? If so, please specify the name of the individual and/or organization.			

If you agree, Imagine! will make a reasonable effort to provide the amendment to other persons who we know have received the information in the past and who may have relied, or are likely to rely, on such information.

☐ I agree to allow Imagine! to release any amended information to individuals or entities as described above.

_____

Signature of Person Authorized to Make this Request | Print Name | Date

For Internal Use Only

Date Received		**Request Has Been:**	☐ Approved ☐ Denied
If Denied, check reason for denial:	☐ PHI is not part of the designated record set ☐ PHI is accurate/complete	☐ Imagine! did not create the record ☐ Record is unavailable for inspection under Federal Law	
Comments			

_____

Signature of Privacy Officer | Date

Request for Accounting of Disclosures of Protected Health Information

Complete and email this form to rnovinger@imaginecolorado.org or mail to 1400 Dixon St. Lafayette, CO 80026

Revised: August 1, 2017

Name of Person Receiving Services from Imagine!			
Date of Birth		**Today's Date**	
Name of Person Completing this Form		**Relationship to Person Receiving Imagine! Services**	☐Self ☐Parent/Guardian/Personal Representative

Imagine! is required to provide you with the opportunity to request a list of the disclosures made of your protected health information above and beyond the disclosures allowed by law. You may request a list of disclosures for any time period less than six years from the date of this request.

Imagine! is not required by law to include any of the following disclosures of your protected health information in an accounting to you:

- Disclosures made pursuant to an authorization signed by you or your personal representative;
- Disclosures to carry out Imagine!'s treatment, payment, and health care operations;
- Disclosures made to you or your personal representative;
- Disclosures made to persons involved in your care and/or payment or notification of next-of-kin or family members;
- Disclosures for national security or intelligence purposes;
- Disclosures as required by law; and
- Disclosures that occurred more than six years prior to the date of this request.

Please provide me with a list of disclosures made of my protected health information, above and beyond the disclosures allowed by law, for the following time period:

_____ TO _____

Month Year Month Year

_____

Signature of Person Authorized to Make this Request Print Name Date

For Internal Use Only

Date Received		**Request Has Been:**	☐Approved ☐Denied
Comments			

_____

Signature of Privacy Officer Date

Solicitud de revelacion de informacion de salud protegida

Complete y envíe este formulario por correo electrónico a rnovinger@imaginecolorado.org o envíe un correo electrónico a 1400 Dixon St. Lafayette, CO 80026

Revisado: 1 de agosto de 2017

Nombre de la persona que recibe los servicios de Imagine!			
Fecha de nacimiento		**Fecha de hoy**	
Nombre de la persona que completa este formulario		**Relación con la persona que recibe los servicios Imagine!**	☐Si mismo ☐ Padre / Tutor / Representante legal

Es requerido para Imagine! que le brinde la oportunidad de solicitar una lista de las divulgaciones hechas de su información de salud protegida más allá de las divulgaciones permitidas por la ley. Puede solicitar una lista de divulgaciones para cualquier período de tiempo inferior a seis años a partir de la fecha de esta solicitud.La ley no exige a Imagine! que incluya ninguna de las siguientes divulgaciones de su información de salud protegida en un informe para usted:

- Divulgaciones realizadas de conformidad con una autorización firmada por usted o su representante personal;
- Divulgaciones para llevar a cabo las operaciones de tratamiento, pago y atención médica de Imagine!
- Divulgaciones hechas a usted o su representante personal;
- Divulgaciones a personas involucradas en su cuidado y/o pago o notificación a los familiares o parientes más cercanos;
- Divulgaciones de seguridad nacional o de inteligencia;
- Divulgaciones según lo requerido por la ley; y
- Divulgaciones que ocurrieron más de seis años antes de la fecha de esta solicitud.

Por favor, proporcione una lista de las divulgaciones hechas de mi información médica protegida, más allá de las divulgaciones permitidas por la ley, para el siguiente período de tiempo:

_____ HASTA _____

Mes Año Mes Año

_____

Firma de la persona autorizada para hacer esta solicitud Nombre Impreso Fecha

Para uso interno solamente:

Fecha de recibo:		**Solicitud:**	☐ Aprobada ☐Negada
Comentarios			

_____

Firma del Oficial de Privacidad Fecha

Request for Restrictions on Uses and Disclosures

Effective: January 1, 2019

I hereby request that the following restrictions be placed on uses and disclosures of my protected health information.

Check either or all of the following:

☐ To carry out treatment, payment and health care operations

☐ To the following family members, other relatives or close personal friends of mine or other persons identified by me: _____

_____

☐To a public or private entity authorized by law or its charter to assist in disaster relief efforts.

Description of Restrictions and Timeline: _____

_____

_____

_____ _____

Witness Signature of Individual or Personal Representative

_____

Printed Name of Person Receiving Imagine! Services

_____ _____

Date Name of Personal Representative or Legal Guardian (If applicable)

_____

Description of Personal Representative's Authority to Act for the Individual (If applicable)

Imagine! hereby agrees with the following requested restrictions:

_____

_____

_____ _____

Date Imagine! Privacy Officer

Request for Non Secure Communications

Complete and email this form to rnovinger@imaginecolorado.org or mail to 1400 Dixon St. Lafayette, CO 80026

Revised: January 1, 2019

It is Imagine!'s policy to make every effort to secure the confidentiality and privacy of protected health information sent over email. Further, it is Imagine!'s policy to use encrypted email when an email message contains protected health information. However, the law allows individuals to request emails without encryption as long as the individual:

1. Is clearly informed of the security risks of non secure (unencrypted) email and that encryption is always recommended;
2. Indicates in **writing** that Imagine! has permission to send them email containing their protected health information non securely; and,
3. Imagine! keeps a record of this request.

Unencrypted email is not a secure form of communication. There is some risk that your protected health information and other sensitive or confidential information in such email may be misdirected, disclosed to, or intercepted by unauthorized third parties. However, you may consent to receive unencrypted email from us regarding your services from Imagine!. We will use the minimum necessary amount of protected health information in any communication.

By signing this form, you are stating that you understand the risks of unencrypted email and are giving permission to Imagine! to send you unencrypted emails that may contain your personal health information or the personal health information of the person served.

☐ *I request and accept the risk in receiving information via unsecure, unencrypted email. I understand I can withdraw my request at any time. I also understand that I am not required to sign this agreement in order to receive services from Imagine!.*

Information about Individual Receiving Services from Imagine!:	Information about Person Consenting to this Release
Name:	Name:
Phone/Email:	Phone/Email:
DOB:	Role: ☐ Self ☐ Parent/Guardian/Personal Representative

_____ _____

Signature of Person Authorizing Consent Date Print Name

Solicitud de comunicaciones no protegidas

Complete y envíe este formulario por correo electrónico a rnovinger@imaginecolorado.org o envíe por correo a 1400 Dixon St. Lafayette, CO 80026

Revisado: 1 de enero de 2019

Es política de Imagine! Hacer todos los esfuerzos para garantizar la confidencialidad y privacidad de la información médica protegida que se envía por correo electrónico. Aún más, es política de Imagine! utilizar el correo electrónico encriptado cuando un mensaje de correo electrónico contiene información de salud protegida. Sin embargo, la ley permite que las personas soliciten correos electrónicos no codificado siempre y cuando la persona:

1. Está claramente informado de los riesgos de seguridad de un correo electrónico no seguro (sin codificar) y que siempre se recomienda el correo encriptado;
2. Indica por escrito que Imagine! tiene el permiso para enviarles correos electrónicos que contengan su información de salud protegida de forma no segura; e,
3. Imagine! mantiene un registro de esta solicitud.

El correo electrónico no codificado no es una forma segura de comunicación. Existe cierto riesgo de que su información de salud protegida y otra información confidencial en dicho correo electrónico pueda ser desviada, divulgada o interceptada por terceros no autorizados. Sin embargo, puede dar su consentimiento para que le enviemos un correo electrónico no encriptado con respecto a sus servicios de Imagine! Utilizaremos la mínima información necesaria de salud protegida en cualquier comunicación.
Al firmar este formulario, usted declara que comprende los riesgos de un correo electrónico no encriptado y que está dando permiso a Imagine! para enviarle correos electrónicos no encriptado que puedan contener su información de salud personal o la información de salud personal de la persona atendida.

☐ *Solicito y acepto el riesgo de recibir información por correo electrónico no seguro y no encriptado. Entiendo que puedo retirar mi solicitud en cualquier momento. También entiendo que no estoy obligado a firmar este acuerdo para recibir servicios de Imagine !.*

Información sobre el individuo recibiendo los servicios de Imagine !:	Información sobre la persona que acepta esta authorizacion:
Nombre:	Nombre:
Telefono/correo electronico:	Telefono/correo electronico:
Fecha de nacimiento:	Papel: ☐Si mismo ☐ Padre / Tutor / Representante Legal

_____ _____

Firma de la persona que autoriza el consentimiento Fecha Nombre Impreso

Imagine! Records Retention Schedule Policy

Effective Date: March 28, 2006
Revised Date: August 1, 2017

POLICY

Imagine! will retain records in accordance with legal and government requirements, to include waiver, regulation, contract, and certification and licensing requirements. Records will be retained to meet the requirements with the most stringent timelines.

PROCEDURE

The HIPAA Privacy Rule indicates that PHI, including medical and financial records contained in the master record, should be retained for a minimum of six (6) years. Colorado regulation specifies that medical records should be retained for at least ten (10) years after the last date of service and all medical records for minors shall be retained after the last date of service for the period of the minority (18 years old) plus ten (10) years. Imagine! will comply with the stricter Colorado requirements and maintain consumer master records for the longer duration of time. In no case shall records be destroyed before the recommended retention period or before local statutory requirements. Any record that is subject to litigation, investigation, audit, or enforcement shall be kept until the action is resolved.

Record Retention Guidelines

Accounting

Accounts Payable Ledger	7 years
Accounts Receivable Ledger	7 years
Audit Reports	Permanent
Audit Work papers	7 years
Bank Statements/Reconciliations	7 years
Budget Work papers	3 years
Capital Ledger/Vouchers	Permanent
Checks Register & Canceled Checks	7 years
Disbursement Vouchers	7 years
Journal Entries	7 years
General Ledger – Year End	Permanent
General Ledger – Monthly	2 years
Financial Statements – Monthly	2 years
Financial Statements – Year End	Permanent

REFERENCE:
COLORADO: 6 C.C.R. § 1011-1, CH. VIII, § 11.3
45 CFR § 164.530(j)(1)(2)
10 CCR 2505-10 8.500.17 C
12 CCR 2509-10 7.915
Federal Record Retention Guide

REBECCA NOVINGER

Insurance Policies (Expired)	3 years
Tax Returns (990, 1099, etc.)	Permanent

Payroll and Human Resources

Applications	1 year
Benefit Plans	Permanent
Check Register	7 years
Earnings Records	Permanent
Employee Files	7 years after termination
Payroll Register	Permanent
Payroll Records/Timesheets	7 years
W2s	Permanent

Corporate Records

Board Minutes	Permanent
Business Licenses	Permanent
By Laws, Articles of Incorporation	Permanent
Contracts, Notes, Mortgages	7 years after expiration
Policies & Procedures	6 years after change

Program Records

Case Management Records	6 years after discharge or for the period of a minority (18 years old) plus 10 years
Medical Records (for consumers)	10 years after discharge or for the period of a minority (18 years old) plus 10 years

Storage of Documentation

Documentation may be stored on paper or electronic media. Storage of archived paper records should be maintained in locked storage areas with limited access. Access to financial and personnel related records should be limited to designated Finance and HR officers.

Documentation stored electronically should be stored on the network server. Procedures for backup are addressed in the HIPAA Privacy and Security Policies and Procedures.

Record Destruction

After each year end, all files exceeding their designated holding period will be destroyed. Emails will be deleted from the system 183 days from receipt unless otherwise archived. Destruction of records should be performed in one of the following ways:

1. Recycle non-confidential records.
2. Shred confidential records by an independent outside service.
3. Erase or destroy electronic data. Procedures to erase electronic PHI data are addressed in the HIPAA Privacy and Security Policies and Procedures.

REFERENCE:
COLORADO: 6 C.C.R. § 1011-1, CH. VIII, § 11.3
45 CFR § 164.530(j)(1)(2)
10 CCR 2505-10 8.500.17 C
12 CCR 2509-10 7.915
Federal Record Retention Guide

REBECCA NOVINGER

Bring Your Own Device (BYOD) Policy

Effective 3/1/2017

This policy establishes Imagine! guidelines for employee use of personally owned electronic devices for work-related purposes.

Bring Your Own Device (BYOD) Mobile Devices are defined as devices that are bought and paid for by Imagine! employees and owned individually by the employee or any entity that is not Imagine!. ***These devices are NOT owned by Imagine!*** Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops, wearables, and computers.

Procedure

Eligibility

Employee eligibility will be determined by job function and management approval. The IT department holds the sole right to deny access to the company network if all conditions are not met.

Technology devices that are eligible for this service must be in compliance with Imagine! security settings on servers, able to receive updates and able to sync with Imagine! server systems that administer services to mobile devices.

Devices and support

Imagine! will provide LIMITED connectivity support for eligible employees; employees should contact the device manufacturer or their carrier for operating system, hardware-related issues or applications not affiliated with the Imagine! mobile device management (MDM) applications.

Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

Devices that are used to access company data may be required to be registered through the Imagine! MDM enrollment procedure to ensure proper job provisioning and configuration of standard Imagine! MDM applications, which may include office productivity software and security tools, before they can access the network.

Devices that cannot meet these requirements will not be eligible for support from the IT department and will be blocked from Information Technology systems.

In order to prevent unauthorized access, devices must be password protected using the features of the device which is required to access the company network. Employees will not download any application or service to their mobile device which allows the password feature to be bypassed for access to Imagine! data.

When devices are registered with the MDM application, the following restrictions will be enforced:

- The device must lock itself with a password or PIN if it's idle for 10 minutes.
- The PIN or password must contain at least 4 characters.
- After 15 failed login attempts, the device will lock. Contacting the IT Department may be required to regain access to company data.

Mobile device features and specifications are subject to change without notification due to technology changes and the sensitive nature of our business.

Rooted (Android) or jail broken (iOS) devices are strictly forbidden from accessing the network. Employees will not modify the operating system of a mobile device in any way that allows them to bypass limitations and protections Imagine! imposes as a condition of connecting to its systems.

Access to company data will be terminated if 1) the device is lost, 2) the employee or employer terminates his or her employment, 3) or IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Imagine! will not take responsibility for the employee's personal data, software, applications or hardware in the event it is remote wiped. It is the employee's responsibility to take additional precautions, such as backing up applications, music, and other personal settings.

Restrictions on authorized use

Employees whose personal devices have camera, video, or recording capability are required to follow Imagine! policies on HIPAA and confidentiality while at any Imagine! facility or function. All protected health information and other client information must be safeguarded, protected, and kept confidential. Individuals receiving services cannot be photographed, videoed, or recorded without a release completed by the individual or guardian.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Imagine! policies pertaining to harassment, discrimination, retaliation, confidential information, and ethics apply to employee use of personal devices for work-related activities.

Excessive personal calls, e-mails, or text messaging during the workday, regardless of the device used, can interfere with productivity and be distracting to others. Employees are expected to handle their personal matters on non-work time.

In accordance with applicable law, Imagine! requires non-exempt employees to obtain the express authorization of their manager or supervisor to work outside of their normally scheduled hours. Access to Imagine! information (such as email) via a mobile device does not constitute authorization to work outside of normally scheduled hours.

Employees may not use their personal devices for work purposes during certain leaves, such as unpaid leave or medical leave, without authorization from their supervisor. Imagine! reserves the right to deactivate company access on the employee's personal device during certain leaves.

Employees are responsible for ensuring that company information and data stored on or accessible from their personal devices remains secure. Employees must delete any client related data (including contact information) and other work related information from their personal device upon separation of employment. Upon separation, employees will arrange for IT to have Imagine! applications and related information removed from their phones.

Privacy/company access

No employee using her or his personal device should expect any privacy except that which is governed by law. Imagine! has the right, at any time, to monitor and preserve any communications that use the Imagine! networks in any way, including data, voice mail, telephone logs, internet use and network traffic, to determine proper use.

Imagine! may have incidental access to personal information on personal devices. In such event. Imagine! will only review, retain, release, or disseminate personal and company related data on personal devices as required by law to government agencies and its representatives in the event of an investigation or litigation. Imagine! may review the activity and analyze use patterns, as it relates to use of the personal device for work purposes, and may choose to publicize these data to ensure that Imagine!'s resources in these areas are being used according to this policy.

Company stipend

Employees authorized to use personal devices under this policy may receive an agreed on monthly stipend based on the position and estimated use of the device. If an employee obtains or currently has a plan that exceeds the monthly stipend, Imagine! will not be liable for the cost difference. Imagine! reserves the right to terminate or modify the stipend. The stipend does not constitute an increase to base pay and will not be included in any calculations of base pay.

Safety

Employees are expected to follow applicable local, state, and federal laws and regulations regarding the use of electronic devices at all times.

Employees are expected to refrain from using their personal devices while driving for work. Employees are required to use a hands free device or pull off to the side of the road and safely stop before accepting a call or texting.

Employees who are charged with traffic violations resulting from use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost, stolen, hacked, or damaged equipment

If an employee device is registered with the MDM application and the device is lost or stolen, the employee must notify the Imagine! IT department immediately.

IT will terminate access to company data upon notification of the following:

- Termination of employment
- Lost or stolen device
- Devices no longer in use by the employee

Violations of policy

Employees who have not received authorization from Imagine! will not be permitted to use personal devices to access company data.

Imagine! reserves the right to modify or disable (or both) an employee's access to Imagine! systems any time that the user violates the BYOD Policy or such a violation is reported. Imagine! may take any one or more of the following actions (in any order Imagine! deems necessary), in its sole discretion, in response to a reported or otherwise discovered violation:

- Issue verbal or written warnings.
- Suspend or terminate the user's Imagine! MDM account or service.
- Wipe all company data from the employee's device.
- Run reports on the employee's device usage of company resources.
- Capture company data from the employee's device.
- Terminate the user's employment.
- Pursue legal remedies for violations.