MANAGEMENT OF INFORMATION SECURITY & AVAILABILITY OF INFORMATION (rvs 21-11)

Executive Summary

At Refuge House, information is the backbone that supports the services we provide to families and children. Having access to accurate complete and accurate information enables our personnel and service providers to make informed assessments and decisions regarding the services provided to our children and families. Without this information, we encounter barriers to the delivery of service that are unnecessary and, in some cases, may also be harmful or counter productive. Another facet of information availability is the securing of information so that unauthorized parties do not have access to the information, or parties have limited access to information that could be considered harmful.

Information Management and Use

(RPM 5; RPM 5.01; RPM 5.02; RPM 5.03; FIN 1 a, b, c, e; PQI 1.04; FIN 2; FIN 5; FIN 6; FIN 7; FIN 8; PQI 4; RPM 6; RPM 7; RPM 8; TS 2.03)

Refuge House makes continuous efforts to remove barriers to information availability in order to support operations and enhance service delivery. The organization routinely evaluates both the availability and speed of access to information by reviewing physical infrastructure, tools, software, methodologies to obtain, record, store, access, review or distribute information. Refuge House information systems must be routinely reviewed and assessed to ensure that the information management system has the capacity to support the organization's operations, planning and evaluation.

- Unavailable or inaccurate information may reduce the quality of care or cause harm to a service recipient.
- Obstacles to data access may cause frustration by personnel, negatively impacting service delivery and personnel or service recipient satisfaction.
- Unavailable, incomplete or inaccurate information may indicate a failure to comply with licensing or regulatory standards.
- Refuge House has selected a completely cloud-based solution to implement our corporate Information Systems infrastructure, including data failovers, ease of access, strong security profiles, redundancy, extensibility and professional management and support.
- The cloud-based information system methodology permits secure access to records by personnel at any allowable time, from a variety of authorized locations.
- Refuge House uses a completely electronic solution to store, access, maintain, review and manage the following records: child, family and caregiver, contracted service providers, as well as financial records.
- Electronic records are stored in a secure and consistent manner, ensuring that records are not lost or misplaced, either intentionally or accidentally, ensuring

continuity and integration of care across settings.
- Records that are distributed outside the organization are de-identified/redacted according to legal and regulatory guidelines.

Refuge House may access electronic backups of data in the event of a failure of electronic systems. The cloud-based solution provides a number of redundancy and fail-over solutions in the event that a physical system becomes unavailable.

The primary responsibility for the security and availability of data rests with the Information Services department, working in conjunction with the contracted IS providers.

Records are made available to authorized personnel only, according to their role within the organization, as well as their relation to other individuals, including other personnel and service recipients. The nature, breadth and depth of information is dependent upon the user's unique login and their assigned jurisdictions.

Case records, personnel records and company management records are stored, accessed, maintained, reviewed and managed in the Radius Solutions data management system. Access to Radius Solutions is only available to individuals through the virtual desktop environment, which is secured by a domain login provided by Refuge House. (HR7)

Financial records are stored, accessed, maintained, reviewed, managed and reports generated in QuickBooks, which is accessed by secure login through CPAASP. CPAASP is a secure SaaS platform used by financial companies.

Radius stores and formats records according to a pre-determined configuration, unique to each type of file. Radius provides the ability to convert and store both electronic and paper record types in a consistent manager within a predictable and secure case record structure. All activity in Radius, including record updates and the addition of information and documents, is "fingerprinted" with the user's unique identity and the date and time of the particular type of activity. Data and reports may be reviewed and reported in a longitudinal fashion. Because information is stored and managed in Radius in a logical and consistent format, the framework for the process of extracting, formatting, reporting and disseminating data is also be consistent.

Financial information, including Payroll, is stored in Quickbooks, with supporting information being scanned and stored in an electronic file system managed by the Finance Office. Refuge House maintains an account with CPAASP, which is a SaaS provider supporting financial companies. Quickbooks is accessible through CPAASP, secured by unique login, and accessible only to individuals specifically responsible for

financial data. Quickbooks is an industry standard electronic financial accounting package that provides a framework for storing and managing financial data according to sound financial practice and GAAP. The payroll function within QuickBooks provides routine updates to the software that ensure currency of tax rates, state and federal tax regulations, including FICA and compensation reporting. The Finance Office accesses Quickbooks in order to enter financial information, conduct ongoing financial activities, analysis, comparison and budgeting, generate reports, manage payroll, maintain vendor and customer records, and prepare financial statements for Management, including routine reports for Executive and Board review on a monthly, quarterly, yearly and ad-hoc basis. (*FIN 1 a, b, c, e, FIN 2, FIN 5, FIN 6, FIN 7, FIN 8; PQI 4)*

Continuous, as-needed.

Security of Information

(RPM 6, RPM 6.01 a, b, c, d; RPM 6.02; RPM 6.03; RPM 6.04; RPM 6.05; RPM 2.01;)

Electronic and printed information is protected against intentional and unintentional destruction or modification and unauthorized disclosure or use.

- Unauthorized access to information can result in legal and regulatory exposures.
- Unauthorized access to information can result in a negative impact on a service recipient.
- Refuge House digitizes all paper documents and stores them in electronic format that is secured by unique user login. Historical records are scanned and stored in the electronic system.
- Refuge House shreds any document that has been digitized, provided the document that is not the only legal instrument in its original or certified form. Refuge House engages a bonded document shredding service to destroy documents.
- Documents that require storage as a physical document are stored in a fireproof safe or a safety deposit box. Refuge House limits access to physical documents to required personnel.
- Refuge House policy prohibits client information to be left in any location that is accessible by the public, or by any unauthorized individual. This includes copy machines, physical desktops, and trash receptacles.
- Radius does not provide a delete function to users, except for the Global Administrator, who must complete multiple steps in order to remove any record.
- Radius Solutions enforces an extremely granular record access framework that is based upon a user's unique login and the jurisdictions assigned to the user's role in the organization and the user's relationship to other entities (children, families, employees) within the organization.
- Refuge House secures confidential information and meets HIPAA requirements by

ensuring that any access to electronic information stored in the case record management system (Radius) is secured by multiple unique logins.

- Refuge House implements an automatic timeout feature for every session, ensuring that an individual cannot leave secure information visible on their computer screen after a certain time interval.

In the event that unauthorized access to records is identified, Refuge House personnel will take initial steps to identify the source of the problem and prevent any further unauthorized access. Immediately following that, specific exposure of any individual (service recipient, employee, Board Member, contractor, etc.) will be addressed in order to prevent direct or indirect harm. Refuge House IS or the responsible department manager will develop a plan to prevent future unauthorized access or dissemination of information.

In the unlikely event that data is determined to have been lost, IS may request access to data backups in order to restore the lost information.

All personnel are responsible for ensuring that information is appropriately used and secured against unauthorized access or distribution.

IS Management is responsible for ensuring that appropriate rules for access of records are implemented in Radius based upon business rules, as well as ensuring the data systems are in compliance with federal and state regulations, including privacy laws, segregation of duties requirements, confidentiality policy, and HIPAA requirements. IS Management ensures that only authorized personnel have access to financial records.

Access to and activities within case files, company files and personnel files are configured by each user's specific jurisdiction and authority within the record type based upon a detailed security matrix that is developed by the Program Director, Quality Development and Operations Director, unless otherwise dictated by written policy and procedure. Access to files of specific individuals within the organization is dependent upon specific assignments to the user.

Financial Data is maintained on a separate framework from the organization's main operating framework. No unauthorized personnel may access the framework upon which the financial information resides. Only Executive Management and the Finance Office are authorized to access financial data through CPAASP and QuickBooks.

Data systems are secured by access and restricted by user roles. Physical documents are secured by location and physical locks.

Refuge House utilizes a cloud-based data access and storage solution that has

redundancy and backup procedures built in. Data, by virtue of this framework, is backed up and stored off-site, reducing any risk that damage to the organization's physical office will result in damage to the case records, personnel or company records in the electronic data system. The cloud provider has infrastructure and data redundancy and fail-over procedures that are automatically implemented when there is damage or failure of any component. Also built-in to the cloud framework are firewall and antivirus features, as well as ongoing system monitoring and other safeguard features that identify potential or actual issues and alert the provider's technicians immediately.

Refuge House maintains electronic records perpetually, including adoption and foster child records. Data may be archived in the Radius Solutions system; however the data is never purged from electronic archive. In the event that the company is dissolved, adoption records will be discharged to the Adoption Registry. Refuge House will consult the authority for other child records to obtain information from that entity regarding the disposition of case records.

In the event that confidential information is delivered electronically, personnel will take every precaution to ensure sensitive or identifying information is safeguarded to the extent possible, and in accordance with applicable regulations. Refuge House has posted the Privacy Policy on the website.

Refuge House has a Web-based Technologies and Electronic Communications policy that is provided to personnel and available via the Refuge House website to stakeholders and service recipients. Refuge House personnel include a privacy and confidentiality statement on the signature for all outgoing emails. Personnel receive training on confidentiality and the security of case records.

Refuge House enforces a policy of multi-tiered logins in order to access case record information. Each user must authenticate first to the Refuge House organization by a unique login and password, and then to the document management system (Radius) by a unique login and password. Refuge House information systems enforce an automatic timeout policy for each session, ensuring that after a specified time interval of inactivity, the user's screen will go to a screensaver or blank screen and require a password to reactivate the session.

Refuge House maintains an account with CPAASP, which is a cloud-service provider for financial operations. CPAASP manages and maintains updates to QuickBooks, as well as secure routine backups of the QuickBooks data. Access to Financial data is only obtained through login to the CPAASP website (not on the Refuge House cloud framework) and by

a second login to open the QuickBooks file.

Ongoing

Access to Records

(RPM 8; RPM 8.01 a, b, c, d, e, f; RPM 8.02 a, b; RPM 8.03 a, b)

Service recipients or designated legal representatives can access their case record, consistent with legal requirements. In many cases, a child may be required to review and sign documents in their own case file, however due to the nature of the services provided by Refuge House, and the fact that children may not understand how to keep their own information secure, this information is not provided in physical copy to the child.

Individuals may request access to specific information contained in a child's file, which is authorized by the child's DFPS (Texas Department of Family and Protective Services) or the court of jurisdiction. Internal personnel, as well as external parties (DFPS, court officials) must review and handle records in a manner that is consistent with Refuge House privacy and confidentiality policies. Refuge House ensures that the child's guardian (DFPS) provides written authorization for release of information to third parties, including contracted service-providers.

- An individual's right to review his or her care or treatment may be denied, or otherwise limited, only in the most extreme circumstances where serious harm is likely to ensue. In such cases, objective criteria must guide decisions to deny access. In all cases, the Refuge House will operate in accord with applicable law.
- In some cases, if information contained in a file is deemed harmful to a child, then this information will not be made available to the child.
- At any time, a child may request access to the following information contained in their file, but information must be reviewed to ensure no violation of security or confidentiality.
- Case information should not be left in public areas such as on carts in hallways, on desks, or in non-secured areas. When not being used by authorized personnel, files should be returned to a secure area.
- Records are reviewed by service recipients with a service professional, and in a manner that ensures confidentiality.
- Refuge House ensures that access to a child's case file is secured by unique user logins.
- Any individual who accesses confidential information about a client shall be provided a copy of the Refuge House privacy and confidentiality policy, and return a signed copy which will be maintained in the appropriate record.

See Responding to Risk under Security of Information

It is the responsibility of all staff and contractors at Refuge House to ensure that confidentiality is maintained for all clients and personnel.
A child or the child's legal guardian (DFPS), auditors, contractors, and licensing or accrediting personnel and court officials may request access to any information in the child's file. Also, an Agency into whose care the child is transferring may request to receive information in the child's file.

A foster child in the care of Refuge House has access to specific information in his/her own case record, in accordance with the child's developmental level, legal authorization to review the information, degree to which the information is not considered harmful by the child's treatment team, and the nature of which does not infringe upon the confidentiality of family members and others whose information may be contained in the record.

External parties may request information from a child's record, however the entity must be legally authorized to receive that information. A written release of information is required from the child's guardian in order to provide confidential information to a third-party requestor.

In order to ensure that case file information remains secure, the child is not provided with physical copies of documents containing sensitive information that is specifically identifiable with that child. However, a child may request access to specific information in their file, which can be provided to the child by a foster parent or case manager. This information will be presented to the child either electronically, using Radius, or may be presented to the child at the Refuge House facility where considerations for privacy are ensured.

If Refuge House determines that it would be harmful for a service recipient to review his/her case record, and applicable law provides no guidance on case record access, then the Treatment Director reviews, approves in writing, and enters into the case record the reasons for refusal and procedures permit, and the Treatment Director reviews the record on behalf of the child.

When a child/young adult is discharged to another agency or residential child care operation, the Refuge House will draft a letter on letterhead and submit to the child's managing conservator or young adult's DFPS caseworker requesting legal authorization to release discharge and related information to the receiving agency. Refuge House will

document requests to obtain authorization to release discharge information in the child's or young adult's record. If the consent is approved by the managing conservator or DFPS caseworker, the Agency has 15 days to provide this information to the receiving operation. The requested information includes:

- Discharge Summary
- Child's or young adult's background information, including progress notes for the past 6o days
- Unresolved incidents or investigations involving the child/young adult
- Assessment/evaluations for the child/young adult, including admission assessment, diagnostic assessment, educational assessment, neurological assessment, psychiatric or psychological evaluation
- Service plans for the past 12 months
- Medications the child/young adult is taking (including dosage, frequency, reason for the med)
- Treatment for a physical condition that is in progress and requires continuing or follow-up medical care

Any information provided to an external party must be appropriately de-identified/redacted to ensure confidentiality of any party whose information may also be contained in the file.

As applicable.

Case Records

(RPM 7 a, b, c; RPM 7.01; RPM 7.02 a, b, c, d, e, f, g, h, i, j, k; RPM 7.0; RPM 7.03 a, b, c; RPM 7.04 a, b, c, d; RPM 7.05 a, b; RPM 7.06 a, b; RPM 7.07; PQI 4.02 a)

The ability to review complete and accurate case records is a critical component of providing quality services to clients. Refuge House utilizes sound documentation practices, and maintains current, accurate and complete records for each individual service recipient. Refuge House records are maintained in the Radius Solutions document management system, ensuring that each records is constructed in a consistent format, contains the minimum required identifying characteristics, and will be easily searchable. Well-maintained records can help shield the organization from allegations of misconduct and negligence, while poorly-maintained records and improper documentation are a known liability. Every case record for a Refuge House service-recipient clearly identifies the consumer, supports decisions about services provided to the individual, and appropriately documents the delivery of services.

- A foster/adoptive child or foster/adoptive family record does not contain required legal or regulatory information.

- A foster/adoptive child or foster/adoptive record is not recorded in a consistent format.
- Entries into a record are not accurate or complete.
- Entries into a record do not identify the date, time and person entering the data into the record.
- An individual's record does not contain information necessary to support service decisions for the individual.
- Each individual involved in the service delivery process (including foster/adoptive children, foster/adoptive parents, employees, etc.) has a Radius file that information appropriate to the individual and as required by legal and regulatory entities.
- Each record maintained in the Radius Solutions system is automatically configured and formatted according to the type of record, i.e. child record, family record, parent record, etc.)
- Internal documents (i.e. documents that are created and used by Refuge House in the course of service delivery) are pre-set and incorporate all necessary legal and regulatory elements. Individual users do not have the ability or authority to modify document elements.
- Refuge House employs certain automated features into each document that either pre-fill or notify users when required information is incomplete.
- Many documents required multiple signatures, ensuring that a second party reviews the document for accuracy and completeness.
- Some documents prompt the user for required attributes, ensuring that specific key elements are captured by default.
- All entries and updates into Radius Solutions automatically capture "fingerprint" data based upon the system date/time and the user's unique login. A history of record updates is maintained for each internal Radius Solutions document.
- Each type of Radius Solutions record is configured to reflect the specific documentation requirements that support the service-delivery needs of that type of consumer.
- Each type of Radius Solutions record provide an "auditing" feature that allows the Quality Development department to identify business rules (which reflect legal and regulatory requirements) enabling an authorized individual to identify any gaps in the documentation and address those issues directly.
- A random sampling of case records is reviewed each quarter to ensure compliance with applicable legal, regulatory and quality standards.
- Users log in to Radius using a unique login that is tied to particular levels of authorization in each type of case file, limiting the activities the user may perform according to the rules defined by the Program Director and Quality Development
- When a global gap in documentation is identified, the Quality Development department may define a new type of record to be incorporated into a particular type of record.
- When a specific deficiency in a record is identified, the Treatment Manager,

Adoption Director or Treatment Director implements steps to obtain or correct the specific documentation deficiency.

It is the responsibility of the Information Systems department to ensure the availability and operation of the Radius Solutions system.

It is the responsibility of the Program Services department to work in conjunction with the Quality Development department to define the specific documentation requirements and configure each record type according to necessary legal, regulatory and quality of service delivery standards.

It is the responsibility of the Case Manager/Intake Worker/Adoption Worker/Home Developer to ensure the completeness and accuracy of records added or incorporated into each record.

Quality Development director ensures that a random sample of case records (current cases and cases discharged the prior quarter) is selected each quarter. Program Director ensures that each selected record receives a thorough peer review and that an auditing tool is completed and recorded in each record.

Only authorized personnel can enter information into or update records.

Case Manager is the primary person responsible for foster/adoptive child files.

Case Manager and Home Developer are primarily responsible for foster home (and related) files.

HR Department is primarily responsible for personnel files.

Operations Department is primarily responsible for contractor files.

Every record (employee, contractor, foster/adoptive child, foster/adoptive parent, substitute care-provider, home resident, etc.) contains the following basic information:

- First, Middle, Last Name, Common/Preferred Name
- Unique number identifying the record
- Date of Birth
- Address and contact information
- Demographic Information

Each child case record for whom the foster/adoptive child has been in care for a sufficient length of time to warrant each item, contains the following information:
***the following list is not comprehensive, but indicates compliance with accreditation*

standards

- Demographic information
- Contact information for the child's DFPS worker, ad-litem/CASA worker (contact information)
- Refuge House Placement history, including date of placement and family contact information (contact information)
- Court order and DFPS common application (reason for referral)
- Up-to-date Assessments and Evaluations (Admission Assessment, Psychological, Psychiatric, Medical/Dental, Educational/Developmental, Initial Health Screening, Diagnostic Assessments)
- Details on Medical and Psychiatric care (including treatment plans, diagnoses, prescription info, medication logs, consent for psychotropic medication, notification of DFPS)
- Current Individual Service Plan (includes goals and objectives)
- Intake Documents
- Legal Documents (Placement Authorization, DFPS Placement Acknowledgement & Consent, Medical Consent Authorization, Orientation and Child Rights/Grievance Procedure, Court documents, birth certificate and social security number, Medicaid card)
- A description of services provided directly or by referral
- Documentation of Services (Therapy, Psychiatric Care, Medical/Dental, Recreational, Educational, Developmental, etc.)
- Discharge Summary, including aftercare and ongoing needs of the child (when applicable, incorporated within 30 days of discharge)
- Weekly Case Review notes (includes progress, foster/adoptive parent notes, case manager notes/observations, input/statements from foster/adoptive child, any visits or recreational activities, upcoming appointments, significant issues, electronic signatures of foster/adoptive child if able, foster/adoptive parent, case manager)
- Documentation of Supervisory Review (Weekly Case Review by Treatment Manager or Treatment Director or Program Director)

The absence of any required item in the case record is explained by a File Note in the appropriate location.

Family records contain information on each individual in the home, as well as a file for home/family specific information. Documents meet all the criminal background check, legal, agreements and acknowledgements, training and historical information required by RCCL licensing, contract and accreditation standards.

Employee and contractor records contain information for each individual, including

background information, criminal background, training and education, acknowledgements and agreements. Documentation meets all requirements of RCCL licensing, contract and accreditation standards.
Business rules associated with each file type limit or allow activities within that file by a user's login and jurisdictions. This ensures that only authorized individuals may perform certain actions within a file, or within a particular document in that file. The particular authorizations are determined by the user's assigned role(s) and the type of file and document, specifically the rules define whether the user may or may not view, edit, add, hide, print/export, sign, or verify the file. Additionally each user has assigned relationships within Radius, which may also limit the files the user may access by person, as well as by role.

Entries into the child's case record are clearly structured by each type of document, so that information needed is captured in a specific, factual, relevant and legible fashion. Specific timelines are associated with most types of entries, but company policy dictates that any entries into the record must be within 15 days of cycle completion for non-critical records, and sooner for many types of records. Weekly Case Reviews are entered at each visit and reviewed no later than the 3rd day of the following month. Records provided by contracted service providers must be completed, signed and dated by the person who provided the service. Any records requiring supervisory review are signed and dated by the supervisor or treatment professional as applicable.

Upon discharge, the Case Manager completes a Discharge Summary and incorporates other discharge documentation as applicable. The record is moved to the "Foster Child – Discharged" jurisdiction and is maintained indefinitely. Refuge House ensures that any ancillary information (unsummarized notes, impressions, and personal observations) are expunged from the record.

Prior to verification, the Foster Home Developer ensures that all necessary documentation requirements are included in the files for each family, foster/adoptive parent, and any other home resident. Foster Home Development and Case Manager make ongoing updates to the Home/Family files on an ongoing basis and ensure that expiring documents are replaced or updated. Case Managers maintain ongoing reviews of each home, which are updated semi-monthly and closed each quarter.

Upon employment, all pre-employment documentation requirements are incorporated into each employee's file. Documentation requirements include background check information, education, training, application, benefits information

Documentation within each file is ongoing.

Training

Refuge House firmly believes that appropriate and adequate training is one of the foundational pillars of Risk Prevention. To that end, Refuge House is committed to training all personnel and foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers on matters that are the most critical to providing a safe and positive environment and ensuring the quality of service, as well as avoiding potential risks and barriers to service delivery.

- A foster/adoptive parent, substitute care-provider or other resident of the home is not adequately trained, leading to ineffective care or further neglect or abuse for a foster/adoptive child.
- An employee is not adequately trained in service delivery, leading to inability to provide appropriate support to foster/adoptive parents or inability to provide adequate assessment and case management activities.
- An employee is not adequately trained on operational issues, leading to poor performance or legal issues.
- Refuge House provides required pre-service training to foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers and employees.
- Refuge House provides required ongoing training to foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers and employees.
- Refuge House develops yearly training plans for foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers to meet minimum standards and COA requirements, as well as optional/elective trainings to enhance service delivery.
- The PQI committee monitors progress in ongoing training on a quarterly basis.

When a gap in training is identified, either individually or for a group as a whole, Refuge House ensures that a training or program is implemented to address the gap.

It is the responsibility of the Home Developer to ensure that foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers complete required pre-service training prior to verification, as well as to ensure that ongoing training is current.

It is the responsibility of each department's manager to ensure their staff has completed pre-service training, as well as to monitor their ongoing training and identify areas that

need further training.

All employees are required to complete general training on human resources and office policies. Individuals involved in treatment or Program Services may require additional training specific to the nature of their job.

All foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers must complete pre-service training, as well as maintaining a minimum number of required ongoing training and elective training hours.

The nature and number of trainings required may vary by employee, but must meet RCCL minimum standards and contract requirements, as well as requirements specified by accreditation standards.

Foster/adoptive parents, other residents of the home (as applicable) and substitute service-providers must complete pre-service and ongoing training that meets RCCL minimum standards and contract requirements, as well as requirements specified by accreditation standards.

The specific trainings and hours may vary by individual and the nature of their involvement with foster/adoptive children. Each individual will have a training plan that is developed according to their needs and in accordance with the nature of their involvement with foster/adoptive children. The specific requirement are based upon the following:

- RCCL minimum standards
- DFPS contract requirements
- COA accreditation standards
- Current experience and qualified verifiable training
- Gaps in the individual's experience or knowledge

Once the Home Developer begins the verification process with a home, each individual in the home is assessed for training needs, including foster/adoptive parents, other adults living in the home, young adults nearing the age of 18, and any substitute care-providers who may assist the home in the care of the children. Each individual must complete training pre-requisites, however certain individuals may not require a full battery of training requirements if their involvement with foster/adoptive children will be limited. The Case Manager or Home Developer will record any trainings and attach the certificate in the individual’s Radius binder.

Upon employment, each new employee receives the general human resources and office policy training. Personnel who will are responsible for any aspect of treatment, including

Case Manager, Treatment Managers, Treatment Directors and Program Managers must complete a full battery pre-service training, usually aligning directly with foster/adoptive parent training. Depending on the nature of their job, some employees may require additional program-specific training in order to perform their work duties. The Department manager will forward any certificates to Human Resources to incorporate into the individual's Radius binder.

A history of all training, including certificates for each training, is maintained in each individual's Radius binder, providing necessary information for monitoring of training requirements and expiring training.

Each Department manager may review training for their personnel in Radius. The Program Director reviews Foster/Adoptive and Program Services personnel for status on training requirements on a monthly basis.

The Home Developer reviews Foster/Adoptive homes for status on training requirements on a monthly basis. .

Case Manager provides information on upcoming due dates and training requirements for each foster/adoptive parent during Home Reviews, either by phone or in the home.

Pre-service training requirements are completed prior to verification for foster/adoptive parents, other adults living in the home, young adults nearing the age of 18, and any substitute care-providers.

Employees complete training upon their employment.

Ongoing training requirements are completed yearly.

Training status is reviewed monthly by Department managers and the Home Developer.

PQI committee reviews aggregate data on a quarterly basis.

Policy for Administrative, Technical and Physical Safeguards To Protect Confidential Health Information and Minimize the Risk of Unauthorized Access, Use or Disclosure of Confidential Information

Purpose

The purpose of this policy is to provide information for management and workforce members involving the safeguarding of confidential patient health information and to minimize the risk of unauthorized access, use or disclosure of confidential information

Policy

General

Refuge House must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information.

Safeguarding Confidential Information – Workplace and Workstation Practices

PAPER

Each of Refuge House's workplaces and workstations will store files and documents in locked rooms or storage systems.

In workplaces and workstations where lockable storage is not available, Refuge House's staff and workforce members must take reasonable efforts to ensure the safeguarding of confidential information.

Each of Refuge House's workplaces and workstations will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.

Each of Refuge House's workplaces and workstations will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements and policies.

ORAL

Refuge House staff and workforce members must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.

Each of Refuge House's workplaces and workstations shall make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.

Exception: In work environments structured with few offices or closed rooms, such as open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that Refuge House has met the reasonable safeguards and minimum necessary requirements.

Each Refuge House workplaces and workstation must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

VISUAL

Refuge House staff and workforce members must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.

> **Computer Screens**: Each Refuge House workplace and workstation must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
>
> **Paper Documents:** Refuge House staff and workforce must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

Safeguarding Confidential Information – Administrative Safeguards

Implementation of Role-Based Access (RBA) and the *Minimum Necessary Policy* will promote administrative safeguards.

Role Based Access (RBA) is a form of security allowing access to data based on job function in accordance with Refuge House security procedures. Refuge House's staff and workforce members shall be given access only to the minimum necessary information to fulfill their job functions.

Conducting internal reviews periodically will permit Refuge House to evaluate the effectiveness of safeguards.

All Refuge House managers, supervisors, staff and workforce members, including volunteers and trainees, are required to sign a document constituting a formal commitment and understanding to adhere to Refuge House privacy and security policies.

Safeguarding Confidential Information – Workplace and Workstation Practices

PAPER

> Files and documents being stored:
>
> A. Lockable desks, file rooms, open area storage systems must be locked.

B. Where Refuge House has desks, file rooms, or open area storage systems, that are not lockable, reasonable efforts to safeguard confidential information must be implemented.

Files and documents awaiting disposal/destruction:

A. Desk-site containers: Refuge House's workplaces and workstations will ensure that confidential information awaiting disposal is stored in containers that are appropriately labeled and are properly disposed of on a regular basis.
B. Storage rooms containing confidential information awaiting disposal: Each Refuge House workplace and workstation workforce member will ensure that storage rooms are locked after business hours or when authorized staff or management are not present.
C. Centralized waste/shred bins: Each Refuge House workplace and workstation workforce member will ensure that all centralized bins or containers for disposed confidential information are clearly labeled "confidential", sealed, and placed in a lockable storage room.
D. Each Refuge House workplace and workstation workforce member that does not have lockable storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to confidential information.

Shredding of files and documents authorized consistent with record retention requirements:

A. Refuge House managers and supervisors must ensure that shredding is done timely, preferably on a daily basis.
B. Outside contractors: Refuge House must ensure that such entity is under a written contract that requires safeguarding of confidential information throughout the destruction process.

ORAL

Refuge House staff and workforce members must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs, and should be aware of risk levels.

Locations of verbal exchange with various levels of risk:

A. Low Risk: interview rooms, enclosed offices and conference rooms.
B. Medium Risk: employee only areas, telephone and individual cubicles.
C. High Risk: public areas, reception areas and shared cubicles housing multiple staff where clients are routinely present.

VISUAL

Refuge House staff and workforce members must ensure that observable confidential information is adequately shielded from unauthorized disclosure.

Computer screens: Refuge House managers, supervisors, staff and workforce members must ensure that confidential information on computer screens is not visible to unauthorized persons. Means for ensuring this protection include:

A. Use of polarized screens or other computer screen overlay devices that shield information on the screen from persons not the authorized user;
B. Placement of computers out of the visual range of persons other than the authorized user;
C. Clearing information from the screen when not actually being used;
D. Locking-down computer work stations when not in use; and
E. Other effective means as available.

PAPER DOCUMENTS

Refuge House staff and workforce members must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

Refuge House staff and workforce members must take special care to ensure the protection and safeguarding of, and the minimum necessary access to, paper documents containing confidential information that are located on:

A. Desks;
B. Fax machines;
C. Photocopy machines;
D. Portable electronic devices (e.g., laptop computers, palm pilots, etc.);
E. Computer printers; and
F. Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

Safeguarding Confidential Information – Administrative Safeguards

Role Based Access (RBA): Roles will be created and defined based on the information in Refuge House's possession and where it is located and how it is used and why. A determination of who should have access to the specific data will be established.

Refuge House managers and supervisors will decide the role of each of their staff and workforce members and request exceptions based on the needs within their jurisdiction or area of responsibility.

Managers are responsible for allowing access to enough information for their staff and workforce members to do their jobs while holding to the Minimum Necessary standard and policies.

Refuge House's managers and supervisors will:

A. Follow all instructions and policies to safeguard confidential information;
B. Foster a secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving Refuge House's **privacy** goals.
C. Assess and update as necessary the safeguards in place every 6 months, seeking to achieve reasonable administrative, technical and physical safeguards.
D. Utilize all security policies to augment safeguard procedures.

Enforcement

Refuge House's office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

Policy for Ensuring Confidentiality of Protected Health Information By Workforce Members While Away from Facility(s)

Purpose

The purpose of this policy is to provide information for management and workforce members regarding procedures for best practices for workforce members to utilize when away from the organization's facility(s).

Definitions

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

Individually Identifiable Health Information: Any information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse; and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual

Authorized Persons: Those individuals involved in the treatment, payment or health care operations pertaining to the subject of the PHI.

Designated Record Set: A group of any records under the control of a covered entity from which personal health information is retrieved by the name of the individual or by identifying number.

Vehicle: Any mode of transportation utilized in Refuge House's business.

Patient: Any individual who has received or is receiving services Refuge House

IS Manager and/or Quality Personnel: The person officially designated to oversee all ongoing activities related to the development, compliance, implementation, maintenance of, and adherence to the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state laws that may apply.

Policy

General

PHI that is unattended shall be secured in a manner to protect such information from persons without authorized access to this PHI.

Vehicles containing any PHI shall be kept locked while unoccupied. PHI shall be kept locked in the trunk of the vehicle, when possible. In the event of extreme temperature situations, an electronic device (laptop, personal digital assistant (PDA), etc.) containing PHI shall be maintained in the temperature controlled cab in a case while the vehicle is occupied.

In the event of a vehicle accident any Refuge House employee who suspects there is PHI in the vehicle shall make every reasonable attempt to make sure that the PHI is not accessible to anyone who does not need to have access to it, after assuring the health and safety of any individual(s).

Upon an employee leaving an area where they have materials containing PHI, e.g. to use the restroom, the employee shall take the materials with them or ensure that the area is protected from viewing by those without authorization by locking the area, or informing Refuge House's personnel if they are facility records, or using some other reasonable intervention.

Electronic devices containing PHI and other forms of PHI shall not be left in a hotel room for the day when cleaning service is expected. Upon leaving the hotel, employees shall take these items with them or ensure they are locked in the valuables area at the front desk or locked in a safe in the room if one is available. Should this not be possible, each document that is contained on the laptop shall be password protected on an individual basis.

Employees shall travel in the field taking only PHI necessary to carry out their duties.

Any documentation or equipment such as laptops, pagers, briefcases, palm pilots, etc. that may contain PHI shall be secured from access by those without authorization to the PHI. This includes all locations including an employee's home. Each document that is contained on the laptop shall be password protected on an individual basis.

If a designated record set is checked out from Refuge House's facility, the medical records policy of Refuge House shall be followed. Careful consideration should be used to determine whether checking out any original records containing PHI is appropriate, and what measures may be used to secure these when unattended.

Data contained on all laptops, etc., should be backed-up to a disk or to the network when at all possible to avoid loss of valuable consumer protected health information.

If PHI in any form is lost or stolen, Refuge House's IS Manager and/or Quality Personnel, or designee, shall be notified as soon as practical, but not to exceed 24 hours, in order to initiate the mitigation process.

PHI that is potentially within view of others, even if Refuge House's staff is present, shall be protected in a manner that such information is not communicated to persons without authorized access to this PHI.

All PHI within a vehicle shall be maintained so as to protect from plain view through the windows of the vehicle.

Any electronic device containing PHI shall not have the screen placed in view of others and if left unattended briefly, a screen saver with password shall be employed consistent with Refuge House's security and information systems requirements.

All documentation containing PHI shall be maintained out of the view of unauthorized persons.

1. While working with PHI, the employee shall keep the documentation within line of sight or within arm's reach.
2. This documentation shall be viewed in the most private settings available.
3. Only PHI documentation necessary for the task at hand shall be in view.
4. Briefcases containing PHI shall remain closed when not in use.
5. When having PHI material copied, the employee shall ensure that this material is only viewed by authorized persons.
6. When the employee is finished with reviewing records containing PHI, the records shall be returned to Refuge House's personnel and secured prior to the field employee departing, or in the case of an ongoing audit or investigation, etc., at the time of completion.

Employees shall send and receive faxed materials containing PHI to and from Refuge House's locations only, unless such locations are not readily available and timely transmission of records is necessary for safety needs. If in non- Refuge House's **locations**:

1. When sending or receiving a fax containing PHI, the employee shall ensure only those authorized to view have access to the material during the process of transmission.
2. The fax cover sheet shall not contain PHI.
3. Upon sending or receiving material containing PHI, the employee or designee shall call the location to verify with the sender or the receiver that the transaction was successful.
4. The employee shall be waiting to receive the fax at the fax machine when the transmission is expected if the material could be accessed by those without authorization to view the PHI.

To ensure confidentiality, field based employees shall not wear identification badges in public areas where they are conducting business with those individuals receiving services Refuge House

1. Any Refuge House identifying information shall not be in plain view such as agency logo on a notebook or briefcase, etc.
2. However, Refuge House staff shall wear badges or identification if they are accompanying a consumer within the facility or to a hospital, clinic, doctor's appointment, or some other formal appointment.

When using sign language interpreters where PHI may be transmitted, the most private setting available out of view of others shall be used.

PHI that is verbally transmitted to others shall be protected in a manner that such information is not communicated to persons without authorized access to this PHI.

Conversations where PHI is discussed shall occur in the most private settings. There shall be as much distance as possible between any individuals without authorized access to the PHI.

Conversations where PHI is discussed shall occur with the employee using a volume level which cannot be overheard by those without authorized access to the PHI. This includes telephone conversations. If there is no way to prevent being overheard, a specific code shall be used to identify an individual such as chart number, or consumer initials.

1. The employee shall make every effort to keep the volume level of all participants low enough so as to not be overheard.
2. Conversations shall involve using only the first name of an individual whenever possible.

Wireless/cellular and cordless telephones shall be used for communicating PHI only if necessary.

1. Home cordless telephones can be monitored up to one mile away. The employee shall switch to their regular landline telephone (if available) or digital cellular telephone for increased security if they receive a call on a cordless telephone. Employees shall not communicate PHI on a cordless telephone, unless using a code specified above.
2. There is currently no device to monitor digital cellular telephone calls, so PHI discussions are currently acceptable. The employee shall not communicate PHI on analog cellular telephones, unless using a code specified above.

PHI that may be shared with others in the course of an employee carrying out duties shall be protected in a manner that such information is not communicated to persons without authorized access to this PHI.

When the use of an interpreter is required, the following minimal requirements shall be ensured:

1. The interpreter shall not be an immediate family member or close family friend of the subject of the PHI, unless the subject of the PHI consents.
2. The interpreter shall not use or disclose any PHI obtained as a result of providing interpretation services. If at all possible, the interpreter shall sign a confidentiality agreement.

Enforcement

Refuge House office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

Policy for Discipline and Dismissal

Purpose

The purpose of this policy is to define the disciplinary and dismissal policies and procedures to workforce members when breaches of the HIPAA Privacy Regulations and Refuge House policies occur.

Policy

All employees are expected to acquaint themselves with performance criteria for their particular job and with all rules, procedures, and standards of conduct established by Refuge House An employee who does not fulfill the responsibilities set out by such performance criteria, rules, procedures, and standards of conduct may be subject to disciplinary action.

Conduct which is Subject to Disciplinary Action

Work Performance

Failure of an employee to maintain satisfactory work performance standards constitutes good cause for disciplinary action which may include dismissal. The term "work performance" includes all aspects of an employee's work.

• Work performance is judged by the supervisor's evaluation of the quality and quantity of work performed by each employee.

• When, in the opinion of the office manager or supervisor, the employee's work performance is below standard, the office manager or supervisor should take appropriate disciplinary action.

Misconduct

All employees are expected to maintain standards of conduct suitable and acceptable to the work environment. Disciplinary action, which may include dismissal, may be imposed for unacceptable conduct. Examples of unacceptable conduct, as applicable, include but are not limited to:

• Falsification of time sheets, personnel records, or other institutional records.

• Neglect of duties, or wasting time during working hours.

• Misappropriation of Refuge House’s resources.

• Improper use or disclosure of a patient's Protected Health Information (PHI).

• Improper storage, copying, printing, and disposal of PHI.

• Creating or developing PHI documents that are greater than the minimum necessary for the specific task.

• Smoking (except in designated areas in Refuge House’s facilities).

• Gambling, including participation in lotteries or any other games of chance on the premises at any time.

• Soliciting, collecting money, or circulating petitions on the premises other than within the rules and regulations of Refuge House

• Bringing intoxicants or drugs onto the premises of Refuge House, using intoxicants or drugs, having intoxicants or drugs in one's possession, or being under the influence of intoxicants or drugs on the premises at any time.

• Disregard for or failure to adhere to established internal controls.

• Abuse or waste of tools, equipment, fixtures, property, supplies, or goods of Refuge House

• Creating or contributing to unhealthy or unsanitary conditions.

• Violations of safety rules or accepted safety practices.

• Failure to cooperate with a supervisor or co-worker.

• Impairment of function of work unit, or disruptive conduct.

• Disorderly conduct, horseplay, harassment of other employees (including sexual harassment, or use of abusive or profane language on the premises.

• Fighting, encouraging a fight, or threatening, or attempting to cause or causing injury to another person on the premises.

• Neglect of duty or failure to meet a reasonable and objective measure of efficiency and productivity.

• Theft, dishonesty, or unauthorized use of Refuge House property including records and confidential information.

• Creating a condition hazardous to another person on the premises.

• Destroying or defacing Refuge House's property or records or the property of a student or employee.

• Refusal of an employee to follow instructions or to perform designated work that may be required of an employee or refusal to adhere to established rules and regulations.

• Repeated tardiness or absence, absence without proper notification to the supervisor or without satisfactory reason, or unavailability for work.

• Violation of policies or rules of Refuge House

Procedure

All incidents that involve the potential for disciplinary action shall be investigated by Refuge House's office manager or employee's supervisor or other designated administrative official. If the investigation results in evidence that establishes with reasonable certainty that the employee engaged in conduct which warrants disciplinary action, the office manager or employee's supervisor shall follow the pre-disciplinary hearing procedures before seeking approval for the proposed disciplinary action.

Pre-Disciplinary Hearing

An employee shall be informed of the basis for any proposed disciplinary action which may result in demotion, suspension without pay, or dismissal and have an opportunity to respond before a final decision is made to take disciplinary action. The hearing serves as an opportunity to avoid mistaken decisions to impose discipline and is not intended to definitely resolve the propriety of the disciplinary action being considered.

There is no prescribed form for a pre-disciplinary hearing. It should be informal. However, before reaching a final decision to impose discipline, the office manager or supervisor shall:

• Inform the employee, in writing, of the reasons for the proposed disciplinary action, the facts upon which the office manager or supervisor relies, the names of any persons who have made statements about the disciplinary incident, and the content of such statements.

• Give the employee access to any documentary material which the office manager or supervisor has relied upon.

• Give the employee an opportunity to respond to the charges either orally or in writing within a reasonable time and to persuade the office manager or supervisor that the evidence supporting the charges is not true. If the office manager or supervisor is not persuaded that the evidence is untrue, the office manager or supervisor may review the evidence and proposed disciplinary action with Refuge House's owner or managing partner or other appropriate authority before proceeding to impose the disciplinary penalty.

Imposing the Disciplinary Penalty

Notice

Upon completing pre-disciplinary hearing procedures and obtaining the approval of the appropriate authority, the office manager or supervisor shall inform the employee in writing of the following:

• The specific incident, conduct, course of conduct, unsatisfactory work performance, or other basis for the disciplinary penalty.

• Any previous efforts to make the employee aware of the need to change or improve work performance or conduct.

• Reference to any relevant rule, regulation, or policy.

• Whether the disciplinary penalty is demotion, suspension without pay, or dismissal.

• The effective date if demotion or dismissal is imposed.

• The specific period for a suspension without pay if applicable, not to exceed five working days.

Effect upon Employee Benefits

An employee who is demoted or suspended without pay continues to accrue vacation and sick leave, to be covered by group insurance, and to be entitled to other employee benefit programs.

If a demotion or suspension without pay is appealed and it is determined that there was not good cause for the demotion or suspension, the employee shall be entitled to payment for wages lost as a result of demotion or suspension.

If it is determined upon appeal that a dismissal was not for good cause, the employee shall be reinstated to the same or similar position and shall be entitled to payment of back wages less any

unemployment benefits received by the employee after the date of dismissal. Employee benefits such as vacation and sick leave shall be credited back to the date of dismissal.

References

45 C.F.R. §164.503(e) (1)

Policy for Electronic Mail Containing Protected Health Information (PHI)

Purpose

The purpose of this policy is to define appropriate standards for secure and effective use of Refuge House's electronic mail system.

Policy

Electronic mail is an integrated tool in Refuge House's business processes. This policy applies to all usage of Refuge House's electronic mail systems where the mail either originated from or is received into a Refuge House's computer or network. It applies to all users including, but not limited to, employees, medical staff, contractors, and volunteers.

User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via Refuge House's electronic mail system.

Electronic mail is intended to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee s job. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Users have an obligation to use e-mail appropriately, effectively, and efficiently.

Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

E-mail should not be used for urgent or time-sensitive communications.

Business e-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

Prohibited Uses:

Use of electronic mail is to be in compliance with all applicable state and federal statutes and Refuge House's policies and procedures. Prohibited usage of Refuge House's electronic mail system includes, but is not limited to:

1. Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner;
2. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
3. Use of e-mail system for solicitation of funds, political messages, gambling, commercial, or illegal activities
4. Disclosure of an individual's personal information without appropriate authorization
5. Transmission of information to individuals inside or outside the company without a legitimate business need for the information.
6. Use of e-mail addresses for marketing purposes without explicit permission from the target recipient.
7. Transmission of highly confidential or sensitive information, e.g., HIV status, mental

illness, chemical dependency and workers compensation claims.

8. Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the company without the express authorization of counsel.
9. Misrepresenting, obscuring, suppressing, or replacing a user s identity on an electronic communication.
10. Obtaining access to the files or communications of others with no substantial company business purpose.
11. Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

This list is not considered all-inclusive. Further questions regarding appropriate use of electronic mail should be directed to the employee's supervisor or **IS Manager.**

Ownership and User Privacy of E-Mail

Use of electronic mail is a part of Refuge House's business processes. All messages originated or transported within or received into Refuge House's electronic mail system are considered to be the property of Refuge House's**.**

All users of e-mail systems do so with the understanding that they have no expectation of privacy relating to that use. Refuge House's reserves the right to access the electronic mail system for the purpose of ensuring the protection of legitimate business interests and proper utilization of its property. Such purposes may include, but are not limited to:

1. Locating and retrieving lost messages,
2. Performing duties when an employee is out of the office or otherwise unavailable;
3. Maintaining control of the system by analyzing message patterns and implementing revisions as needed;
4. Collecting or monitoring electronic communications in order to ensure the ongoing availability and reliability of the system.
5. Recovering from systems failures and other unexpected emergencies; and
6. Investigating suspected breaches of security or violations of policy with probable cause;
7. Electronic mail information is occasionally visible to staff and contractors engaged in routine testing, maintenance, and problem resolution. Staff and contractors assigned to perform such assignments will not intentionally seek out and read, or disclose to others, the content of e-mail.

Confidentiality of Electronic Mail

Users of Refuge House's electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore:

1. Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.
2. When e-mail is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information. These safeguards are as follows:
    a. Information considered confidential or sensitive must be protected during transmission of the data utilizing encryption or some other system of access controls that ensure the information is not accessed by anyone other than the intended recipient.
    b. A notation referring to the confidential or sensitive nature of the information should be made in the subject line.
    c. Confidential or sensitive information may be distributed to multiple recipients; however, the use of distribution lists is prohibited.

d. Confidential or sensitive information is to be distributed only to those with a legitimate need to know.

Retention of Electronic Mail

Generally, e-mail messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an e-mail message, it may be considered a more formal record and should be retained pursuant to Refuge House's record retention schedules.

Refuge House utilizes a Compliance-based email service that ensures emails are backed up and retained for compliance purposes. This ensures that emails are backed up on a continuous basis and may be available even in the event that a communication is deleted or removed by a user.

Provider/Patient Use of E-mail

Use of provider/patient e-mail can facilitate improved communication between an individual and his or her provider. However, due to the inherent risks involved in e-mail use, the following policy considerations must be clearly addressed prior to using e-mail for provider/patient communications.

Patient informed consent and agreement to guidelines for use of e-mail must be documented.

Informed consent should address the following:

a. E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
b. No one can guarantee the security and privacy of e-mail messages. Employers generally have the right to access any e-mail received or sent by a person at work.
c. Highly sensitive or personal information should not be communicated via email.
d. Communication guidelines defined, including, (1) how often e-mail will be checked, (2) instructions for when and how to escalate to phone calls and office visits, and (3) the types of transactions that are appropriate for e-mail.
e. Staff other than the health care provider may read and process the mail.
f. Clinically relevant messages and responses will be documented in the medical record.
g. E-mail message content must include (1) the category of the communication in the subject line, i.e., prescription refill, appointment request, etc., and (2) clear patient identification including patient name, telephone number and patient identification number in the body of the message.
h. Indemnify Refuge House's for information loss due to technical failures.

2. Boundaries for operational staff usage of patient electronic mail must be defined. Considerations include:
   a. All employees, including health care providers, sign a confidentiality and security agreement that addresses electronic technology.
   b. Use of a central address for receipt of all e-mail messages.
   c. Identification of processes to manage triage, routing, response and filing of e-mail messages.
   d. Process to verify that message is from an established patient before responding.
   e. Reasonable precautions to ensure that e-mail responses to patients are not misdirected or otherwise become available to unintended parties.
   f. Use of discreet subject headers such as personal and confidential communication.
   g. Incorporation of all relevant e-mail messages, including the full text of the patient s query as well as the reply to the sender, in patient s electronic or paper medical record.
   h. Obtaining of patient s express authorization prior to any forwarding of patient-identifiable information to a third party such as a consultant or health plan.
   i. Prohibitions on use patient's e-mail addresses for marketing or the supplying of addresses to third parties for advertising or any other use.

3. Technical security practices
    a. Restriction of access to the professional e-mail account in the same way access to medical records is restricted.
    b. Use of password protected programs and screen-savers for all workstations.
    c. Firewalls
    d. Use of the auto-reply feature to notify patients when an e-mail account will not be monitored during a vacation or office closure.
    e. Protection of information considered confidential or sensitive by utilizing encryption or some other system of access controls that ensure the information is not accessed by anyone other than the intended recipient.
    f. Prohibition on use of unsecured wireless e-mail communication when sending patient-identifiable information.

Compliance

Employees and users of Refuge House's electronic mail system(s) who are found to be in violation of any part of this policy are subject to disciplinary action up to and including dismissal.

Policy for Enforcement, Sanctions, and Penalties For Violations of Individual Privacy

Purpose

The purpose of this policy is to provide information for management and workforce specifying enforcement, sanction, penalty, and disciplinary actions that may result from violation of policies regarding the privacy and protection of an individual's protected health information (PHI) and to offer guidelines on how to conform to the required standards.

Policy

General

All staff and workforce members must guard against improper uses or disclosures of Refuge House's patient information.

Refuge House staff and workforce members who are uncertain if a disclosure is permitted are advised to consult with the Refuge House IS Manager and/or Quality Personnel. The Refuge House IS Manager and/or Quality Personnel is the responsible resource for any Refuge House employee who cannot resolve a disclosure question, and may be consulted in accordance with all privacy policies of Refuge House

All staff and workforce members are required to be aware of their responsibilities under Refuge House privacy policies.

Refuge House staff and workforce members will be expected to sign an *"Employee Statement of Understanding of Privacy Policies",* indicating that they have been informed of Refuge House's business and privacy practices as they relate to Privacy, and that they understand their responsibilities to ensure the privacy of protected health information of Refuge House patients. Management and supervisors are responsible for assuring that employees who have access to confidential information, whether it be electronic, hard copy, or orally, are informed of their responsibilities.

Refuge House staff and workforce members who violate Refuge House policies and procedures regarding the safeguarding of an individual's information are subject to disciplinary action by Refuge House up to and including immediate dismissal, and legal action by the individual.

Refuge House staff and workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.

Retaliation Prohibited

Neither Refuge House as an entity nor any Refuge House employee will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

A. Any individual for exercising any right established under Refuge House policy, or for participating in any process established under Refuge House policy, including the filing of a complaint with Refuge House or with DHHS.
B. Any individual or other person for:
    1. Filing of a complaint with Refuge House or with DHHS as provided in Refuge House privacy policies;
    2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to Refuge House policy and procedures; or
    3. Opposing any unlawful act or practice, provided that:
        A. The individual or other person (including a Refuge House staff and workforce member) has a good faith belief that the act or practice being opposed is unlawful; and
        B. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected health information in violation of Refuge House policy.

Disclosures by Whistleblowers and Workforce Crime Victims

A Refuge House staff, workforce member, or contractor may disclose an individual's protected client information if:

A. The Refuge House staff, workforce member, or contractor believes, in good faith, that Refuge House has engaged in conduct that is unlawful or that otherwise violates professional standards or Refuge House policy, or that the care, services, or conditions provided by Refuge House could endanger Refuge House staff, workforce members, patients, or the public; **and**
B. The disclosure is to:
    1. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Refuge House;
    2. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by Refuge House; or
    3. An attorney retained by or on behalf of the Refuge House staff, workforce member, or contractor for the purpose of determining the legal options of the Refuge House staff, workforce member, or contractor with regard to this policy.

Refuge House's staff and workforce members may disclose limited protected information about an individual to a law enforcement official if the staff or workforce member is the victim of a criminal act and the disclosure is:

A. About only the suspected perpetrator of the criminal act; and
B. Limited to the following information about the suspected perpetrator:
    1. Name and address;
    2. Date and place of birth;
    3. Social security number;
    4. ABO blood type and rh factor;
    5. Type of any injury;
    6. Date and time of any treatment; and
    7. Date and time of death, if applicable.

Enforcement

Refuge House staff and workforce members who violate Refuge House policies and procedures regarding the safeguarding of an individual's information are subject to:

A. Appropriate disciplinary action by Refuge House, up to and including immediate dismissal from employment.
B. Legal action by the individual who may also want to pursue a tort claim against Refuge House

Refuge House staff and workforce members who knowing and willfully violate state or federal law for improper invasions of personal privacy may be subject to:

A. Criminal investigation and prosecution, both by the state and by the federal government, depending on the nature of the violation. Federal and state law provides substantial fines and prison sentences upon conviction, depending on the nature and severity of the violation.
B. Civil monetary penalties that the federal Department of Health and Human Services (DHHS) may impose.
C.

Refuge House's office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

References

45 CFR 164.530

Policy for Fax Transmittal of Protected Health Information (PHI)

Purpose

The purpose of this policy is to define appropriate standards for transmitting protected health information by fax.

Definitions

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

Treatment, Payment, and Health Care Operations (TPO): Three core functions of providing health care to patients. ***Treatment*** involves the administering, coordinating and management of health care services by Refuge House for its patients. ***Payment*** includes any activities undertaken either by Refuge House or a third party to obtain premiums, determine or fulfill its responsibility for coverage and the provision of benefits or to obtain or provide reimbursement for the provision of health care. ***Health care Operations*** are activities related to Refuge House's functions as a health care provider, including general administrative and business functions necessary for Refuge House to remain a viable health care provider.

Policy

It is the policy of Refuge House to protect the facsimile transmittal of PHI and hold individuals responsible for following the proper procedure when PHI is sent via facsimile. Refuge House protects the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. This policy defines the minimum guidelines and procedures that must be followed when transmitting patient information via facsimile.

Procedure

All workforce members of Refuge House must strictly observe the following standards relating to facsimile communications of patient medical records:

PHI will be sent by facsimile only when the original record or mail-delivered copies will not meet the needs for TPO. For example, personnel may transmit PHI by facsimile when urgently needed for patient care or required by a third-party payer for ongoing certification of payment for a patient.

Information transmitted must be limited to the minimum necessary to meet the requester's needs.

Except as authorized by the individual's consent to TPO or federal or state law, a properly completed and signed authorization must be obtained before releasing PHI. The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied without specific written patient authorization, unless required by law.

- Confidential details of psychotherapy (records of treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist).
- Other professional services of a licensed psychologist.
- Social work counseling/therapy.
- Domestic violence victims' counseling.
- Sexual assault counseling.
- HIV test results. (Patient authorization required for EACH release request.)
- Records pertaining to sexually-transmitted diseases.
- Alcohol and drug abuse records protected by federal confidentiality rules (42 CFR Part 2)

A "Facsimile Cover Letter" must be used to send faxes containing PHI. All pages plus the cover page of all confidential documents to be faxed must be marked "Confidential" before they are transmitted.

Personnel must make reasonable efforts to ensure that they send the facsimile transmission to the correct destination including:

- Preprogramming frequently used numbers into the machine to prevent misdialing errors.
- Periodically and/or randomly checking all speed-dial numbers to ensure their currency, validity, accuracy, and authorization to receive confidential information.
- For a new recipient, the sender must verify the fax number by requesting the recipient submit a faxed or email request for PHI, which would include the fax number of the recipient.
- Periodically reminding those who are frequent recipients of PHI to notify Refuge House's if their fax number is to change.

Procedure for Faxes Sent Successfully:

A copy of the fax transmittal and fax confirmation sheet must be maintained for future reference.

Procedure for Misdirected Faxes (for both TPO and non-TPO purposes):

If a fax transmission containing PHI is not received by the intended recipient because of a misdial, check the fax machine to obtain the misdialed number. If possible, a phone call (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed. If the recipient cannot be reached by phone, a fax using the "Letter for Misdirected Fax" should be sent to the recipient requesting that the entire content of the misdirected fax be destroyed.

A log of misdirected faxes will be maintained by the office manager.

Receipt of Faxes Containing PHI:

Fax machines used for patient care or patient related services shall not be located in areas accessible to the general public but rather must be in secure areas, and the office manager is responsible for limiting access to them.

When receiving faxed PHI:

Immediately remove the fax transmission from the fax machine and deliver it to the recipient.

Manage PHI received via fax as confidential in accordance with policy.

Destroy, or follow sender's instructions for patient information faxed in error and immediately inform the sender.

Enforcement

All supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject will be subject to the disciplinary process for faculty, staff, students, or volunteers.

Policy for Completing and Maintaining Forms and Documents Requiring a Signature

Purpose

The purpose of this policy is to provide information for management and workforce members regarding instructions and procedures for forms and documents requiring signatures from patients.

Policy

General

Be sure the patient or individual understands the form or document before signing it.

Encourage the individual to ask questions about the form or document and what it allows.

If the client cannot read or write, the client may sign by making a mark. They can also ask someone to sign on their behalf.

If an agency has custody of children and its representative signs the form or document, a copy of the custody order must be attached.

A personal representative is allowed to explain and review forms and documents.

Personal Representative

If the signer is a guardian or legal custodian of an adult, emancipated minor or deceased patient and is authorized by state law to act on behalf of the individual for making decisions about them, a copy of the legal authority (guardianship or custody order) must be attached to all forms and documents.

Minors

Minors can consent to medical treatment at age 17; and to mental, emotional or chemical dependency treatment at age 17.

They may sign their own authorization forms and documents related to such treatment.

If the individual is a minor, and a parent is authorized by state law to act on behalf of the minor for making decisions about them, the parent may sign the forms and documents.

If a person or agency has guardianship or legal custody of the minor and is authorized by state law to act on behalf of the minor for making decisions about health care, a copy of the legal authority (guardianship or custody order) must be attached to all forms and documents.

Photocopying

Keep the original form or document in the patient file and send copies to other health care providers, agencies and entities as necessary or required.

Canceling Permission

If the patient later revokes or cancels any forms or documents, the person accepting the revocation or cancellation must write “REVOKED” or "CANCELLED" boldly across the form or document, and must date and sign their full signature on the bottom of the first page of the form or document. The patient must also sign and date the form or document, and a copy must be maintained in the patient's file.

General Policy Regarding Contractors

Purpose

The purpose of this policy is to provide procedures and protocols that must be followed by management and workforce members regarding contractors.

Policy

In general:

A contractor is a person or entity who provides certain functions, activities, or services for or to Refuge House, involving the use and/or disclosure of PHI.

A contractor is not a Refuge House employee.

Refuge House is not liable for privacy violations of its contractors and is not required to actively monitor or oversee the means by which its contractors carry out safeguards, or the extent to which the contractors abide by the requirements of the contract. However, Refuge House is required to act if it becomes aware of a practice or pattern that constitutes a material breach of this policy.

Procedures

All personnel must strictly observe the following standards relating to contractors:

Refuge House must enter into contracts with contractors that contain specific language.

The contract must include language that provides that the contractor will:

Not use or further disclose the information other than as permitted or required by the contract or as required by law;

Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

Report to Refuge House any use or disclosure of the information not provided for by its contract of which it becomes aware;

Ensure that any agents, including any subcontractors, to whom it provides PHI received from, or created by, or on behalf of Refuge House, agree to the same restrictions and conditions that apply to the contractor with respect to such information;

Make available PHI in accordance with the Refuge House policy on Patient Access to PHI;

Make available PHI for amendment and incorporate any amendments to PHI in accordance with the Refuge House policy on Patient's Right to Amend or Correct PHI;

Make available the information required to provide an accounting of disclosures in accordance with the Refuge House policy on Accounting of PHI Disclosures;

Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created by or on behalf of Refuge House, available to DHHS for purposes of determining Refuge House's compliance; and

At termination of the contract, if feasible, return or destroy all PHI received from, or created by or on behalf of, Refuge House that the contractor still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

In the event Refuge House becomes aware of a pattern or practice of the contractor that constitutes a material breach or violation of the contractor's obligations under its contract, Refuge House must take reasonable steps to cure the breach or to end the violation, as applicable.

In the event that the contractor cannot or will not remedy the practice or pattern, Refuge House must terminate the contract if feasible. Where termination is not feasible, contact the Refuge House Privacy Official for reporting to DHHS, as required.

Enforcement

All supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the disciplinary process for faculty, staff, students, or volunteers.

References

45 C.F.R. §164.502(e) (1)

45 C.F.R. §160.103

General Policy on Uses and Disclosures of PHI

Purpose

The purpose of this policy is to provide procedures and protocols that must be followed by management and workforce members regarding uses and disclosures of protected health information (PHI).

Definitions

Use with Respect to Individually Identifiable Health Information:

The sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Treatment: The provision, coordination, or management of health care related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or for the referral of a patient for health care from one health care provider to another.

Payment: Any activities undertaken either by a health plan or by a health care provider to obtain premiums determine or fulfill its responsibility for coverage and the provision of benefits or to obtain or provide reimbursement for the provision of health care. These activities include but are not limited to:

1. Determining eligibility, and adjudication or subrogation of health benefit claims,

2. Risk adjusting amounts due based on enrollee health status and demographic characteristics,

3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care processing,

4. Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges,

5. Utilization review activities, including pre-certification and preauthorization services, concurrent and retrospective review of services,

6. Disclosure to consumer reporting agencies of certain PHI relating to collection of premiums or reimbursement.

Health Care Operations: Any one of the following activities to the extent the activities are related to providing health care:

1. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting patients with information about treatment alternatives, and related functions that do not involve treatment,
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which volunteers, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities,
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care,
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs,
5. Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the practice, including formulary development and administration, development or improvement of methods of payment or covered policies, and
6. Business management and general administrative activities:
    a. Management activities related to HIPAA compliance,
    b. Customer Service,
    c. Resolution of internal grievances,
    d. Due Diligence,
    e. Activities designed to de-identify health information, and
    f. Fundraising activities for the benefit of the practice.

Minimum Necessary: When using or disclosing PHI or when requesting PHI from another health care provider or health organization, Refuge House must limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Minimum Necessary does not apply in the following circumstances:

1. Disclosures by a health care provider for treatment (volunteers, staff and trainees are included as health care providers for this purpose),
2. Uses and Disclosures based upon a valid consent to use and disclose PHI for treatment, payment and health care operations or a valid authorization to use and disclose PHI,
3. Disclosures made to the Secretary of the Department of Health and Human Services,
4. Uses and disclosures required by law, and
5. Uses and disclosures required by other sections of the HIPAA privacy regulations.

Indirect Treatment Relationship: A relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and
2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services, products or reports to the individual.

Defective Consents: Lacking an element required in the consent or becoming defective if the consent has been revoked.

Policy

Refuge House and employees may use and disclose PHI for Treatment, Payment and Health Care Operations (TPO) only if the patient has signed and executed a Consent for the Use and Disclosure of PHI form that grants Refuge House and employees the right to use and disclose PHI to carry out TPO. (See addendum for example of HIPAA Consent form) However, this consent only allows Refuge House and its employees to use and disclose the "Minimum Necessary" amount of information required to complete the desired task.

Unless there is an emergency, Refuge House should not treat a patient if the patient has not signed and executed the proper HIPAA consent form. Refuge House and employees may use and disclose PHI for TPO without obtaining the consent of the patient only in the following instances:

- When an indirect treatment relationship exists,
- When an emergency situation exists,
- When treatment is required by law, or
- When substantial barriers in communication exist and the patient's consent is clearly inferred from the circumstances. If failure to obtain consent occurs, the reasons for the failure to obtain consent must be documented on the consent form.

It should be clearly understood the Consent for the Use and Disclosure of PHI does not allow Refuge House or its employees to use or disclose PHI for any reasons other than for TPO. For Refuge House to use and disclose PHI for purposes other than for treatment, payment and health care operations, see *Policy for Uses and Disclosures of PHI Based on Patient Authorizations* and *Policy Uses and Disclosures of Public Health and Safety.*

We are not required to obtain HIPAA Consents for prisoners. However, prisoner PHI is protected from wrongful use or disclosure if the use or disclosure is for any reason other than TPO. For continuity and normal operations, Refuge House may require HIPAA consents for prisoners.

Psychotherapy notes are not to be included as PHI that may be disclosed, unless consent is sought for such use or disclosure.

Consents to use and disclose PHI for TPO must have the following elements for the consent to be effective:

1. Inform the patient or representative that PHI may be used and disclosed to carry out TPO;
2. Refer the patient or representative to the *Security and Confidentiality Notice* for a more complete description of such uses and disclosures and state that the patient or representative has the right to review the *Security and Confidentiality Notice* prior to signing the consent;
3. State the patient or representative may request a restriction be placed on the consent. Refer to the *Requests for Restricting Uses and Disclosures and Confidential Communications Policy* and
4. The consent must be signed by the patient or representative and dated. Refuge House reserves the right to change its privacy practices described in the *Security and Confidentiality Notice.* If Refuge House changes the terms of its *Security and Confidentiality Notice*, Refuge House will describe how the patient or representative may obtain a revised *Security and Confidentiality Notice*.

Enforcement

Refuge House's office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

INFORMATION SYSTEMS ACCESS POLICY

Purpose

The purpose of this policy is to maintain an adequate level of security to protect Refuge House's data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of Refuge House's information systems.

Policy

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

Who is Affected

This policy affects all workforce members of Refuge House, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

Affected Systems

This policy applies to all computer and communication systems owned or operated by Refuge House Similarly, this policy applies to all platforms (operating systems) and all application systems.

Entity Authentication

Any user (remote or internal), accessing Refuge House's networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- A unique user identifier
- At least one of the following:
    - Biometric identification
    - Password
    - Personal identification number
    - A telephone callback procedure
    - Token

Workstation Access Control System

All workstations used for this Refuge House's business activity, no matter where they are located, must use an access control system approved by Refuge House In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOs. Active workstations are not to be left unattended for

prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks.

Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 1 minute). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

System Access Controls

Access controls will be applied to all computer-resident information based on its' Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

Access Approval

System access will not be granted to any user without appropriate approval. Management is to immediately notify the Security Official and report all significant changes in end-user duties or employment status. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred or assigned to a different job.

Limiting User Access

Refuge House's approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.

Need-to-Know

Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required performing their jobs.

Compliance Statement

Users with access to Refuge House's information systems must sign a compliance statement prior to issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by Refuge House's policies and procedures related to computers and information systems. Semi-annual confirmations will be required of all system users.

Audit Trails and Login

Logging and auditing trails are based on the data classification of the systems.

Confidential System

Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account

- Method of access
- All privileged commands must be traceable to specific user accounts

In addition logs of all inbound access into Refuge House's internal network by systems outside of its defined network perimeter must be maintained.

Audit trails for confidential systems should be backed up and stored in accordance with Refuge House's back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports.

Access for Non-Employees

Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the Refuge House's computers or information systems unless the written approval from Refuge House has first been obtained. Before any third party or business partner is given access to this Refuge House's computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.

Unauthorized Access

Employees are prohibited from gaining unauthorized access to any information systems or databases that do not require their access, or in any way damaging, altering, or disrupting the operations of any system(s). System privileges allowing the modification of "production data" must be restricted to "production" applications.

Remote Access

Remote access must conform at least minimally to all HIPAA and state statutory requirements.

Policy for Minimum Necessary Use and Disclosure of Protected Health Information (PHI)

Purpose

The purpose of this policy is to provide information for management and workforce members to conform to the requirements regarding the use and disclosure of the minimum amount of information necessary to provide services and benefits to patients, and to ensure that management and workforce members have access to the information they require to accomplish their health care goals and objectives.

Policy

General

Refuge House will use or disclose only the minimum amount of information necessary to provide services and benefits to patients, and only to the extent provided in Refuge House policies and procedures.

This policy does not apply to:

A. Disclosures to or requests by a health care provider for treatment;
B. Disclosures made to the individual about his or her own protected information;
C. Uses or disclosures authorized by the individual that are within the scope of the authorization;
D. Disclosures made to the United States Department of Health and Human Services (DHHS), Office of Civil Rights, in accordance with subpart C of part 160 of the HIPAA Privacy Rule;
E. Uses or disclosures that are required by law; and
F. Uses or disclosures that are required for compliance with the HIPAA Transaction Rule. The minimum necessary standard does not apply to the required or situational data elements specified in the implementation guides under the Transaction Rule.

Minimum Necessary Information

When Refuge House policy permits use or disclosure of an individual's information to another entity, or when Refuge House requests an individual's information from another entity, Refuge House staff and workforce members must make reasonable efforts to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

If Refuge House policy permits making a particular disclosure to another entity, Refuge House staff and workforce may rely on a requested disclosure as being the minimum necessary for the stated purpose when:

A. Making disclosures to public officials that are permitted under 45 CFR 164.512 if the public official represents the information requested is the minimum necessary for the stated purpose(s).
B. A "public official" is any employee or workforce member of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.
C. The information is requested by another entity that is a "covered entity" under the HIPAA Privacy rules. A "covered entity" is a health plan, a health care provider who conducts electronic transactions, or a health care clearinghouse;
D. The information is requested by a professional who is a member of the workforce of a "covered entity" or is a contractor of the "covered entity" for the purpose of providing professional services to the "covered entity," if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
E. Documentation or representations that comply with the applicable requirements of uses and disclosures for research purposes have been provided by a person requesting the information for research purposes.

Access & Uses of Information

Refuge House will establish role-based categories that identify types of information necessary for staff and workforce members to perform their jobs. Refuge House will identify the category of information needed for persons, or classes of persons, in their respective workforces to carry out their duties, and will further identify any conditions appropriate to such access. Categories will include all information, such as information accessible by computer, kept in files, or other forms of information consistent with administrative, technical and physical safeguards.

Routine and Recurring Disclosure of an Individual's Information

For the purposes of this policy, "routine and recurring" means the disclosure of records outside Refuge House, without the authorization of the individual, for a purpose that is compatible with the purpose for which the information was collected. The following identifies several examples of uses and disclosures that Refuge House has determined to be compatible with the purposes for which information is collected:

- Refuge House will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed.
- Routine and recurring uses include disclosures required by law. For example, a mandatory child abuse report by a Refuge House employee would be a routine use.
- If Refuge House deems it desirable or necessary, Refuge House may disclose information as a routine and recurring use to the State Department of Justice for the purpose of obtaining its advice and legal services.
- When federal or state agencies - such as the DHHS Office of Civil Rights, the DHHS Office of Inspector General, Refuge House's State Medicaid Fraud Unit, or the Refuge House's Secretary of State - have the legal authority to require Refuge House to produce records necessary to carry out audit or oversight of Refuge House activities, Refuge House will make such records available as a routine and recurring use.

- When Refuge House determines that records are subject to disclosure under the Refuge House's State laws, Refuge House may make the disclosure as a routine and recurring use.

Non-Routine Disclosure of an Individual's Information

For the purpose of this policy, "non-routine disclosure" means the disclosure of records outside Refuge House that is not for a purpose for which it was collected.

Refuge House will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor.

Requests for non-routine disclosures must be reviewed on an individual basis in accordance with the criteria set forth in this policy.

For Non-Routine Disclosures, Refuge House will:

A. Implement procedures to limit the information disclosed to only the minimum amount of information necessary to accomplish the purpose for which the disclosure is sought; and
B. Review requests for non-routine disclosures on an individual basis in accordance with such procedures.

Refuge House's **Request for an Individual's Information from another Health Care Provider or Entity**

When requesting information about an individual from another health care provider or entity, Refuge House staff and workforce members must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made.

Refuge House will not request an individual's entire medical record unless Refuge House can specifically justify why the entire medical record is needed.

Disclosures of an Individual's Information on a Routine or Recurring Basis:

For Routine and Recurring Disclosures, Refuge House will:

A. Determine who is requesting the information and the purpose for the request. If the request is **not** compatible with the purpose for which it was collected, refer to and apply the "Non-Routine Use" policies.
B. Confirm that the applicable Refuge House policies permit the requested use and/or disclosure.
C. Identify the kind and amount of information that is necessary to respond to the request; and
D. If the disclosure is one that must be included in the Refuge House accounting of disclosures, include required documentation in an accounting log.

Disclosures of an Individual's Information on a Non-Routine Basis

For Non-Routine Disclosures, Refuge House will:

A. Determine who is requesting the information and the purpose for the request. If the request **is** compatible with the purpose for which it was collected, apply the "Routine and Recurring Use" policies from the above previous section.
B. Determine which information of the individual is within the scope of the request, and what Refuge House policies apply to the requested use;
C. If the information requested can be disclosed under the applicable policies, limit the amount of information to the minimum amount necessary to respond to the request; and;
D. Document the disclosure in an accounting log.

References

45 CFR Parts 160 and 164

Non-Retaliation Policy

Purpose

The purpose of this policy is to provide procedures for management and workforce members regarding non-retaliation in cases involving the reporting of violations or infractions of HIPAA or other federal or state laws or regulatory requirements.

Policy

All Refuge House workforce members and employees shall be allowed to freely discuss and raise questions to Refuge House's office manager or to the appropriate personnel about situations they feel are in violation of HIPAA and other federal and state laws, Refuge House's policies, and/or accreditation and regulatory requirements.

All Refuge House workforce members and employees have a personal obligation to report any activity that appears to violate HIPAA or other applicable laws, regulations, rules, policies, and procedures.

Refuge House shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against the following individuals or in the following situations:

> Any patient, legally authorized representative, employee, workforce member, volunteer, associate, association, contractor, organization or group that in good faith:
>
> (1) Discloses or threatens to disclose information about a situation they feel is inappropriate, or potentially illegal;
> (2) Provides information to or testifies against the alleged offending individual or Refuge House;
> (3) Objects to or refuses to participate in an activity they feel are in violation of HIPAA or any other federal and state law, Refuge House's policies, or accreditation requirements;
> (4) Is involved in any compliance review or peer review process; or
> (5) Files a valid or legitimate report or a complaint, or an incident report.

Investigation of Retaliation

Refuge House will review any allegation of retaliation and will ensure that a proper investigation is conducted as appropriate. The investigation will be in accordance with the Refuge House's *Complaints and Grievances.*

Enforcement

Refuge House's office manager and all supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to appropriate and applicable disciplinary action, up to and including termination or dismissal.

References

45 C.F.R. §164.530(g)

PASSWORD POLICY

Purpose

The purpose of this policy is to ensure that only authorized users gain access to Refuge House's information systems.

Policy

To gain access to Refuge House's information systems, authorized users, as a means of authentication must supply individual user passwords. These passwords must conform to certain rules contained in this document.

Who is Affected

This policy affects all employees of Refuge House, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

Affected Systems

This policy applies to all computer and communication systems owned or operated by Refuge House Similarly, this policy applies to all platforms (operating systems) and all application systems.

User Authentication

All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an individual user will be deleted or disabled.

Password Storage

Passwords will not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

Application Passwords Required

All programs, including third party purchased software and applications developed internally for Refuge House must be password protected.

Choosing Passwords

All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character. The use of control characters and other non-printing characters are prohibited. All users must be automatically forced to change their passwords appropriate to the classification level of information. To obtain a new password, a user must present suitable identification.

Changing Passwords

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. All users must be forced to change their passwords at least once every sixty (60) days.

Password Constraints

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or (c) if dial-up or other external network connections are involved, disconnected.

Policy for Copying and Printing Protected Health Information (PHI)

Purpose

The purpose of this policy is to provide information for management and workforce members regarding copying and printing protected health information.

Policy

All Refuge House's personnel must strictly observe the following standards relating to the printing and copying of PHI.

- PHI in hardcopy format must be disposed of in accordance with the *Confidentiality and Security of Information Policy*.
- Printed versions of PHI should not be copied indiscriminately or left unattended and open to compromise.
- Printers and copiers used for printing of PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
- PHI printed to a shared printer should be promptly removed.
- Media and hardcopy containing PHI must have access controls during transportation and disposal, see *Disposal of PHI Policy.*

Enforcement

Refuge House's office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Privacy Complaints

Purpose

The purpose of this policy is to provide information for management and workforce members for handling privacy complaints.

Policy

Any individual who believes his or her rights granted by the Health Insurance Portability and Accountability Act (HIPAA) Privacy regulations or any other state or federal laws dealing with privacy and confidentiality of health information have been violated may file a complaint regarding the alleged privacy violation.

Filing HIPAA Complaints

Any privacy related complaint made by a patient, employee or volunteer at anytime must be forwarded to the IS Manager and/or Quality Personnel. Complaints may also be made anonymously by calling Quality Development.

Investigation of Complaints

Refuge House will investigate alleged privacy violations and complaints made by patients regarding alleged breaches of their privacy. Employees and workforce members may be requested to assist in investigations regarding complaints made by patients and other employees who believe fellow employees have violated patient privacy standards.

Simultaneously, Refuge House will undertake an investigation to determine if a breach of privacy has occurred. Any employee or workforce member found to be in violation of this policy or breaches the confidentiality of a patient's protected health information will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Uses and Disclosures of Psychotherapy Notes

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's psychotherapy notes.

Definitions

Disclosure: The release, transfer, provision of access to, or divulgence in any other manner, of patient protected health information to any individual or organization outside of Refuge House

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within Refuge House

Psychotherapy Notes: Notes (i.e. process notes) that capture the therapist's impressions about the patient containing details of the conversation considered to be inappropriate for the medical record, and are used by the provider for future sessions. Psychotherapy notes can also be recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Psychotherapy notes are kept separate from the rest of the individual's medical record.

Policy

Patient Access

A patient does not have a right to inspect or obtain a copy of psychotherapy notes. A patient may not request a review of an originator's denial of access to psychotherapy notes. However, a patient may be provided access to a summary of the psychiatric treatment.

Refuge House may not release psychotherapy notes, except in specific situations or as required by law.

Psychotherapy notes (i.e., process notes) shall be maintained separately from the medical record.

Summary information (i.e., progress notes) such as current state of the patient, symptoms, summary of the theme of the psychotherapy session, diagnoses medications prescribed, side effects, and other information needed for treatment or payment shall be placed in the medical record.

Authorization for the disclosure of psychotherapy notes is not required in the following circumstances:

a. For use by the originator for treatment;
b. For use in educational programs involving practicing counseling;
c. To defend a legal action brought by the patient;

d. For purposes of the Department of Health and Human Services in determining compliance with the privacy rule;
e. As otherwise required by law;
f. By a health oversight agency for a lawful purpose related to oversight of a psychotherapist;
g. 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; or,
h. To law enforcement in instances of permissible disclosure related to a serious or imminent threat to the health or safety of a person or the public.
i.

Enforcement

Name of Health Care Provider]'s office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

References

45 C.F.R.§164.508(a) (2)

45 C.F.R. §164.524

Policy for Ensuring the Security of Electronic Data

Purpose

The purpose of this policy is to provide information for management and workforce members in prescribing practices which secure electronic patient protected health information.

Definitions

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

Individually Identifiable Health Information: Any information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse; and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual.

Computer Systems: Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email.

Network: Electronic network allowing access to the Refuge House's personal computers, facility-based systems, and centrally-based systems (e.g. AS/400, Windows 2000 Server, Mainframe, etc.) and electronic data.

Local Area Network: Electronic network access allowing access to an individual facility's electronic data and computers.

Network Attached Computer: Any computer with access to a local area network and/or the Refuge House's network.

Workforce: Includes employees, volunteers, contract workers, trainees and other persons who are in Refuge House's facility on a regular course of business. This shall include client workers employed by Refuge House or any of its facilities.

Patient: Any individual who has received or is receiving services from Refuge House

Restricted Access: Computer systems with access limited to specific systems, activities, or files.

IS Manager (ISM): Individual designated by Refuge House to oversee all activities related to the development, implementation, maintenance of, and adherence to Refuge House policies and procedures covering the electronic and physical security of, and access to, protected health

information and other Refuge House data in compliance with HIPAA and other federal and state laws and regulations.

Media: Backup tapes, hard drives, floppy diskettes, CDs, zip drives cartridges, optical, and paper hard copies.

Policy

General

Users shall be automatically logged off their VDI after a maximum period of 3 minutes of inactivity.

Access to Refuge House networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of designated Refuge House IT staff.

Designated Refuge House IT staff shall back up data nightly to backup tapes and backup Refuge House databases in their entirety nightly. Patient information and other data shall be backed up incrementally nightly and fully once a week.

Designated Refuge House IT shall ensure that all media has been thoroughly cleansed of any patient data before the media is surplussed or disposed of.

Access to media containing patient data shall be controlled, by designated IT staff through:

1. Access control lists to network media
2. Physical access control to Refuge House's hardware
3. Purging Refuge House's data on any type of media before it is surplussed or discarded
4. Storage of data on media that is backed up

Virus protection for the Refuge House's network or computer systems shall be maintained by designated IT staff, pursuant to the following virus protection procedures:

1. All Refuge House's email servers, including the central office bridgehead server if appropriate, shall be protected using email-specific anti-virus software.
2. All network and member servers shall be protected using anti-virus software.
3. All workstations, laptops, PDAs or any other device that connects to the Refuge House's network shall be protected using anti-virus software for that device and installed by designated IT staff.

Equipment that has not been purchased or authorized by Refuge House shall not be allowed to connect to the Refuge House's network.

Virus Signature Updates

Anti-virus server software shall be configured by designated IT staff to check for virus signature updates daily.

Anti-virus PC, laptops, PDAs software will check for virus signature updates hourly from the master console of the anti-virus program, as a result of IT staff actions.

Special virus signature updates created in the event of a known virus, will be manually pushed by designated IT staff to all servers, PCs, laptops, and PDAs within 24 hours of the time the receipt of the update has been received at the master console.

Software Updates

Anti-virus software shall be kept by designated IT staff at the current release or no more than one release below the most current release version.

Software Support

Refuge House IT staff shall maintain a support contract with the anti-virus software vendor(s) to ensure uninterrupted support.

Attachments

Refuge House's workforce shall not load software, from any source, onto their assigned workstation or any other Refuge House's equipment. This software includes but is not limited to software from the internet, a CD, or a floppy diskette. Software shall be loaded on workstations only by designated employees of Refuge House's IT staff.

Refuge House workstations shall be situated by respective designated IT staff to prevent more than incidental observation of work product.

Enforcement

Refuge House office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

Certification of Compliance

1820 Providing Certification of Compliance to DFPS

If DFPS requests it, the Agency will promptly give DFPS written certifications of compliance with controls and provisions relating to information security. This includes, but is not limited to, those related to confidential data transfers and the handling and disposal of personally identifiable information (PII). Written compliance may be, but are not limited to:

- Statement on Auditing Standards No.70, Service Organizations (SAS- 70) Report;
- General Security Controls Audit;

- Application Controls Audit;
- Vulnerability Assessment; and
- Network/Systems Penetration Test.

Policy for Security Audit Control

Purpose

The purpose of this policy is to provide information for management and workforce members for ensuring that the activity of all information systems containing individually identifiable protected health information is recorded in a manner commensurate with its risk.

Policy

All Refuge House computers, computer systems and networks and all other electronic devices containing medium and high risk individually identifiable protected health information in electronic form (EPHI) must utilize a mechanism to log and store system and user activity.

- Each system's audit log must include, but is not limited to, user ID, login date & time, and activity time.
- Audit logs may include, but are not limited to, system and application login reports, activity reports, exception reports or any other mechanism to document and manage system and application activity.
- System audit logs must be reviewed on a regular basis.

The implementation of an audit control mechanism for systems containing low risk EPHI is not required.

An Audit Control and Review containing the following elements will be created and maintained by the Security Officer:

- Systems and Applications to be logged;
- Information to be logged for each system;
- Log-in Reports for each system;
- Procedures to review all audit logs and activity reports

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Automatic Logoff

Purpose

The purpose of this policy is to provide information for management and workforce members to ensure that access to all servers and workstations that access, transmit, receive, or store EPHI is appropriately controlled.

Definitions

EPHI - Protected Health Information – Individually identifiable health information that is transmitted or maintained by electronic media.

Individually Identifiable Health Information – Health information which includes demographic information that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual and that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Policy

The following procedures must be followed:

- Refuge House's servers, workstations, or other computer systems containing EPHI must employ inactivity timers or automatic logoff mechanisms. The mechanisms must terminate a user session after a maximum of 3 minutes of inactivity
- Refuge House's servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms. (I.E. Password protected screen saver that blacks out screen activity.) The mechanisms must terminate a user session after a maximum of, but not limited to, 3 minutes of inactivity.
- Applications and databases using EPHI, such Electronic Medical Records, must employ inactivity timers or automatic session logoff mechanisms. Application sessions must automatically terminate after a maximum of, but not limited to, 3 minutes of inactivity.
    - Refuge House's servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
    - If a system requires the use of an inactivity timer or automatic logoff mechanism as detailed in the above procedures, but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
    - The system must be upgraded or moved to support the minimum Automatic Logoff procedures.
    - The system must be moved into a secure environment.
    - All EPHI must be removed and relocated to a system that supports the minimum Automatic Logoff procedures.
- When leaving a server, workstation, or other computer system unattended, Refuge House's workforce members must lock or activate the systems Automatic Logoff Mechanism (e.g.

CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing EPHI.

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Data Backup and Retention

Purpose

The purpose of this policy is to provide information for management and workforce members for performing periodic computer system backups to ensure that critical data is adequately preserved and protected against loss and destruction.

Policy

General

The backup and recovery process for Refuge House's computers, networks and systems must be documented and reviewed annually and tested on a regular basis.

The backup should, at a minimum, include:

1. Physical Access Controls
    a. The minimum acceptable level of physical security for any backup system or server(s) is to place it behind a locked door, with a paper-based sign-in/sign-out sheet.
    b. Physical access to backup equipment must be approved by the Security officer.
2. Backup schedule
    a. At a minimum, modified data on computers must be incrementally backed up at the end of each work day and a full system backup must be performed at least once per month. Critical data should be backed up, regardless of where it resides. On a monthly basis at least one full backup must be stored off-site.
    b. A process must be implemented to verify the success of the electronic information backup.
    c. Backup schedule logs:
        1. The backup software should capture a list of all files and directories encountered and saved. Logs should contain information about successful backups, unsuccessful backups, backup media that was left in place accidentally and overwritten, when and where the media was sent offsite, the success or failure of restore tests and bad media encountered which may affect your ability to obtain files from a previous backup.
        2. Assign a primary and backup workforce member to rotate the media and note any problems or exceptions. Write an entry for successful backups, the date and which media was utilized. Keep the written log with the computer that performs the backup.
    d. Legible, unique labels shall be placed on all backup media.

3. Length of Data Retention
    a. Full system backup should be copied and or archived and not be stored in the same geographic location as the source systems on a monthly basis.
    b. Archived backups must be periodically tested to ensure that they are recoverable.
4. Off Site Storage Procedures

a. Archived backups shall be stored off site. Refuge House will contract with a vendor (who will be a HIPAA Contractor) to provide backup storage.
b. Security access controls implemented at offsite backup and storage facilities must meet or exceed the security access controls of the source systems.

5. Documentation
    a. The backup restore and recovery processes must be documented.
    b. What is backed up, when, and how often the backups occur must be documented.
    c. A list of mission critical servers and type of data contained on each server.
    d. Procedures and processes to restore backup client.
    e. Procedures and processes to restore backup server.
    f. Reconstruction times for the existing data backup system.
    g. Contact information:
        1. List of designated staff to be contacted in an emergency. A copy of this list must be kept in a secure location, such as with off-site backups, and be readily accessible in case of an emergency
        2. Vendor contact and support information
        3. Offsite storage contacts
    h. License codes and media.
    i. Hardware and software for data backup system
6. Backups must be performed in accordance with the backup documentation for that backup system.

Unacceptable Use

The following activities are prohibited. Refuge House workforce members may be exempted from these restrictions during the course of their job responsibilities (e.g., systems administrators and computer technicians may have a need during maintenance periods to disable computer or network access.).

Under no circumstances is a workforce member of Refuge House authorized to engage in any illegal activity while utilizing Refuge House resources.

Unacceptable use activities include, but are not limited to the following:

1. The backup system is not considered to be an electronic archiving process for the storing of files for future retrieval. The backup system is to be used for the purposes of disaster recovery only.
2. Data retention systems are available for Refuge House data only. Users may not store personal or non-Refuge House information on any Refuge House data retention system.

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Accessing the Internet

Purpose

The purpose of this policy is to provide information for management and workforce members for the prudent and acceptable practices regarding the use of the internet and to educate workforce members who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

Definition

Information Resources Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. It also includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

User An individual, automated application or process that is authorized to access the resource by Refuge House, in accordance with Refuge House procedures and policies.

Internet A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

Intranet A private network for communications and sharing of information like the Internet but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a security firewall.

World Wide Web A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Microsoft Internet Explorer.

Vendor: Someone who exchanges goods or services for money.

Policy

The following policies apply when accessing the Internet or any Intranet:

- Software for browsing the Internet is provided to authorized users for business and research use only.
- All software used to access the Internet must be part of Refuge House standard software suite or approved by the Security Officer. This software must incorporate all vendor provided security patches.
- All files downloaded from the Internet must be scanned for viruses using the approved distributed software suite and current virus detection software.
- All software used to access the Internet shall be configured to use a firewall.
- All sites accessed must comply with the Refuge House Acceptable Use Policies.
- All user activity on Refuge House Information Resources assets is subject to logging and review.
- Content on all Refuge House Web sites must comply with the Refuge House Acceptable Use Policies.
- No offensive or harassing material may be made available via Refuge House Web sites.
- Non-business related purchases made over the Internet are prohibited. Business related purchases are subject to Refuge House procurement rules.
- No personal commercial advertising may be made available via Refuge House Web sites.
- Refuge House Internet access may not be used for personal gain or non-Refuge House personal solicitations.
- No Refuge House data will be made available via Refuge House Web sites without ensuring that the material is available to only authorized individuals or groups.
- All sensitive Refuge House material transmitted over external network must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Incidental Use

- Incidental personal use of Internet access is restricted to Refuge House approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Refuge House
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to, Refuge House
- Storage of personal files and documents within Refuge House's Information Resources should be nominal.
- All files and documents – including personal files and documents – are owned by Refuge House, may be subject to open records requests, and may be accessed in accordance with this policy.

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Intrusion Detection

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the detection of intruders onto the computers and computer systems and networks, and the mechanisms that determine when to activate planned responses to an intrusion incident.

Definitions

Information Resources (IR) Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Security Incident In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Information Attack An attempt to bypass the physical or information security measures and controls. The attack may alter, release, deny or destroy data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information Operations Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Security Officer (SO) Responsible for administering the information security policies.

Host A computer system that provides computer service for a number of users.

Server A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Firewall An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Policy

- Operating system, user accounting, and application software audit logging processes must be enabled on all computers, networks, hosts and server systems.
- Alarm and alert functions of all firewalls and other network perimeter access control systems must be enabled.
- Audit logging of all firewalls and other network perimeter access control systems must be enabled.
- Audit logs from the perimeter access control systems must be monitored/reviewed on a regular and routine basis by the system administrator or Security Officer.
- System integrity checks of all firewalls and other network perimeter access control systems must be performed on a regular and routine basis.
- Audit logs for computers, servers and hosts must be reviewed on regular routine basis.
- Intrusion tools will be checked on a regular and routine basis.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Security Officer. See Also “Policy for Breach Response”
- Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the Security Officer.

Enforcement

Refuge House’s Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for the Response to a Suspected or Confirmed Data Breach

Purpose

The purpose of this policy is to provide steps to respond to a confirmed security breach within one of the Information Systems containing PII related to clients or employees of the Agency or DFPS.

To fulfill requirements set forth in Section II of the DFPS Vendor Supplemental and Special Conditions Section II Article 8 and DFPS Information Security Requirements 1800.

Definitions

Digital Information Resources (IR) Any and all online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Policy

1) Agency SO will notify DFPS Contract Manager and Office of Information Security (infosec@dfps.texas.gov) verbally and in writing of any confirmed or suspected breach of its systems that may affect Sensitive Information within one calendar day after discovery of a breach or of receiving notification of a breach. Refuge House report will identify:
   a) the nature of the unauthorized access, use or disclosure;
   b) the information accessed, used or disclosed;
   c) the person(s) who accessed, used, disclosed and/or received information (if known);
   d) what Refuge House has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
   e) What corrective action Refuge House has taken or will take to prevent future unauthorized access, use or disclosure
2) Refuge House must notify the DFPS Office of Information Security within 24-hours of discovery if Refuge House experiences or suspects a breach or loss of PII or a security incident which includes SSA-provided information.

   In the event of a confirmed or suspected breach, Refuge House will keep DFPS informed regularly as determined and required by DFPS of the progress of its investigation until the reported breach and all accompanying issues are resolved.

3) Investigation, Response and Mitigation: Refuge House will fully cooperate with DFPS's investigation of any breach experienced by Refuge House. Agency's full cooperation will include but not be limited to Refuge House:
    a) immediately preserving any potential evidence relating to the breach;
    b) promptly (but in no event no later than 48 hours after breach or notification of breach event occurred) designating a contact person to whom DFPS will direct inquiries, and who will communicate Refuge House's responses to DFPS inquiries;
    c) as rapidly as circumstances permit, applying appropriate resources to remedy the breach condition, investigate, document, restore DFPS service(s) as directed by DFPS, and undertake appropriate response activities;
    d) providing status reports to DFPS on breach response activities, either on a daily basis or a frequency required by DFPS;
    e) Coordinating all media, law enforcement, or other breach notifications with DFPS in advance of such notification(s), unless expressly prohibited by law;
    f) Ensuring that knowledgeable Agency staff is available at all times, if needed, to participate in DFPS-initiated meetings and/or conference calls regarding the breach; and
    g) DFPS may direct Vendor to provide notification to individuals, regulators, or third-parties including consumer reporting agencies, if applicable, following a breach as required by 15 U.S.C. 7001 et seq. If requested to provide notification, Vendor must comply with all applicable legal and regulatory requirements for breach notification as provided to Refuge House by DFPS. Vendor will have the burden of demonstrating to DFPS's satisfaction that any required notifications Refuge House is asked to provide was timely made.
4) In the event of a breach involving Sensitive Information, DFPS may, at DFPS's sole discretion and without limitation, do any or all the following:
    a) Require that Vendor obtain cyber security, crime theft, and notification expense insurance coverage with policy limits sufficient to cover any liability arising under this Contract, naming the State of Texas through DFPS as an additional named insured and loss payee with primary and non-contributory status;
    b) Require that Vendor indemnify DFPS;
    c) Require that Vendor defend DFPS in any court or administrative proceeding
    d) Assess liquidated or actual damages, sanctions, or remedies as permitted by the Contract or law.
5) Assistance in Litigation or Administrative Proceedings. Refuge House will make itself and any employees, subcontractors, or agents assisting Refuge House in the performance of its obligations available to DFPS at no cost to DFPS to testify as witnesses, or otherwise, in the event of a breach or other unauthorized disclosure of information caused by Refuge House that results in litigation, governmental investigations, or administrative proceedings against DFPS.

Policy for the Process of Security Management

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the processes to prevent, detect, contain and correct all security violations that will ensure the confidentiality, integrity and availability of all confidential and protected health information (PHI) residing on all electronic information systems.

Definitions

Protected Health Information – Individually identifiable health information that is transmitted or maintained by electronic media or transmitted or maintained in any other form or medium.

Individually Identifiable Health Information – Health information which includes demographic information that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual and that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Policy

- Refuge House will conduct periodic security assessments that will identify potential risks and vulnerabilities in Refuge House's efforts to secure confidential and protected health information. These assessments will be documented by the Information Security Officer or designee. These assessments can be scheduled or unscheduled. These assessments will be reviewed by Refuge House to evaluate and/or modify existing security policies and procedures within the department.
- Refuge House will implement various information security policies and procedures that provide adequate security against threats or hazards to the confidentiality, integrity and availability of all electronic PHI that Refuge House creates, receives, maintains or transmits.

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Misuse of Resources

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the misuse of company resources.

Policy

Regarding Printing

- Refuge House management and workforce will refrain from deliberate wasteful practices such as printing unnecessary listings or multiple copies of files.
- Refuge House management and workforce will refrain from printing documents or files numerous times because the document was not checked thoroughly for all errors and corrections.
- Refuge House management and workforce will print only work related materials and documents.

Regarding Shared Resources

- Refuge House management and workforce will refrain from holding (without activity) shared terminals, hard drives or network or dial-up phone lines.
- Refuge House management and workforce will not prevent others from using shared resources by placing signs on devices to "reserve" them without authorization.
- Game playing, that is not part of an authorized and assigned research or Refuge House activity, is prohibited. Computing and network resources are not to be used for personal recreational purposes.

Regarding Computer Systems

- No Refuge House computers or computer systems may be used for playing games.
- Users should not knowingly run or install on any Refuge House computers or computer system or network, or give to another user, a program intended to damage or to place excessive load on a computer, computer system or network. This includes, but is not limited to programs known as computer viruses, Trojan horses, and worms.
- Users must not use Refuge House computers, computer systems or network as a means of unauthorized access to data, accounts or systems inside or outside the Refuge House systems.
- Activities authorized by the Security Officer or management officials for security or performance testing will not be considered a misuse.
- Incidental use - such as electronic communications or storing data on workstations - must not interfere with other users' access to resources and must not be excessive.
- Use of Refuge House computer resources for personal financial gain is prohibited without the prior approval of authorized management officials.
- Authorized management officials may, at their discretion, allow incidental personal use of Refuge House computer resources in much the same way as they may, at their discretion, allow workforce members to use office telephones for personal calls or to keep personal papers in their desk.

- A Converting Refuge House resource to private endeavors is prohibited without authorization from an authorized Refuge House management official.
- Violations of this policy include behavior that interferes with the fair use of Refuge House computer resources by another workforce member.
- Creating any programs that secretly collect information about Refuge House computer users is a violation of this policy. It includes unauthorized accessing, using, copying or modifying of access rights and usage records.
- Using Refuge House computer resources for improper purposes such as the playing of practical jokes is prohibited.
- Electronic systems should not use "public" access codes that permit the anonymous access to, or distribution of, arbitrary information.

Regarding Administrative Data

- Refuge House workforce members may not use non-Refuge House information for personal non-financial gain, nor obstruct its proper use.
- The use of Refuge House information for personal financial gain or for malicious purposes is prohibited.
- Users may not use any Refuge House data in any application that duplicates any Refuge House data without authorization from Refuge House management.
- Controls over Refuge House information systems shall provide the ability to trace violations of security to individuals who may be held responsible.

Regarding Workstations

- Unauthorized personal use of any software purchased by, or developed by or for, Refuge House is a violation of this policy.
- Computers in public areas that are not locked shall not contain protected health information or any other confidential or sensitive information.

Regarding Computer Networks

- The owner of a privately owned computer and/or computer system connected to Refuge House computers or systems or network is responsible for the behavior of users of that computer and/or computer systems and for all network traffic to and from Refuge House computers and/or systems.
- Private computers and/or computer systems may not be used to provide network access to individuals who would not have had access through Refuge House computers or computer systems.
- Privately owned computers and/or computer systems may not be used as a router to other networks or as an electronic gateway to non-Refuge House computers or computer systems.
- Privately owned computers and/or computer systems may not use Refuge House computers or computers systems or network for commercial gain or profit. Should Refuge House have reason to believe that a privately owned computer or system is using Refuge House computers or systems or network inappropriately, traffic to and from that system will be monitored and, if justified, the system will be disconnected and action taken with the appropriate authorities.
- Receiving more than one set of television signals from a single network tap or distributing these signals to multiple receivers is a violation of this policy.

- Knowingly accepting or using television signals which has been obtained by illegal means is subject to Refuge House disciplinary action.

Miscellaneous

- The use of Refuge House computers, computer systems or networks to effect or receive unauthorized electronic transfer of funds is prohibited.

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Preventing Computer Virus Problems

Purpose

The purpose of this policy is to provide guidelines for management and workforce members for preventing the computers from becoming infected with viruses.

Definitions

Computer Virus A parasitic software program written intentionally to enter a computer without the user's permission or knowledge and which attaches to files or boot sectors and replicates itself, thus continuing to spread. It is designed to invade computers and networks and wreak havoc on them. The mischief caused can be very minor, such as causing a funny image or cryptic message to be displayed on your screen, or it can do some serious damage by altering or even destroying files or the entire computer itself.

Policy

The following processes are required by Refuge House workforce members when using computers to prevent virus problems:

- Always run the anti-virus software approved by Refuge House
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis in accordance with Refuge House Data Backup and Retention Policy.
- If there are application conflicts when running anti-virus software, close the application, run the anti-virus utility to ensure a clean machine, and then re-open the application and try again. If the problem continues, consult the Security Officer. Whenever anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Be sure that the anti-virus software is updated daily.

Enforcement

Refuge House's Security Officer, office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Storage of Protected Health Information (PHI)

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the storage of protected health information.

Policy

Refuge House has a duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. This policy defines the guidelines and procedures that must be followed for the storage of PHI. All personnel must strictly observe the following standards relating to the storage of PHI:

- Refuge House personnel must ensure that, outside of regular working hours, all desks and working areas that contain PHI are properly secured, unless the immediate area can be secured from unauthorized access.
- When PHI is being released through electronic medium such as teleconference, video feed, or over the Internet, Refuge House personnel must treat the protection of PHI is the same manner as PHI recorded on paper, securing and limiting access to the PHI to authorized personnel only.
- When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.
- If PHI is to be stored on the hard disk drive or other internal components of a personal computer or PDA (Personal Digital Assistant), it must be protected by either a password or encryption. Unless encrypted, when not in use, this media must be secured from unauthorized access.
- If PHI is stored on diskettes, CD-ROM or other removable data storage media, it cannot be commingled with other electronic information.

Enforcement

Refuge House's office manager and supervisors are responsible for enforcing this policy. Employees and workforce members who violate this policy will be subject to disciplinary action, up to and including termination or dismissal.

Policy for Uses and Disclosures of Protected Health Information for Fundraising

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's protected health information for fundraising purposes.

Policy

In general, a patient's Protected Health Information (PHI) may not be used for fundraising purposes without specific authorization from the patient or the patient's representative. Refuge House fundraising personnel may only use and disclose dates of treatment and demographic information in connection with fundraising activities unless they obtain specific authorization from individual patients granting more expansive use of the patient's PHI. Demographic information generally includes name, address, other contact information, age, gender and insurance status.

Refuge House personnel and affiliated fundraising associates MAY:

- Use a patient's basic demographic information to solicit gifts.
- Access patients' dates of care.
- Use public information outside its internal database to send fundraising requests, without fear of violating this policy.

Refuge House personnel and affiliated fundraising associates MUST:

- Provide a *"Security and Confidentiality Notice"* to any patients they may be planning to contact. Patients may receive a *Security and Confidentiality of information* while at Refuge House, or calling the security office
- Include an opt-out provision along with the initial fundraising letter sent describing how individuals may opt out of receiving further fundraising materials.
- Exclude information about diagnosis, nature of services, or treatment in any solicitation.
- Remove that patient's information immediately from the mailing list upon receipt of an opt-out clause.
- Sign an appropriate *Contractor Agreement* before disclosing patient information to consultants or outside entities for fundraising activities (See *General Policy for Contractors*). This agreement is not necessary should Refuge House employees perform the fundraising.

After *Security and Confidentiality Notice* is given or sent, information that CAN be used for fundraising without authorization or consent includes:

- Name

- Address
- Other contact information (such as email, phone etc.)
- Age
- Gender
- Insurance status
- Date of service

Information that CANNOT be used *without authorization*:

- Diagnosis
- Nature of services
- Treatment. Caution should be used when divulging the matter of treatment.

When a prospective contributor voluntarily discloses information about diagnosis and treatment to a member of Refuge House's fundraising staff, that information can then be used for other fundraising purposes.

Enforcement

Refuge House's office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

References

45 C.F.R. §164.514(f) (1)

45 C.F.R. §164.508

Policy for Uses and Disclosures of Protected Health Information For Judicial or Administrative Proceedings

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) judicial and administrative proceedings.

Definitions

Disclosure: The release, transfer, provision of access to, or divulgence in any other manner, of patient protected health information to any individual or organization outside of Refuge House

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within Refuge House

Qualified Protective Order Restricting the Use of PHI: with respect to PHI requested under this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

1. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
2. Requires the return to Refuge House or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Policy

As a general rule, Refuge House personnel may not disseminate PHI without authorization, unless it is requested by the individual to whom the PHI belongs, and a valid authorization has been obtained. However, PHI may be used or disclosed for judicial or administrative proceedings if the use or disclosure is made in response to a court order, administrative tribunal order, subpoena, discovery request, or other lawful process.

Permitted Disclosures

Refuge House may use or disclose PHI in the course of any judicial or administrative proceeding if:

1. The disclosure is in response to an order of a court or administrative tribunal, provided that Refuge House discloses only the PHI expressly authorized by such 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 (such as a subpoena), if:
    A. Refuge House receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request (with an affidavit from the requesting party); or

B. Refuge House receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of this section (in Definitions above).

3. Refuge House receives satisfactory assurances from a party seeking PHI along with a written statement and accompanying documentation demonstrating that:
   A. The party requesting such 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);
   B. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
   C. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
   D. No objections were filed; or
   E. All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
4. Refuge House receives satisfactory assurances from a party seeking PHI including a written statement and accompanying documentation demonstrating that:
   A. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
   B. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

5. Notwithstanding this section, Refuge House has the option to disclose PHI in response to lawful process without receiving full satisfactory assurance, if Refuge House of its own accord makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of this section or to seek qualified protective order.

Enforcement

Refuge House's office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

References

45 C.F.R. §164.512(e)

Policy for Uses and Disclosures of Protected Health Information for Marketing

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) for marketing.

Definitions

Marketing: The promotion or advertisement, by Refuge House, of specific products or services if Refuge House receives, directly or indirectly, a financial incentive or remuneration for the use, access, or disclosure of PHI. Marketing does not include a communication for treatment or health care operations by a health care provider, health plan, or participants in an organized health care arrangement or their affiliated covered entities or contractors.

Policy

General Rule on Marketing

Refuge House's employees and workforce members may not disclose, use, sell or coerce an individual to consent to the disclosure, use, or sale of PHI for marketing purposes without the consent or authorization of the patient or representative who is the subject of the PHI. This prohibition includes the disclosure, use or selling of prescription drug patterns. Certain marketing activities, as described below, do not require Refuge House to obtain patient authorization for the use or disclosure of PHI.

Refuge House's employees and workforce members shall not disclose identifiable information such as policy numbers or similar access data codes from a patient's policy or transaction account to any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer unless the patient has authorized the disclosure.

Exceptions to General Rule

Refuge House may use and disclose PHI without obtaining an authorization from the patient to:

1. Provide information on health related products and services in a face-to-face encounter with the patient;
2. Provide information on common health care communications, such as disease management, wellness programs, prescription refill reminders and appointment notifications;
3. Provide the patient with information on participating providers or plans in a network or alternative treatment options;
4. Provide sample products to the patient; and

5. Provide marketing communication involving promotional gifts of nominal value (e.g. calendars, key chains, etc. that promotes Refuge House or a health care manufacturer's products or services).

Rules for Written Marketing Communication from Refuge House

If the marketing communication is not face-to-face but in written form, Refuge House must make a determination prior to sending out the marketing communication that the product or service being marketed may be beneficial to the health of the patient. In addition, Refuge House is required to send envelopes to the patient that has only the addresses of the sender and the recipient and must:

1. State the name and phone number of Refuge House or the Refuge House affiliated entity sending the marketing information,
2. Explain clearly the recipient's right to have his/her name removed from the sender's mailing list,
3. If Refuge House or a Refuge House affiliate for marketing purposes receives a patient's request for removal from the mailing list, such removal must occur immediately, within FIVE days of receipt of request, and
4. Refuge House must explain in the communication why the patient has been targeted and how the product or service relates to their health.

Enforcement

Name of Health Care Provider]'s office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

Reference

45 C.F.R §164.514

Policy for Uses and Disclosures of Protected Health Information to Family and Friends of Patients

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) with patient's family and friends.

Definitions

Disclosure: The release, transfer, provision of access to, or divulgence in any other manner, of patient protected health information to any individual or organization outside of Refuge House

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within Refuge House

Policy

Refuge House may use and disclose certain PHI without the written consent or authorization to release the information from the individual. The individual must be informed in advance of the use or disclosure and have the opportunity to agree, prohibit, or restrict the disclosure.

Refuge House may orally inform the individual of the permitted uses and disclosures and obtain the individual's agreement or objection to a use or disclosure permitted by this policy. In some circumstances, Refuge House may use and disclose certain information without consent, authorization, or oral agreement as outlined within this policy.

Refuge House employees and workforce members must document the agreement, prohibition, or restriction in the medical record.

Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

Refuge House may disclose to a family member, other relative, a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

Refuge House may use or disclose PHI to notify or to assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Refuge House can also use and disclose PHI in these circumstances for identifying or locating the types of persons mentioned above. In order for Refuge House to use or disclose PHI for these purposes, the individual's presence is a determining factor. The following processes outline how Refuge House may use and disclose PHI for these purposes.

Uses and Disclosures with the Individual Present

If the individual is present for, or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, Refuge House may use or disclose the PHI if it:

1. Obtains the individual's agreement;
2. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to such disclosure.

Limited Uses and Disclosures When the Individual is Not Present

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, Refuge House may, in 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. Refuge House may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X rays, or other similar forms of PHI.

Enforcement

Name of Health Care Provider]'s office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

References

45 C.F.R. §164.510(b)

Policy for the Verification of Identity and Authority of Requestor of Protected Health Information (PHI)

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the verification of identity and authority of requestors of protected health information.

Definitions

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

Individually Identifiable Health Information: Any information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse; and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual.

Verification: Process to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity. Verification must include obtaining any documentation, statements, or representations, whether oral or written from the person requesting the protected health information when such documentation, statement or representation is a condition of the disclosure under this subpart.

IS Manager and/or Quality Personnel: The person officially designated to oversee all ongoing activities related to the development, compliance, implementation, maintenance of, and adherence to the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state laws that may apply.

Public Official: A person who has been legally elected or appointed and who has been empowered by law/regulation to exercise the duties and functions of their office for the public good.

Policy

General

Refuge House's IS Manager and/or Quality Personnel, and other staff and employees as required, shall verify the identity of the requestor and ensure the requestor has the proper authority to request such information.

The patient or personal representative must sign a valid authorization for the disclosure of confidential protected health information before such PHI can be released to a requestor, except as required by existing HIPAA exemptions or requirements.

All requests for disclosure shall be forwarded to the IS Manager and/or Quality Personnel or designee including the following:

1. The name of the requesting party or parties and
2. Any documentation, statements or representations from the person requesting the PHI of his/her authority to request such information (i.e., legal representative of consumer, law enforcement official, etc.).

The requestor must present identification prior to receipt of any records regarding themselves.

Refuge House's IS Manager and/or Quality Personnel or designee staff may rely on the following information to demonstrate identity:

1. Presentation of agency identification, credentials or other proof of government status (a badge, identification card, etc.);
2. A written request on agency letterhead or an oral statement if a written statement would not be possible (a natural disaster, other emergency situations, etc.);
3. If the disclosure is requested by a person acting on behalf of a public official, a written statement on government letterhead that the person is acting under the government's authority, or a contract or purchase order evidencing the same; or
4. A court order.

Refuge House's IS Manager and/or Quality Personnel or designee shall verify identity of any phone requests from all individuals, including law enforcement officers and others who have an official need for PHI by using a callback phone number before releasing information.

Refuge House's IS Manager and/or Quality Personnel or designee shall verify facsimile number of any faxed requests. The main number of the sending agency shall be called, and the fax number verified. Fax machines shall be set to imprint the origin. All incoming faxes shall be reviewed for imprint origin.

Refuge House's IS Manager and/or Quality Personnel or designee shall verify e-mail address by calling requestor. The general number for the sending agency shall be called, and then a request shall be made to be transferred to the specific individual who made the contact.

Refuge House's IS Manager and/or Quality Personnel or designee personnel are responsible for copying verification information or obtaining badge number, etc., and for creating a file for the requestor and for maintaining the information in the requestor's file.

Refuge House's IS Manager and/or Quality Personnel or designee must review the forwarded information and determine if he or she is satisfied that the documents verify the identity of the requestor and also demonstrate that the requestor has authority to request the information under state and federal law.

Refuge House's IS Manager and/or Quality Personnel or designee may disclose information to the requestor if all requirements for use and disclosure are met, and if all requirements within this policy are met.

Refuge House's IS Manager and/or Quality Personnel or designee shall contact agencies or other entities for further verification of identity or authority to receive PHI, if necessary.

Refuge House's IS Manager and/or Quality Personnel or designee may deny access to information, if verification of identity or authority is not accomplished.

Refuge House's IS Manager and/or Quality Personnel shall assure that a mechanism is in place which tracks disclosure of both written and verbal protected health information. The same format shall be utilized for all facilities.

Enforcement

Refuge House office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

Policy for Mandatory Workforce Training

Purpose

The purpose of this policy is to provide information for management and workforce members regarding mandatory workforce training as required by the Health Insurance Portability and Accountability Act (HIPAA).

Definitions

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

Individually Identifiable Health Information: Any information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse; and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the facility holding the information.

Health Insurance Portability and Accountability Act (HIPAA): Public Law 104-191 enacted on August 21, 1996.

Code of Federal Regulations (CFR): Refers to 45 CFR Parts 160, 164 and 142, for Privacy and Security rules.

Privacy Training Rule: 45 CFR § 164.530(b)(1) states “a covered entity must train all members of its workforce on policies and procedures with respect to health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity”.

Security Training Rule: 45 CFR § 142.308(a) (12) requires “education concerning the vulnerabilities of the health information in an entity’s possession and ways to ensure the protection of that information”.

Mandatory Training: Refers to the requirements as noted in HIPAA's Privacy and Security Rules as defined above.

Initial HIPAA Training: Workforce training which shall only be conducted under the direction of Refuge House’s IS Manager and/or Quality Personnel.

Patient: Any individual who has received or is receiving services from Refuge House

Policy

Mandatory Training

All workforce members of Refuge House, including staff, volunteers, students, interns and contract employees in a Refuge House facility on a regular course of business, shall attend training on the Privacy and Security provisions of HIPAA. This training shall follow a specific curriculum established by Refuge House

HIPAA training curriculum must remain consistent practice-wide to assure appropriate implementation of the HIPAA Privacy and Security regulations. To maintain that important consistency, no local customization at a branch facility of Refuge House shall be permitted.

Employees and workforce members, including staff, volunteers, students, interns and contract employees in a Refuge House facility on a regular course of business, hired or engaged **prior** to April 14, 2003, shall receive HIPAA privacy and security training prior to April 14, 2003.

Employees and workforce members, including staff, volunteers, students, interns and contract employees in a Refuge House facility on a regular course of business, hired or engaged **after** April 14, 2003, shall receive training as part of their initial employee orientation. The content for the HIPAA new employee orientation shall be the same as for employees hired before April 14, 2003. HIPAA new employee orientation must take place within 14 days of the date of hire.

- Trainings shall be conducted either in person for via electronic conference.
- Additional mandatory privacy training shall be scheduled every six months or whenever there is a material change in Refuge House's privacy policies or procedures as determined by Refuge House's IS Manager and/or Quality Personnel.
- Periodic mandatory security training shall be scheduled every six months.

If applicable, each manager at each branch facility of Refuge House shall identify group(s) or individuals who, due to the nature of their job function, will require in-depth training related to HIPAA, and that specialized training shall be provided by Refuge House's IS Manager and/or Quality Personnel.

Documentation of Mandatory Training

Mandatory HIPAA training shall be documented and maintained for so long as the workforce member is in the employee of Refuge House

Enforcement

Refuge House office manager and supervisors are responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

MIS & IS REVIEW MATRIX

Item for Review	Frequency	By Whom (may be a designee)
HIPAA Policy and Procedure	Annually	• IS Director • CEO
Accounting Systems Personnel	Annually	• IS Director • CEO
Radius Jurisdictions Authorities Framework	Semi-Annually	• IS Director • CEO • Program Director • Quality Development
Radius Employee Jurisdictions	Quarterly, Upon Hiring/Separation	• HR/Office Personnel • IS Director • Program Director • Quality Development
Radius Client Jurisdictions	Quarterly	• IS Director • Program Director
Radius Relations	Monthly, Ongoing/As Needed	• Program Director • Treatment Director(s)
Radius Functionality Framework	Annually, As Needed	• IS Director • Quality Development
Cloud Framework Operation and Security	Quarterly, Ongoing/As Needed	• IS Director • CEO • Quality Development
Cloud Users and Authorities	Monthly, Upon Hire and Separation	• Office/HR Personnel • IS Director • CEO