MANAGEMENT

OF

INFORMATION

SUBJECT INFORMATION MANAGEMENT

Administrative Safeguards

General Guidelines to Safeguard Protected Health Information Reference: 45 CFR § 164.308(a)(1)(ii)(A) & (B)

Responsibility: EXECUTIVE DIRECTOR and all members of the workforce.

Background:

The following guidelines are in accordance with the final Security Rule and consistent with the HIPAA privacy requirement to safeguard protected health information (EPHI). See 45 CFR § 164.530(c).

POLICY:

The Compass Recovery will use reasonable administrative, physical, and technical safeguards to guard the privacy of protected health information and limit incidental uses or disclosures of protected health information. An incidental *use* or *disclosure* is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a byproduct of an otherwise permitted use or disclosure. For example: a conversation that is overheard despite attempts by the speakers to avoid being heard.
All members of the Compass Recovery workforce will follow these guidelines in handling protected health information (PHI) to guard the privacy of protected health information and limit incidental uses and disclosures.
Guidelines to Safeguard Protected Health Information
1. Bulletin boards:
Bulletin boards may not contain any documents with PHI of clients, unless the client has authorized the display in accordance with the AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION. - This includes:

a. Baby pictures (even without a name or other identifying information)
b. Cards and notes of appreciation

2. Computer Screens:

A. Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display.
B. Computer displays will be configured to go blank, or to display a screen saver when left unattended for more than a brief period. The EXECUTIVE DIRECTOR will determine the period. Wherever practicable, reverting from the screen saver to the display of data will require a password.

3. Conversations:

a. Conversations concerning clients and potential clients' treatment, or other PHI must be conducted in a way that reduces the likelihood of being overheard by others.

4. Hardcopies of PHI

a. Claims and other medical record documents that contain PHI must be placed face down on counters, desks, and other public places where third parties might see them.

b. Wherever it is reasonably possible to do so, claims and other documents containing PHI will not be left on desks and countertops after business hours or for extended periods of time unsupervised. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers, or other means to secure PHI during periods when the area is left unattended.
c. In areas where locked storage after hours cannot reasonably be accomplished PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

5. Disposal of paper with PHI:
   a. Paper documents containing PHI must be shredded when no longer needed.
6. Key policy
   a. The EXECUTIVE DIRECTOR will develop a list of personnel, by job title, which may have access to which keys. This includes electronic key cards and metal keys, and applies to keys to storage cabinets, storage rooms, secure areas, and buildings.
   b. Keys must be surrendered upon termination of employment.
   c. The security official will change locks whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.
7. Portable Electronic Devices
   a. The Compass Recovery privacy and security policies apply to any EPHI that is stored on a portable electronic device.
   b. Users of portable electronic devices may not download EPHI to their portable electronic device without permission of the EXECUTIVE DIRECTOR.
   c. Users of portable electronic devices are responsible for assuring that the EPHI on their devices is kept secure and private.
   d. Any loss or theft of a portable electronic device thought to contain EPHI must be reported to the EXECUTIVE DIRECTOR immediately.
   e. Users of portable electronic devices who store EPHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords, token devices, or biometrics).
   f. At termination of employment, users of portable electronic devices will surrender to Compass Recovery the portable electronic device or remove the employer's EPHI from the user’s portable electronic device under direction of the Security Official.
8. Printers:
   a. Printers must be in secure areas, where only authorized members of the workforce can have access to documents containing PHI are being printed.
9. Subsidiary databases:
   a. Any member of The Compass Recovery workforce who maintains a separate database containing EPHI must make it known to the EXECUTIVE DIRECTOR. e.g. Microsoft Excel or Microsoft Access.
   b. No member of The Compass Recovery workforce may maintain a separate database containing EPHI without specific permission of the EXECUTIVE DIRECTOR.
   c. The EXECUTIVE DIRECTOR must determine whether this database constitutes a "designated record set."
   d. Definition: Designated record set means:

e. A group of records maintained by or for a covered entity that is: The medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or used, in whole or in part, by or for the covered entity to make decisions about individuals.
f. The EXECUTIVE DIRECTOR must assure that the data is secure, and in compliance with relevant Compass Recovery policies.
g. If the data is to be synchronized with other databases additional procedures must be in place to ensure integrity.
h. Any member of the workforce who uses and discloses EPHI in a subsidiary database must follow The Compass Recovery policies.

10. Workforce Vigilance:
    a. All members of the workforce have a responsibility to watch for unauthorized use or disclosure of EPHI, to act to prevent the action, and to report suspected breaches of privacy and security policies to their supervisor, or to the Privacy or Security Official (example of a breach: client or visitor accessing an unattended workstation).
    b. This responsibility will be included in workforce training.
    c. This responsibility will become a part of all work staff job descriptions.

Risk Analysis and Ongoing Risk Management

The final federal HIPAA regulations relating to the security of all electronic *protected health information* (EPHI) requires each covered entity to create and implement policies and procedures designed to balance the following:

- The organizations ability to keep electronic protected health information confidential and true to its source with;
- Its availability to support the health care process.

Risk analysis is a process that can be used to identify possible threats and vulnerabilities, and to identify possible ways to reduce the associated risk. Once the risk baseline is determined via an initial analysis, the risk management process allows for the application of policy and technology to reduce, mitigate, or manage the risk. Thus, a covered entity uses the risk analysis and risk management process to reduce risk to organizationally acceptable levels. The acceptable level depends on the size of each organization and value of its assets. At a minimum, an organization should put in place safeguards to minimize the risk of inappropriate use or disclosure of PHI whenever workforce members act.

POLICY:

1. Compass Recovery recognizes the importance of the risk analysis and risk management functions. As such, it has focused time and resources to develop an effective risk management process involving individuals at all levels of the organization. Risk management validates the effectiveness of chosen policy and/or solutions serving to balance the protection of confidentiality of electronic protected health information (EPHI) with the ability to make it available to support the client care and related health care process.

.

2. Risk Management includes three components:
    a. Risk Assessment- The process to determine level of risk
    b. Risk Mitigation- The process to decrease the determined level of risk

c. Evaluation and Assessment – The process to monitor and act to maintain the decreased level of risk. *(Note: Evaluation and Assessment also becomes part of ongoing Risk Management.)*

3. The EXECUTIVE DIRECTOR will work with operational and business representatives to develop a focused team to conduct an initial, comprehensive risk analysis. The initial risk analysis will be utilized as a template to form the basis of ongoing and future risk management and evaluation activities. The initial risk analysis will include the following components at a minimum:

a. Baseline development and value determination covering Administrative, Physical, and Technical requirements
b. Determination of level of reasonability and scalability for the organization by weighing size, complexity, organization capabilities, cost, technical capabilities, probable threats, and related costs.

4. Unique Factors Determine Level of Reasonable and Scalability. All information gathered will be considered in accordance with the following factors:

a. Size, complexity, and capabilities of Compass Recovery technical infrastructure, hardware, software, and security capabilities.
b. Costs of security measures
c. Probability and criticality of potential risks to electronic protected health information. Potential risks or threats will be thoroughly evaluated. *A threat is an incident that can reduce the value of an asset. Threats can be natural (floods, earthquakes), accidental, or man-made (terrorist activities).*

5. The EXECUTIVE DIRECTOR will oversee the performance and documentation related to the risk analysis project. All information gathered will be organized, maintained securely and retained in accordance with Compass Recovery Center's documentation policies (at least six years from the initial date of creation or the date when it last was in effect whichever is greater).

6. Risk Mitigation
The EXECUTIVE DIRECTOR will work with a chosen committee to choose Compass Recovery preferred process and/or technical solution(s) designed to address the Security requirement and decrease or mitigate the associated level of risk. The following factors will be considered during this process:

a. Various other factors including initial organization size and subsequent changes in size, complexity, capabilities, cost, and probability of threat to the protected health information
b. All areas defined in the procedure as "Implementation Considerations"
c. Investigation of technical solutions or products designed to meet the goals of the policy
d. The ability for the process and/or technical solution to balance the confidentiality of the protected health information with the ability of the solution to allow for data integrity and availability

The EXECUTIVE DIRECTOR will additionally assure that all related policies and procedures will be updated, including training materials.

a. To the extent that workforce functions are affected by the chosen solution, the training department will work with managers to coordinate and assure that the solution is implemented, and each affected member is trained.
b. Once a process and/or technical solution is chosen, the EXECUTIVE DIRECTOR will work with the committee to assure the various related implementation subtasks are appropriately assigned allowing for a realistic implementation process.

The EXECUTIVE DIRECTOR will assure that routine monitoring (ongoing risk evaluation and assessment) of this solution is carried out on a (daily, monthly, quarterly) basis to continually assess the effectiveness of Compass Recovery's ability to balance the confidentiality of the protected health information with its integrity and availability.

Sanctions for Violating Privacy and Security Policies and Procedures
Reference: 45 CFR §§ 164.308(a)(1)(ii)(C) and 164.530(e)

Responsibility: Privacy Officer, Executive Director

Background:
Federal HIPAA privacy and security regulations require covered entities to establish and apply sanctions against members of the *workforce* who violate the entity's privacy and/or security policies that relate to the privacy and security of protected health information.
Additionally, it is important that a covered entity also have sanctions for privacy and security violations for applicable state and federal laws that relate to protected health information.
POLICY:
1. Members of Compass Recovery workforce are subject to disciplinary action for violation of policies and procedures. Disciplinary action is utilized to hold workforce members accountable for their behavior as it relates to the use and disclosure of protected health information, including the application of the minimum necessary concept. Violations that jeopardize the privacy or security of *protected health information* are particularly serious. This seriousness is reflected the disciplinary action, up to and including termination of employment.

a. All workforce members are thoroughly trained on the consequences of violating privacy and security policies. This training occurs upon initial employment and then on a routine and recurring basis in accordance with policy entitled TRAINING PROGRAM: USES AND DISCLOSURES IN SAFEGUARDING EPHI. User Confidentiality Agreements or Acceptable Use Policies are reviewed and signed upon initial employment and then annually thereafter.
b. All members of the workforce will be treated fairly and equitably in the imposition of sanctions for privacy and security violations. All penalties for non-compliance resulting in sanctions will be applied consistently across the organization. All breaches of privacy and security policies will result in immediate consequences in accordance with the defined penalties regardless of job status or reason for violation.

c. Sanctions will be integrated into Compass Recovery Center’s overall employee discipline policy. This policy will be in writing.
d. Management shall also reserve the right to monitor system and media device activity to ensure the enforcement of policies.
e. Disciplinary actions due to breaches of privacy or security of EPHI will be documented,

and the documentation must be retained for six years. Disclosure of EPHI in violation of policy is reportable under the ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION policy.

f. No member of the workforce, and no business associate, will be subject to sanctions for a *disclosure* of EPHI made in good faith in accordance with the following policies which function to assure the organization does not retaliate against an individual who performs whistleblower activity or reports EPHI as a victim of a crime:

DISCLOSURE OF PROTECTED HEALTH INFORMATION BY "WHISTLE BLOWERS"

PROCEDURE:
These policies will be incorporated into Compass Recovery's overall employee discipline and sanction policy.
1. All Managers are trained to contact the EXECUTIVE DIRECTOR in an expeditious manner whenever a workforce member is suspected of or knowingly violates any of the organization's Privacy and/or Security Policies and Procedures. The violation may be reported in a variety of ways including but not limited to the following:

a. Resulting from Management activity,
b. Privacy Complaint,
c. Security Incident Report

Determine if organizational mitigation is appropriate. Take into consideration if the individual attempted to mitigate the situation if applicable.
Determine if other workforce members were involved or had knowledge of the violation and whether reasonable action should have been taken.
Determine if report was conducted in bad faith or malicious in nature.
Determine application and management workforce responsible to communicate and carry out disciplinary sanctions of any involved workforce members as necessary in accordance with the Sanctions Policy.

2. All necessary actions, including outcomes, will be handled promptly and documented in accordance with Compass Recovery' policy.

3. On a routine basis (quarterly or monthly) the EXECUTIVE DIRECTOR, provides to the organization's senior management level representatives, aggregate reporting of all received privacy and security violation reports, and the organization's response, including level of sanctions applied, mitigation attempts and/or resulting changes to policies and procedures.

4. The EXECUTIVE DIRECTOR will periodically perform the following:
   a. Determine if each issue should be evaluated as part of a larger review (such as part of ongoing risk analysis), and whether systems configuration and/or changes to other related Compass Recovery policies and procedures are necessary to lessen the chance that similar workforce behavior/violation will reoccur.
   b. Address communication and training to all affected workforce members if policies and procedures are to be implemented or modified in accordance with MAINTENANCE OF

POLICIES AND PROCEDURES document.

c. Review Compass Recovery' discipline policies to assure that breaches of security and privacy of EPHI are dealt with adequately and fairly.

5. The EXECUTIVE DIRECTOR will document disciplinary actions and will retain the documentation for at least six years.

Assignment of Security Responsibility
Reference: 45 CFR § 164.308(a)(2)(3), (4), (6), (7).

Responsibility: EXECUTIVE DIRECTOR

Background:
The final federal HIPAA regulations relating to the security of all *protected health information* (PHI) require an assigned security responsibility. The individual designation serves to enhance the accountability of Security issues for the organization by defining a clear structure with distinct lines of responsibility. Each covered entity must designate a Security or Privacy Officer (PO) to oversee the development and implementation of the policies and procedures required for compliance with the privacy and security of HIPAA regulations.

The PO should hold special knowledge and training in the administration and execution of a security management process covering administrative, physical, and technical safeguards necessary to guard data integrity, confidentiality, and availability. The PO should also possess a thorough understanding of importance of protecting organization critical information assets and can assure the appropriate level of integration of overall security into the budget and capital planning process
.
POLICY:

1. The Compass Recovery recognizes the importance of specialized oversight for the development and implementation of the organization's security responsibilities. For this purpose, a PO has been designated with the assigned responsibility to help develop, implement, manage, and supervise the execution and use of a consistent entity wide security program. The PO's duties shall include, but not be limited to, the following:
   a. Establish entity wide security management structure. This includes the development of a documented and current Security Program or Plan.
   b. Work to develop, implement, and oversee the Security Management Process including Risk Analysis and Risk Management provisions. Security Management Process refers to creating, administering, and overseeing policies to ensure the prevention, detection, containment, correction, and mitigation of security breaches. The requirement for this process includes the use of risk analysis and risk

   c. management, and must include formal security, information system activity review, and sanction policies.
   d. Oversee process for systems evaluation: The technical evaluation that establishes the extent to which a computer system or network design and implementation meet a pre-specified set of technical and non-technical security requirements.
   e. Coordinate development and execution of the Compass Recovery *contingency plan:* The

contingency plan will include at a minimum:

i. Applications and data criticality analysis,
ii. A data backup plan,
iii. A *disaster recovery* plan, [Please refer to the P&P Manual]
iv. An *emergency mode operation* plan, and
v. Testing and revision procedures.

f. Unify and oversee information access control standards including assisting management in assigning appropriate system access to data.
g. *Access* refers to the ability or the means necessary to read, write, modify, *or* communicate data/information or otherwise make use of any system resource
h. *Access control* refers to a method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day access, and classification or role-based access.
i. Monitor internal *audit controls* of system records activity and respond to variances. *Audit controls* refer to mechanisms to record and examine system activity. This includes recording pertinent data relating to the creation, modification, transmission, deletion of records, and access to sensitive records, including access log monitoring. Sensitive records include records of employees and VIPs, or records of *patients/clients* with protected diagnoses such as HIV or mental illness. Audit controls may also include procedures to monitor access to a statistical sample of all records. Audit controls allow an organization to identify suspect data activities and respond to potential weaknesses.
j. Maintain and manage personnel *authorization controls* and clearance records. *Authorization controls* refers to a mechanism for obtaining consent within the system for
k. the use and *disclosure* of health information. These controls may be role-based or user-based.
l. Oversee Security Configuration Management: The integration process to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses.
m. Oversee Incident Response procedures. Security Incident Procedures refers to the requirement to implement formal, documented instructions for reporting and responding to security breaches.
n. Coordinate initial access management, termination, and/or modification of *access* to information systems.
o. Oversee Malicious Software Infrastructure. Ensure entity wide anti-virus infrastructure is in place and operational.
p. Provide technical assistance for company-wide security awareness training.
q. Develop and oversee Device and Media Controls: The requirement for formal, documented policies and procedures that govern the receipt, removal,

r. and storage of data storage media into and out of a facility. They are important to ensure total control of media containing health information.
s. Assessing and monitoring ongoing compliance with Security policies and procedures including addressing new requests for data.
t. Performance of troubleshooting for security and security related issues.

Assignment and Management of Information Access Privileges
Reference: 45 CFR §§ 164.308(a)(3), (a)(4)(i) and 164.514(d)(2)

Responsibility: EXECUTIVE DIRECTOR/Privacy Officer

Background:
Not all members of The Compass Recovery workforce need to have *access* to all *electronic protected health information* (EPHI). Limiting or restricting access to those with a "need to know" is a basic component of security. The Compass Recovery assigns minimum *access profiles* to job titles based on how much information, pertaining to which types of workforce *member,* is needed to accomplish work assignments. These vary based upon the workforce member needs, the management information system capabilities, and the specific data to be accessed. The technical mechanism used to control or limit the access based upon this profile will vary depending upon the application or technology used but often consists of at a minimum, a uniquely assigned user login and password.
These access profiles are used for the following purposes:

- Authorization. For PHI that is entered or stored electronically, the *access profile* determines which information an individual member of the workforce may read through a computer terminal.
- Access Authorization, Establishment, and Modification. Once authorization and workforce clearance are assigned based upon job category, the technical process used to initially grant or authorize, and then to establish and maintain the access is carried out. Access may be modified on an ongoing basis as well depending upon job category and subsequent need.

POLICY:
Workforce Clearance and Authorization Access Profiles

1. The Compass Recovery will maintain workforce clearance and authorization access profiles to specify which electronic protected health information may be used by workforce members in each job class. These profiles will specify the data elements that comprise protected health information.
2. Access profiles are based upon two principles: First, that access to information must not be so restricted as to interfere with the efficiency of operations or the quality of services; and second, that access must be sufficiently restricted to afford individuals as much privacy and security as possible.
3. Access profiles will be used to limit electronic access to protected health information and will comply with the Privacy MINIMUM NECESSARY RULE.
4. Access Establishment and Modification
    i. Upon creation of any new access profiles and based upon those rights or limits defined in

    ii. accordance with the job description, measures are taken to secure current systems with commensurate access.

    iii. Upon successful demonstration of need, a specific access profile may be modified for members of the workforce who have a demonstrated need to

read additional information to accomplish their work assignments.

Termination or Modification of Access to Protected Health Information: Facility Controls and Electronic Systems
Reference: 45 CFR § 164.308(a)(3)(C)
RESPONSIBILITY: EXECUTIVE DIRECTOR, Human Resources Director

Background:
When an employee ends his/her employment, or when an internal or external information systems user's *access* to certain types of data is withdrawn, appropriate security measures must be taken to minimize the possibility of unauthorized access to secure data by those who are no longer authorized to have access to that information. This may include *business associates,* such as system maintenance contractors, as well as employees and other members of the *workforce.* Procedures that may be appropriate upon the termination of access privileges include:

- Changing locks/access codes
- Removal from access lists
- Removal of user account(s)
- Turning in keys, tokens, or cards that allow access to PHI
- Review of any employment agreements
- Turning in any TSN-owned hardware

POLICY:
Compass Recovery will terminate access to information systems and other sources of *protected health information* (PHI), including access to paper files and access to rooms or buildings where PHI is located, when a Compass Recovery employee, agent, or contractor ends his/her employment or engagement. Compass Recovery will modify/terminate access to specific types of PHI when the status of any business associate or member of the workforce either no longer requires access to those types of information or requires a different degree of access.

It is the duty of the EXECUTIVE DIRECTOR or person assigned to such task to receive all notices of termination or modification of access authorization, and to document that all required procedures have been followed to accomplish termination of access in a timely fashion.

The EXECUTIVE DIRECTOR will coordinate these actions with Human Resources (or a designee). *When warranted, the advice of legal counsel will be sought for termination of contract resulting from breach or involuntary termination of workforce member involving special circumstances.*

PROCEDURE:
Upon termination of employment, contract, or assignment requiring a level of access

authorization, the department manager overseeing the employee, consultant, or agent, will immediately complete a Notice of Termination or Modification of Access form (Notice).

The Notice will include the individual's name, department (contractor, company, or agency), access site, known information access rights, a description of the modifications to

access required by the change in status, and date that the termination or modification is effective.

The Notice will be sent to the EXECUTIVE DIRECTOR or person assigned to this task in the most expeditious manner available. *Whenever possible, this Notice is to be completed and submitted at least several days prior to the effective date of the change of access status.*

a. A copy of the Notice will be sent to the Director of Information Systems.
b. If the termination or modification of access is for an employee, a copy of the Notice will be sent to the Human Resources department for inclusion in the employee's file.
c. If the termination or modification of access applies to a business associate, a copy of the Notice will be sent to the general management for inclusion in the business associate's contract file.
d. The EXECUTIVE DIRECTOR will maintain a copy of all termination or modification Notices.

The EXECUTIVE DIRECTOR will record receipt of the Notice and initiate the process of access termination or modification in the relevant information system(s) as well as the following steps, as deemed necessary to maintain overall systems' security:

a. Retrieving Keys, Tokens, or Cards that Allow Access: The EXECUTIVE DIRECTOR will coordinate with the Human Resources department to assure that all materials allowing access to Compass Recovery properties, buildings, or equipment are retrieved from a terminated employee, agent, or contractor prior to his/her final exiting of the premises. Similarly, keys, tokens, and cards that allow access to types of information that an individual is no longer authorized to use must be retrieved when the change in access status becomes effective.
b. Removal or Modification of User Accounts: The EXECUTIVE DIRECTOR will assure the deletion of an individual's access privileges to the information, systems, services, and resources for which they no longer require authorization. *The EXECUTIVE DIRECTOR will decide, based on the type of termination and systems in place whether it might make more sense to simply disable the account and change the password. This will allow appropriate personal to access information that might have been created or encrypted by the terminated user and change the rights of that information. Once it is determined the account is no longer needed then it will be removed.*
c. Prior to the final exit of an employee, he or she should be reminded of and review any non-disclosure or employment agreements that have been signed. The employee should be reminded that any PHI received during employment still falls under these agreements. This reminder should be documented as part of the exit interview.

On a routine basis, the EXECUTIVE DIRECTOR will review a representative sampling of Notice of Termination or Modification of Access Forms to determine that the forms are being utilized appropriately and that the process is working efficiently and in a timely manner.

Any issues associated with this review will be communicated appropriately and monitored for compliance improvement.

Rationale:
This policy and procedure for termination or modification of information access

should be combined with existing Compass Recovery policies and procedures for termination of employees, contractors, and agents. The important elements stated here are the control and oversight of the EXECUTIVE DIRECTOR to assure immediate information systems access termination or modification, changing of locks, and retrieval of security keys, tokens, or cards. Each department manager will need to be trained in the proper procedures to maintain information systems' security as well as all Department of Human Resources requirements for termination of employment.

SUBJECT: INFORMATION MANAGEMENT PLAN

Purpose:
Compass Recovery recognizes that the provision of healthcare is a complex endeavor that is highly dependent on information. This includes information regarding the individual client, the care provided, the outcomes of care and the performance of the organization. Due to the collaborative nature of the provision of care, all activities performed are coordinated and integrated throughout all services. It is because of this dependent relationship that information is an important resource that is to be used effectively and efficiently managed.

Goal

The goal of the Information Management Plan is to obtain, manage and use information to enhance and improve individual and organizational performance in client care, governance, management and support processes.

Objectives

Information management is a function, a set of processes and activities focused on meeting Compass Recovery' information needs. Issues of timeliness, accuracy, security, confidentiality, access, efficiency, collaboration, integrity and uniformity of data are considered in the overall management of information.

To plan for managing information, including:

- Identification of internal and external information needed to provide safe, quality care.
- Identification of how data and information enter, flow within, and leave the organization.
- Use of the information identified to guide development of processes to manage information.
- Selection of staff to participate in the assessment, selection, integration, and use of information management systems for the delivery of care, treatment, or services.
- To plan for continuity of the information management process, including establishing a written plan for managing interruptions to information processes.
- To protect the privacy of health information throughout the information management process.
- To maintain the security and integrity of health information.

Standards & Management of Information

The standards of timeliness, accuracy, completeness, security, confidentiality, protection and safeguarding, access, efficiency and collaboration, integrity and uniformity of data are considered in the overall information management function.

Security and Confidentiality of Information: Compass Recovery has considered the need for and appropriate levels of security and confidentiality of data and information. Each individual employee authorized to enter, and access information will be provided with a unique username and will create a unique password.

- Data is protected in accordance with a Policy on "Integrity and Security of Health Information"
- Clinical staff will have access to all pertinent client information to allow for optimum assessment, treatment and care of the client in accordance with general policies and privacy.
- Medical Director/staff will have access to all pertinent client information that will allow them to render optimum treatment to any client involved in services.
- Clerical staff will have access to all necessary client information that allows for appropriate billing, insurance and financial procedures.
- All other individuals including ancillary staff and administrative staff will have access to client data and information on an as needed basis, restricted to level of authority, in accordance with facility-wide policies and procedures governing information security and confidentiality.

Flow of Information:

- Internal and external information needed to provide safe, quality care will be obtained in accordance with the Policy for Client Records.
- All disclosure of information contained in the medical record must comply with Policy on Medical Records. Information disclosure must be documented in the client record.
- Client records in our paper-based record system need to meet the minimum requirements for information – a staff person's name must be fully spelled out, no initials, credentials must also be included. Writing must be clear and legible, and the date and time clearly indicated. Processes are in place that allow the client to release information to a third party and to define what information is released per HIPAA and 42 CFR
- Staff will respond to authorized records requests by transmitting data via secure means. When hard copies of documents are requested, secure means may include a secured portal provided through a certified HIPAA compliant application, certified mail, HIPAA compliant internal e-mail, or in-person delivery. Faxing may occur in accordance with the faxing protocol.

Interruptions to information processes:

- A fully charged backup battery able to power a minimum of one laptop and one cell phone for a period of 24 hours will be maintained on site for use in the event of a power failure.
- A wifi hotspot, powered by a 3G or 4G cell phone network will be maintained on site for use in the event of an internet failure.

- In the event of a power and/or internet failure, staff are to utilize the backup laptop connected to these devices to access electronic information systems.

In the event that the Medical Record becomes inaccessible, for any reason, i.e., access to medical records room is inaccessible, staff members are to use the following procedures:

- Staff members are to use the Word document versions of all appropriate forms saved in the Policy folder in the Egnyte Drive to document care delivery.
- The EXECUTIVE DIRECTOR has created a folder titled "For Emergency Use" within the Egnyte Drive.
- Staff members will save each document according to the following format [document type][client first name][client last initial].
- Once the Medical Record system is again accessible, each staff member is responsible for inserting the documents he/she created into the appropriate clients' charts.
- Within 48 hours, the EXECUTIVE DIRECTOR will ensure that all documents in the "For Emergency Use" folder have been uploaded. Once the EXECUTIVE DIRECTOR has verified that all documents have been saved to the appropriate client files, the "For Emergency Use" folder will be deleted.
- Basic principles of information management are discussed with the appropriate individuals during initial orientation. In-service updates are provided on an as needed basis and/or during annual performance evaluation.
- The plan for managing interruptions to electronic information systems will be tested at least annually.

Performance Improvement Information

- To allow for appropriate designing of processes that provide for systematically measuring, assessing and improving performance to improve client health outcomes, information is required that will facilitate this goal. Performance improvement is performed on an organization wide basis and requires integration of all information and data gathered throughout the facility. The following areas are key components of the information management function that integrate with organization wide performance improvement:
    - Reporting formats, aggregated data: Who requires reports, for what reason, type of information needed, security of information, timeliness of data
    - Risk Management: Organization wide
    - Safety Reporting: Organization wide
    - Performance Improvement Program:

Key aspects, clinical service groups, functions, priority focus areas and performance dimensions

- Performance measures and related outcomes
- Sentinel Event Reporting/Root Cause Analysis and Action

Tools: Ability to gather necessary data in usable format

Information-based Decision Making

- Information management activities support timely and effective decision making at all levels throughout the institution. Information management processes

support administrative, managerial and performance improvement activities (as listed above). Information management processes also support client care, treatment and service decisions. The support of clinical decision making is based on information contained in the client record. This information will be readily accessible throughout the organization, accurately recorded, complete, organized for efficient retrieval of needed data and timely. Data and information will be collected and aggregated to support care, treatment and service delivery and operations, including the following:

- Individual care and care delivery
- Decision making
- Management and operation
- Analysis of trends over time
- Performance comparisons over time within the facility and with other organizations
- Performance improvement
- Client safety

Evaluation of Information Management System:

- The EXECUTIVE DIRECTOR, or designee will conduct medical record audits in accordance with Policy on Medical Records.
- The Performance Improvement Committee will evaluate the information management system at least annually.
- As a comprehensive needs assessment is based on review and analysis of the Compass Recovery mission, goals, services, staff, client safety considerations, quality of care, treatment and services, mode of service delivery, resources, access to affordable technology and identification of barriers to effective communication among caregivers.

The following examines identified areas for consideration: Compass Recovery' scope of services

Individuals/groups served through information management:

- Client and families
- Governing Board
- Managers/leaders, both clinical and clerical
- Medical Director
- Payers/purchasers
- Accrediting agencies (Joint Commission)

Resources and support necessary for planning information and educational services:

- Time
- Space
- Staff
- Equipment
- Financial allotment

Requirements for internal and external transmission of data and information:

- Staff
- Training

- Equipment
- Mode of transmission
- Time factors

Requirements for internally and externally generated data to support facility wide performance improvement:

- Types of data required
- Confidentiality of data
- Generation of data
- Receipt of data
- Responsibility

Requirements for benchmarking with comparative facilities and current literature
Appropriateness of the technologies utilized at this facility:

- Knowledge of staff
- Capabilities of computer database
- Financial consideration
- Reporting formats

Need to support customer/supplier relationships:

- Client satisfaction surveys
- Community assessment
- Staff evaluation

Support needed for clinical and administrative decision making:

- Types of information required
- Individuals responsible for data generation, aggregation and analysis
- Equipment
- Confidentiality

The need for coordination across the organization of all elements of the information management function is considered a primary focus for staff development. Those individuals/departments identified as requiring knowledge and proficiency in the principles of information management are:

- Medical staff
- Performance Improvement staff
- Clinical service departmental staff

- Before new technology is added, an interdisciplinary team shall evaluate the ease and use of the product.

TJC Standard(s): IM 01.01.03, EP 3; IM 01.01.01; IM 01.01.03; IM 02.02.03; IM 02.01.03

Subject: **Medical Records Content Guidelines**

Purpose:
This policy serves to identify the purpose, content and guidelines for the medical records at Compass Recovery, including charting, access to records**,** and accuracy of information, timeliness, signature and privileges as well as security. All clients will have a designated, unique medical record of treatment while receiving services from Compass Recovery.

Policy:
A client record will be maintained for each client admitted to Compass Recovery through an electronic medical record, Sun Wave Health

The purpose of the medical record is to provide the following:

- Identifying client information
- Data planning for client care
- A record of care planned and provided
- A source of information for evaluation of care
- A mechanism for communication among all members of the treatment team
- A mechanism for teaching and discharge planning
- Assistance in protecting the provider's assets
- A record for utilization review and medical reimbursement

The accuracy of medical records is critical to maintaining quality care and protecting both the client and the provider. The medical record is the legal documentation of a client's course of treatment and accurately reflects the chronological order of that treatment.

Compass Recovery will grant access to clients who request their medical records, in compliance with established guidelines (i.e., written request), unless such access would be harmful to the client. If a request is initially denied, the client may make additional requests at any time.

Medical records are secured at all times to reduce the likelihood of loss or intentional destruction of documentation. Each record is kept confidential, including any financial information, in accordance with state and federal laws and requirements and the Confidentiality Policy.

Procedures:
A single record of care will be created upon admission and maintained for each client in the medical record system.

- The content of the medical record will include, but not be limited to:
- Admission date
- Client's name, sex, and client identifiers (e.g., DOB, SSN, Picture, MRN)
- Client SOGI data: sexual orientation and gender identity
- Home address/phone and emergency contact information
- Client's preferred language and any special communication needs
- Special needs to be considered during treatment, including any sensory impairments

- All allergies, particularly to food or medications
- External Provider and Referral Information:
    - Current physician and other care providers, if any
    - Any emergency care, treatment or services provided prior to arrival
    - Documentation of referrals to outside resources and any consultation reports
    - Documentation of transfers
- Required intake and pre-admission information (e.g., race, ethnic background, marital status, referral source) and criteria for admission
- Legal documents, including but not limited to:
    - Admission and Financial Responsibility Agreement
    - Informed consent for treatment
    - Informed consent for medications
    - Any consents for disclosure of information
    - If applicable, advance directives
- Results of all assessments, including the comprehensive clinical assessments
- Diagnoses, including:
    - Initial diagnosis, diagnostic impression(s) or condition(s)
    - Any diagnoses or conditions established during the course of care, treatment or services
- The initial and updated plan of care, including recommendations for psychotherapy and any updates resulting from clinical collaboration or supervision
- Information related to medical care, including:
    - Conclusions or impressions drawn from the medical history and physical and lab work
    - All physicians' orders, including medication orders, medical clearance, and any appropriate admitting orders
    - A medication list that is updated when medications are changed
    - For any clients to whom staff dispenses medications, medication administration records that are updated as new orders are received as well as on a monthly basis
    - Adverse drug reactions, as applicable
    - Any applicable laboratory/diagnostic reports
    - Documentation of significant illnesses or changes in health status
- Documentation of client teaching and education
- Plan of Care and progress in relation to plan of care, including
    - Updates and Revisions
    - All services and interventions provided to the client
    - Progress notes, including any observations relevant to care, client condition, changes in client condition and client response to care
- Contract agreements
- Discharge documentation, including:
    - Discharge orders and notice of involuntary discharge if applicable
    - Discharge summary from treatment team including discharge diagnosis
    - Discharge and follow-up care recommendations from treatment team
- Documentation of protective services
- Record of communication with individual served
- Documentation of involvement in care and his/her family
- Unusual occurrence documentation

- Resident satisfaction evaluation
- Any other information pertinent to client care
- Standardized formats will be used to document the care, treatment or services provided to individuals served in the form of assessments, forms and templates
- Progress notes must be recorded by program clinical staff in a timely manner and will be completed in accordance with timelines in policy on Client Records. The progress notes should reflect any diagnostic changes and any recommendations for revisions in the treatment plan as indicated as well as objective assessments of the client's symptom status, functional status, and progress in accordance with the original or revised plan of care.
- If notes or records in any medium are maintained for personal use by an individual providing treatment services and are available to others, these notes must become part of the treatment record.
- As medical records are considered legal documents, entries will follow the guidelines listed below:
- Entries will be made only by employees of Compass Recovery, consultants, privileged affiliated staff members and/or mental health practitioners under the direct supervision of a responsible staff member in accordance with the Clinical Collaboration and Supervision Policy.
- Entries will be legible, factual, accurate, and permanently recorded.
- Entries will be signed by the person making the entry, with that person's full name and credentials. For any hand-written entries, there should be no space between the entry and the signature/credentials, with a single line drawn out from the signature to the end of the margin.
- Entries by student interns will be reviewed and co-signed by the assigned preceptor.
- Entries will be completed within 24 hours of service provision, including date and time of each entry.
- Discharge summaries must be complete, signed and entered into the client's chart in accordance with the discharge policy. Interdisciplinary discharge summaries will be completed if the treatment team has met at least one time, no matter what type of discharge the client had (e.g., AMA, irregular). If a client has **not** had a treatment team meeting, the primary therapist assigned to the client will write a note describing the discharge circumstances.
- Handwritten entries will be made in ink only – entries will never be made in pencil or corrected with any type of correction fluid or tape.
- Handwritten entries made in error will be corrected by drawing one single line through the mistake and initialing and dating the error.
- If a session is not documented within 24 hours, it is considered a "late entry". Documentation of the session should be completed as soon as possible thereafter. Late entries must be identified as such, using the words "late entry". They must include the date and time of the late note, as well as the actual date/time of the session.
- Entries will use only approved abbreviations.
- Entries will not skip lines – if so, the unused line will be voided with a single line through the space, thus prohibiting the creation after the fact, alteration or falsification of the original entry.

- Client identification information must appear on every record page, to include name, DOB and MRN.

Transmission of medical record or information contained within will be done at the request of the client or the client's legal representative. Transmission of medical records to other providers will occur when the information is needed to ensure the continued medical care of the client, maintaining data integrity at all times. There will be proper authorization from the client with the "Authorization for Disclosure" form. Any transmission of medical records or disclosure of client information must be documented in the client's record of care. Faxing information will follow the guidelines listed to maintain confidentiality and security of information:

- There should be an immediate need for the information that cannot be satisfied by more secure methods (e.g. post-office mailing).
- Prior to faxing, make sure the requesting party is available to receive the transmission.
- Once the information is sent, have the party call and verify that the records were received.
- All faxed records must be accompanied by a cover sheet stating that the transmittal is confidential, and the receiving party is prohibited from disclosing the information to any unauthorized person(s).
- Once the record is faxed, the transmission record is filed with the correspondence section of the medical record.
- If staff is informed that the information was misdirected an incident report must be completed.
- If multiple members of the same family are in treatment as a unit, records for individual family members will be maintained separately and will not be maintained in composite client files.
- Active medical records will be kept confidential and maintained in a secure manner in a designated place. Access to the records will be restricted to providers who have clinical care responsibilities and a need to know the information contained therein. Entries into the medical records will be made in a private area where bystanders cannot easily view the information being recorded. If the individual making an entry in the record must leave the record while making an entry, that individual will be responsible for ensuring that the record is not available to unauthorized personnel during that individual's absence.
- Upon termination of a staff member, any records for which that staff member had responsibility will remain in the custody of Compass Recovery.
- 10% of active medical records will have an administrative review to check for accuracy and appropriateness of documentation. Treatment plans for clients currently under the care of Compass Recovery will be reviewed by clinical staff members for content and completeness during weekly treatment team meetings. All completed records will be reviewed at the time of discharge for both clinical and administrative content. This will ensure quality, completeness, content, timeliness and clarity. There will be an assessment of aggregate findings from administrative reviews, at least quarterly, which will be reported at a PI Committee meeting. Recommendations and corrective actions based on data collected will be reported and if necessary, appropriate staff training will be used to remedy negative findings.

- Should an employee be terminated or resign, access to the Medical Record will be terminated on the employee's last day of employment with Compass Recovery.
- An individual client has the right to access, inspect and obtain a copy of his or her protected health information for as long as that designated record set is maintained by the facility, however the request must be in writing. Access to records while the client is still receiving treatment at the facility will be assessed on an individual basis and may be denied if such access would compromise treatment (i.e. detrimental to the client's health) or it would present a threat of physical harm to a third party. Access will be accorded within 30 days of the written request, except when legally specified reasons for denial exist. When a client requests a copy of his or her medical records the following guidelines will be followed:
- A written request will be submitted (HIPAA-2).
- The request will be reviewed by the appropriate staff and the Clinical Director.
- If approved, a fee for copying/printing will be charged as well as postage and handling in accordance with the most current federal and state regulations.
- If access is denied for cause, such denial will be given in writing, stating the reason for the denial. The client has the right to submit a statement of disagreement and to file a complaint with Compass Recovery or with the regulatory body responsible for Compass Recovery 's licensure status. Once the records have been reviewed, the client has the right to request an amendment of his or her health information. A "Request for Amendment of Health Information" must be submitted in writing for appropriate action to take place (HIPAA-3). A written response will be given to the client in cases of either approval or denial of the request. If denied, the client has the right to submit a statement of disagreement and to file a complaint with Compass Recovery or with the appropriate regulatory body.
- Compass Recovery shall take reasonable precautions to ensure that all records containing health information are secured against loss, destruction, unauthorized access, unauthorized reproduction, corruption and damage in accordance with the HIPAA Security Regulations.

TJC Standard(s): IM.01.01.01, EP 1; RC.01.01.01; RC.01.02.01; RC.01.04.01; RC.01.05.01; RC.01.03.01; RC.02.03.01