Recovery Technology

Technology Plan 2014

Information Services Department

Technology Plan:

Introduction: Recovery Technology is a growing organization in Jackson, Michigan. Recovery Technology's current strategic plan and business operational needs dictate that the information Technology Department keep pace with the organization's current IT configuration and processes as well as detail a plan for the growth of IT capabilities in order to support the organization's strategic plan.

Information Technology Department Description and Policies: Recovery Technology's IT Department is under the direction and supervision of the agency's Chief Executive Officer. The department is comprised of one contractual Specialist in Information Technology who has a BBA degree, Major: Computer Information Systems and is experienced in both traditional and emerging cloud-based technologies. This Specialist is required to support the full scope of IT department functions from hands on Desktop support to Administrative duties.

Information Confidentiality: Recovery Technology maintains confidential, protected health information regarding its consumers, some of which is maintained electronically. Recovery Technology also maintains proprietary business information that must be protected from unauthorized and/or unlawful access. All electronic documents or files containing confidential treatment or administrative information that are created, maintained, modified, updated or copied using a Recovery Technology computer and/or server must be stored in a location that is secure from unauthorized access.

Confidential information is defined as a) Electronic Protected Health Information (EPHI): electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. Individually identifiable information refers to any coding or descriptive information by which there is a reasonable basis to believe that the information can be used to identify the

individual or by which the individual has been identified in the past. This includes but is not limited to: a person's name (including initials), customer number, address (including zip code), nickname by which the person may be called or commonly known, physical description, description of a particular physical and/or behavioral characteristic, condition, or diagnosis; b) any medical and/or behavioral health information that may be maintained by the company regarding any of its employees or contract workers is considered EPHI; c) Proprietary Business Information (PBI): Information contained in: employee records, contract information and files, company form data, financial data, strategic planning information, company policies and procedures.

Any electronic transmission of confidential information must be protected against unauthorized or unlawful access during the transmission process. This may be accomplished by the encryption at the security level specified within the HIPAA standards and/or utilization of a standardized electronic transfer format specified within the HIPAA standards. Confidential Electronic Information may not be removed from company property on portable computers or any removable media unless they are stored in a double password protected and/or encrypted folder or volume. Removable media is defined as: any media or device that is not internal to company PC that is capable of storing electronic files and information that can be connected to or inserted into another computer that will allow access to the data stored on that device. This includes but is not limited to: a) Externally attached hard drives, b) Floppy disks, c) CD-R/RW and DVD-R/RW media, d) Flash Memory devices.

All employees and contract workers are granted clearance to view and edit confidential electronic information based upon their job functions within the following matrix:

Job Function	*View Confidential Admin. Info.*	*Edit Confidential Admin Info.*	*Transmit Confidential Admin Info.*	*View Confidential Treatment Info.*	*Edit Confidential Treatment Info.*	*Transmit Confidential Admin. Info.*
IT Department Staff	X	P	X	X		X
Leadership: Program Directors	X	X	X	X	X	X
Leadership: Admin	X	X	X	X		P
CEO	X	X	X	X	X	X
Admin Assistant	X		P	X		P
Non-Leadership Admin	X		P	P		P
Other Support	X			P		

Matrix Key: X = Clearance Granted; P = Clearance Granted with Program Director or COO Approval

Recovery Technology staff/contract workers may not transmit or otherwise remove confidential information from a Recovery Technology Computer and/or server unless: a) it is within the scope of their job function to do so, b) The staff/contract worker has the appropriate clearance level to do so, c) Authorization to do so has been granted by the responsible program director.

It is the responsibility of information Services Department to provide all Recovery Technology employees access to an encryption utility to create an encrypted, password protected folder or volume on the hard drive of their desktop or mobile computer or on removable media in which confidential electronic information files can be stored. Further it is the responsibility of Information Services Department to instruct Recovery Technology Employees as to installation and proper use of the encryption utility.

Storage: Confidential electronic information is to be stored by all users with registered domain accounts in a secure location. Documents and files are to be stored in a user's "My Documents" folder, which is automatically re-directed to the Corporate File Server. These folders may only be accessible from password protected User accounts either via the Corporate LAN or by secured Terminal Services login from remote locations. Employees may not store confidential electronic information in their personal computers. Contract workers may store confidential electronic information in their personal or business computers only after the execution of a) a contract with Recovery Technology which delineates the scope of work which will be performed for recovery Technology and b) a Business Associate Agreement which delineates the contract worker's responsibilities regarding the access, use, storage, and destruction of the confidential electronic information they may obtain in the course of performing the contracted functions.

System Security: All access to electronic records maintained by Recovery Technology is restricted by use of strong passwords. All use of company IT resources on the local area network (LAN) and the wide area network (WAN) is also restricted by use of strong passwords.

Company IT resources include, but are not limited to: a) Company owned Computers and all data and files stored on them, b) Company owned Removable Devices and all data and files stored on them, c) Networked Public or private folders on the Company Servers and all data and files stored on them, d) Company owned PDA's and phones and all data and files stored on them, e) All email and contact information on the Company Exchange Server and/or transmitted across Company Network Infrastructure, f) All Internet usage via Company Network Infrastructure, g) All Instant Messaging transmitted across Company Network Infrastructure.

All company owned computers, whether they are logging into domain accounts or local PC accounts are secured from unauthorized access in the following manner:

A. Computers from which it is possible to access confidential consumer or business information are located within a secure location, with at least one

locking door between the computer's location and public areas of the facility.

B. Computers from which it is possible to access confidential consumer or business information are configured with the requirement of a strong password upon startup of the PC and also upon exiting the screen saver on a running PC.
C. Remote access to Company IT Resources shall be granted only to registered Domain Users on the discretion of the Information Services Staff. All access will be protected by strong passwords.

While Recovery Technology IT Department personnel seek to provide a reasonable level of privacy to users of company IT resources, all persons utilizing the system/accessing records on the system must be aware that all data or files created or stored on the Recovery Technology system are the intellectual property of Recovery Technology. The single exception to this standard is any and all electronic information concerning consumers and their treatment, which is adjunct to their medical record and, therefore, the property of the consumer him/herself. Electronic information concerning consumers and their treatment belongs to the consumer, however Recovery Technology maintains custody of this information and, therefore, the security standards included in this policy and procedure are in full effect.

Failure to adhere to this policy and procedure, inappropriate use of company IT resources, and/or actions that place the security of Recovery Technology IT resources and/or electronic records may result in: a) Revocation of access privileges, b) Possible disciplinary/contract action up to and including termination of employment/contract.

Inappropriate use of company IT resources include:

A. Access and/or viewing of consumer records without a need to know for business, payment, or treatment purposes;
B. Access and/or viewing for personal gain
C. Access and/or viewing for reasons that are counter to the best interests of Recovery Technology and/or its consumers.

Upon separation of employment/termination of contract with Recovery Technology, the IT Department personnel must be notified immediately to ensure that the individual's access to IT resources is immediately disabled. The IT Department must be notified regardless of the reason for the employee's/contract worker's separation from Recovery Technology. In the event that access to IT resources is not immediately disabled, access to IT resources by a former employee/contractor is unlawful and subject to legal action.

System Backup: All Recovery Technology servers are automatically backed up every weeknight. Backups include: a) system volume information, b) system state data, c) application data, d) exchange mailboxes, e) the content of all user folders. Backups are stored at a secure data center.

Disaster Recovery: It is the responsibility of the Information Services Department to implement and maintain the following measures to protect against catastrophic loss of data: redundant backups in more than one location.

Summary of Current Technology and Spending: When the Information Services Department was started; Recovery Technology had a small handful of Desktop Computers. Currently we have expanded to laptop computers for all case managers, ACT advocates and other clinical staff. The Majority of staff that provide Case Management, Outpatient therapy and ACT services are better able to provide those services with the help of our primary "Practice Application"; Genius Solutions eThomas-which provides a business critical interface for both scheduling and billing for the consumers we serve.

As a startup company, it was sensible for Recovery Technology to spend very conservatively on its Information Technology needs. However, as growth continues, it has become imperative that we focus our attention on a number of

areas listed below that will be critical toward achieving and sustaining our Strategic Plan and growth.

1. Computer Hardware: Recovery Technology will continue to purchase laptops for new staff in order for staff to access the Electronic Medical Record.
2. Software and Licensing: As we move to acquire new Computer Hardware, we will be buying computers that come with more up-to-date versions of software or linking staff to Recovery Technology's Remote Server which allows access to current software.
3. Network Infrastructure: LAN with high-speed WAN connection, wireless access point, three primary network printers and supporting switches.
4. Disaster Recovery: Experience has revealed that the most common threat we face on a daily basis is the loss of our connectivity to the Internet. When we lose access to the Internet and to our Scheduling and Billing Application and email, this leaves us "dead in the water" and severely impacts our ability to function. This results in a very unfavorable situation for our staff and our consumers. We must formulate a plan that will allow us to diversify our connections to the Internet to include different types of Service Providers to keep us connected to the Internet.
5. Remote Support: Remote monitoring and management technology is at the beginning stages of implementation and will continue across the entire network.

Electronic Medical Record Implementation:

During the end of 2011, LifeWays CMH whom Recovery Technology contracts with to provide an array of services implemented "LifeWays Electronic Organizer" or LEO. "Phase One" of LEO went into effect October 1, 2011. "Phase Two" of LEO began in April of 2012. At this time, LEO is fully functioning. Authorization for services and billing are currently being completed in LEO. During Phase Two, all LifeWays consumers being seen by Recovery Technology now have their medical records in the system. This includes Assessments, Treatment Plans,

Progress notes, and Quarterly Status Reports. Other documents such as hospital information are scanned into the LEO system. Recovery Technology will have challenges related to maintaining both Electronic Medical Records for CMH consumers, and traditional medical records for our private, third party consumers.

Recovery Technology also launched its own website in January of 2013. This website includes electronic versions of all forms that are used by Recovery Technology staff. The website is currently fully functioning and being used by staff. It is continually being updated to meet the needs of our staff and other stakeholders. The website also includes reports and other information that is of interest to our staff and stakeholders. There is also a section on the website for staff only to be able to access policies and procedures as well as surveys and other information applicable to staff.