Avysion Healthcare Services

Information Management

Version 1.1

January 12, 2009

Revision History

Revision	Date	Notes
1.0	11/1308	Initial Draft
1.1	1/12/09	Preparation for Coventry Credentialing Project

Table of Contents

Background & Purpose

Ăvysion Healthcare Services has been entrusted by customers with protected health information to provide services to them, their clients and participants. Ăvysion Healthcare Services will make certain that the privacy, integrity and confidentiality of this confidential information is protected. This information must be handled, stored, maintained and if destruction is required, destroyed in the proper manner

Ăvysion Healthcare Services is committed to remaining in business even in the event of a disaster or extend interruption. It is for this reason Ăvysion Healthcare Services has taken the time to develop a practiced logistical plan as to how recovery and restoration of partially or completely interrupted critical functions will occur within a predetermined amount of time.

1.0 Physical Access

Purpose: It is the intent of this policy to describe the manner in which access to the facility and secure areas are granted.

Policy: Physical Access to the facility is controlled with keys and an alarm code assigned by management and controlled by the Facilities Manager. The server (IT) center and secure file room are also controlled by individual pass coded entry pads.

Procedure: Physical Access privileges will be granted by management and documented appropriately.

Facility Access:

- Access to the facility is obtained with a key and alarm code.
    - When a key and code are issued, paper work must be signed to track individuals with access.
- Access to the IT center is granted strictly on a need to know basis, the individuals with access to the IT center are the Facilities Manager, the Chief Executive Officer, the Chief Technology Officer and Operations Director.
- Access to the secure file room is granted strictly on a need to know basis, the individuals with access to this room are the Facilities Manager, the Chief Executive Officer, the Operations Director, the Credentialing Specialist and the Quality Management Specialist.

2.0 Data Integrity

Purpose: It is the intent of this policy to describe the manner in which trace-ability and accuracy of records will be ensured and maintained.

Policy: Ăvysion Healthcare Services is committed to maintaining the integrity of the data in its possession. Ăvysion Healthcare Services will complete the steps necessary to ensure that accuracy and trace-ability of documentation, both paper and electronic is maintained.

Procedure: Some examples of promoting data integrity are as follows:

- monitoring data entry personnel for accuracy
- cross-checking databases for consistency
- utilizing unique identifiers for client or recipient information
- Prevention of and checking for duplicate entries.

3.0 Data Confidentiality and Security

Purpose: It is the purpose of this policy to briefly review the methods in place for maintaining data confidentiality and security

Policy: All copies of protected health information electronic and paper can only be stored and disposed of by approved means.

Procedure: It is the responsibility of management to make certain that the appropriate means of storage are readily available and operational.

All workstations are required to have the appropriate lockdown mechanism activated to protect confidential information.

All confidential information relevant to personnel, clients and recipients will be maintained in a secure location. The information will be contained in securely locked filing cabinets in a location that will be protected with a pass coded security system.

Ăvysion Healthcare Services employees and medical resources will follow confidentiality guidelines to make certain that confidential data is physically protected to prevent the inappropriate use and disclosure of confidential and protected health information.

"Appropriate safeguards" to be utilized by Ăvysion Healthcare Services and their employees and medical resources in order to protect PHI and confidential information will include, but are not restricted to, the following:

- Technology specific logins and passwords
- Shredding documents containing all confidential information
- Secure removal and destruction of electronic data
- Secure storage of all hardcopies of confidential documents
- Confidentiality disclosure on all e-mail
- Confidentiality statements printed materials such as faxes and reports
- Privacy and Security Training
- Documented Privacy Policies and Procedures
- Documented Disaster Recovery Plans, Business Continuity Plans, Data Security Plans, Emergency Back-up and Recovery Plans.
- Confidentiality language in each employee's "Employment Agreement"

.

4.0 Collection, Transmission and Maintenance of Paper Information

Purpose: It is the intent of this policy to describe the policies and procedures for proper handling of paper or hardcopy information.

Policy: Ăvysion Healthcare Services requires employees to handle and store hardcopy documents containing protected health information and other confidential information in a way that would limit access to the information.

Procedure: Management will ensure that employees are outfitted with the proper knowledge and tools to make certain that the confidentiality of information is maintained. For example:

Faxing Confidential Information

- Assure that faxing is necessary and appropriate as opposed to any other means of transmission.
- Management approval is required for the faxing of sensitive health information. Examples: information pertaining to mental health, chemical dependency, sexually transmitted diseases or HIV.
- Use of proper cover sheets that contain the following information:
    - Date and time of transmittal
    - Sender's name, address, telephone and fax numbers
    - Number of pages transmitted
    - Authorized recipients name
    - Notice of confidentiality statement
    - Ăvysion Healthcare Services Logo
    - Confidentiality Notice:
    -

      Confidentiality Notice: The information contained in this fax transmission is confidential, proprietary or privileged and may be subject to protection under the law, including the Health Insurance Portability and Accountability Act (HIPAA).

      The information is intended only for the use of the individual to whom it is addressed. If you are not the intended recipient, you are notified that any use, distribution or copying of the information is strictly prohibited and may subject you to criminal or civil penalties. If you received this transmission in error, please contact the sender immediately by calling Ăvysion Healthcare Services at 717-939-6500 for further instructions.

- Misdirected Faxes should be immediately returned to the sender or destroyed by the recipient. See that the appropriate precautions are taking to avoid misdirection in the future.
- In the instance that a confidential document is found unattended at a fax machine, be sure to deliver it to the intended recipient.
- Faxed documents are to be stored in a secure place and shredded when no longer needed.
- The fax machine is to be located in a low traffic area when possible and the logging/ auditing feature should be activated to allow for accountability for the management of the fax machine and related documents.
    - Safeguards to avoid inappropriate disclosures of confidential protected health information.

        - Confirmation of fax number
        - Verification upon receipt of faxed information
        - A cover sheet is required for all incoming faxes to prevent staff from viewing the contents
            - If materials should arrive without a cover sheet, a blank sheet should be placed on the fax and then it is to be routed to the intended recipient
- Fax numbers should be verified with the party that is to receive the intended information.
- Fax machines should be place in "sleep mode" after business hours.

Mailing Confidential Information

- The address of the intended recipient is to be verified prior to the protected health information being sent.
- If any electronic media may be contained in a package to be mailed the electronic media must be encrypted.
- Packages containing protected health information must be sent utilizing services such as DHL, UPS or other mail systems with tracking abilities.

Maintenance/Storage of Paper Data

- All confidential information will be stored in filing cabinets that must be securely locked, with keys in a secure place other than in the lock on cabinet.
- Filing cabinets containing confidential information will be located in a securely locked room, requiring a password for entry.

Proper Disposal of Paper Information

All hard copy confidential data must be disposed of properly in the appropriate trash bins and shredders.

The following standards must be followed when disposing of protected health information.

- Any paper or hardcopy items containing any remotely identifying information must be shredded prior to disposal.
    - Shredders are located in most work areas or common areas.
- All Ăvysion Healthcare Services employees are responsible for making certain that all protected health information is disposed of in the correct manner. Management will be responsible for ensuring that all employees adhere to this policy and have access to appropriate confidential trash bins and shredders.

End of Day Procedures

- All desktops are to be cleared of confidential and protected health information.
- Medical records and confidential informaiton are to be stored in a locked file cabinet or secure desk area.
- All file cabinets with a locking capability must be locked and key properly secured.

5.0 Collection, Transmission and Maintenance of Electronic Information

Purpose: It is the intent of this policy to describe the policies and procedures for proper handling of electronic information.

Policy: Ăvysion Healthcare Services values the confidentiality of stored data on its workstations and networks. It is for this reason; substantial resources are dedicated to the protection and safeguarding of this information. All necessary technical safeguards to prevent the use and disclosure of electronic protected health information and other electronic confidential information will be utilized all situations.

Procedure: All appropriate communication channels will be utilized with necessary safeguards in place when sending confidential and protected health information to external entities. Acceptable methods of access controls will be utilized to transmit electronic confidential and protected health information.

For example:

Workstation Security

Examples of electronic information include but are not limited to:

- Application data
- Licensed software
- Licensing keys
- Passwords
- Email
- Other confidential information

When leaving a workstation unattended, locking the station will help prevent unauthorized access to stored information on the workstation or networks accessed through the workstation.

Employees will fulfill this obligation of safeguarding electronic protected health information and all other confidential informaiton in one or both of the following manners:

- Workstations that utilize a manual lockdown feature, the appropriate feature should be activated when leaving the work area. (Most secure and preferred method)
    - For example on a Windows XP Machine this function is activate by Pressing Ctrl+Alt+Del all simultaneously.
- Workstations that utilize a screensaver that is password protected should have the appropriate feature to activate following 10 minutes of inactivity.
    - This feature can be activated by right clicking on the desktop and accessing the Properties menu.

For workstations other than those listed above such please contact IT support for guidance for the appropriate lockdown procedure.

Any information system that houses confidential medical resource information must abide by the following:

- Access to the systems is granted on a need-to-know basis
- Users must utilize strong passwords that must be changed every 90 days
- The information system will not be externally accessible unless all connections are utilizing the appropriate encryption safeguards.

Transmission of Electronic Information

- It is the duty of management to make certain that Ăvysion Healthcare Services employees are familiar with the policies and procedures regarding secure messaging as it relates to email transmission of protected health information.
- If an employee receives an email containing protected health information that has not been encrypted they are to respond with the following message:
- Electronic protected health information may be exchanged with entities in the following ways:
    - Electronic media that is encrypted and sent via mail utilizing a delivery services with tracking abilities
    - All protected health information should be sent in encrypted form via and attachment.
- Outgoing email must contain a confidentiality notice.

> *CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential information for the use of the named addressee. If you are not the intended recipient, please notify us immediately by replying to this e-mail or by telephone at 717-939-6500 and deleting this e-mail.*

- As a result of the insecurity of portable hand held communication devices such as mobile phones and PDAs, text messaging of confidential and protected health information is prohibited.

Proper Disposal of Electronic Information

All electronic copy confidential data must be disposed of properly.

- All hard drives will be sanitized, however, in the event that sanitization is not feasible, the hard drive will be physically destroyed.
- All optical media and removable storage devices, such as thumb drives, flash media and external hard drives will be appropriately destroyed, prior to disposal.

All Ăvysion Healthcare Services employees are responsible for making certain that all confidential and protected health information is disposed of in the correct manner.

6.0 Verbal Communications

Purpose

This policy provides the procedures for handling verbal communications that may exchange Confidential or Protected Health Information.

Policy

Confidential and Protected Health Information will be discussed with other parties only if it is specified by a contract and will only be on a "need to know" basis, furthermore, when discussing confidential information or any kind, make certain the individual receiving the information is authorized to do so.

Procedure

- If contracts that do not include a stipulation regarding verbal communications with individuals, Ăvysion Healthcare Services employees will be required to refer the individual to the provider to discuss medical information.
- When contracts do involve verbal communications with clients, recipients or representatives, Ăvysion Healthcare Employees must follow procedures approved by the customer when handling telephone calls.
- Employees are to verify the identity and/or legal authority of the individuals requesting the information.
- All acceptable forms of identification will be defined by each contract on a per contract basis.
- If the representative of an individual is making the inquiry, verification must be made of the representative's authority to make such a request.
- Management is responsible for making certain that procedures to handle telephone communications from clients, participants and representatives are developed as deemed necessary. .

7.0 Offsite and Remote Access

Purpose:

The intent of this policy is to describe the procedures for safeguarding Protected Health Information and all other confidential information for medical resources that have offsite or remote access to such information.

Policy:

Medical Resources are expected to be responsible users of computer equipment. Medical Resources are expected to take reasonable steps properly safeguard Protected Health Information and other Confidential Information.

- Offsite and remote access of Ăvysion Healthcare computer systems must be approved by management. The manner in which access is obtained will be configured to provide secure access.
- Privileged access controls established by Ăvysion Healthcare Services will be used in instances where the internal network must be accessed from outside of its defined network perimeters
- Medical Resources utilizing personal computers for remote or offsite access to company information and internal networks are responsible for utilizing security precautions to prevent the infiltration of computer viruses and internet threats of Ăvysion Healthcare Services data and network.
- All policies set forth in this section apply not only to company issued property but also to personally owned devices being utilized for work related functions or containing work related data, the procedures also apply:

Procedure:

Appropriate safeguards must be employed to protect the physical security and confidentiality of protected health information and related confidential data.

- Make certain that all individuals with remote or offsite access to Ăvysion Healthcare Services systems and applications understand their obligations associated with such access.
- Establish appropriate security requirements for remote or offsite access of Ăvysion Healthcare Services computing resources.

Examples of appropriate safeguards:

- Protect materials by placing them in closed briefcase, file folder or envelopes
- When performing field work at various locations, utilize a separate folder for each location.
- When working from a home office, be certain that confidential materials are securely stored and remain confidential from unauthorized users. This includes work-related files that may be contained on a personal computer. All electronic protected health information should be kept in password protected files.
- Any confidential data that may be downloaded from Ăvysion Healthcare Services to a home computer should be protected at all times.
- If hardcopy documents are printed at home please employ the same policies as specified in *Policy 4.0 Collection, Transmission and Maintenance of Paper Information*

.

Ăvysion Healthcare Services Workstations

- Installation of unauthorized software on a workstation owned by Ăvysion Healthcare Services is strictly prohibited.
- Any software that is required for end-user purposes must be approved and installed by the Information Technology Team at Ăvysion Healthcare Services. Management will assist in arranging the appropriate installation.
- All workstations must utilize physical safeguards to minimize or eliminate unauthorized access or theft of equipment.
    - Workstations will be placed out of public view and the view of other employees when possible
    - If workstations can not be protected from public view, other precautions will be taken to avoid unauthorized use or disclosure.
- Based on availability of safeguards, workstations and portable computing devices will be protected from exposure to threats including theft.
- Workstations will all be equipped with appropriate security measures to detect and prevent the presence of computer viruses and other related issues.
    - Security measures in the form of software will be updated as necessary.
- Any situations of non-compliance with this policy will be reviewed by management. Corrective action will be taken accordingly and could result in potential termination of employment, vendor contract and or legal action.

Electronic Devices

- The theft of any digital device containing confidential information shall be reported immediately to management.
    - Management will contact the appropriate party in the Information Technology Department.
    - Passwords for authentication and authorization are required on all digital devices containing confidential information. Passwords are required whether or not the device in question is owned by Ăvysion Healthcare Services.
    - Passwords and user IDs should not be stored on electronic devices.
    - Electronic devices containing confidential protected health information belonging to employees may not be shared with unauthorized users, unless the information in question is encrypted and stored in a password protected file.
- If a user feels as though a higher level of security may be required for the information contained on the personal computing device, the Information Technology team at Ăvysion Healthcare Services must be notified.
- Ăvysion Healthcare Services will determine what information is especially sensitive and will employ appropriate security measures to protect that information.
- Any situations of non-compliance with this policy will be reviewed by management. Corrective action will be taken accordingly and could result in potential termination of employment, vendor contract and or legal action.

Computer Resources and Data Security

Ăvysion Healthcare Services medical resources are responsible for maintaining the physical security of computer resources under their control and maintaining the protection and integrity of protected health information contained on those resources. Employees are to utilize the appropriate safeguards including, lockdown devices, password controlled access, encryption of sensitive data, anti virus software and regular back-up procedures.

- Ăvysion Healthcare Services has the right to inspect all data and monitor the use of company owned computer systems.
- Ăvysion Healthcare Services has the right to monitor, control, and access and configure any workstations and the software contained on them.
    - Any situations of non-compliance with this policy will be reviewed by management. Corrective action will be taken accordingly and could result in potential termination of employment, vendor contract or legal action.
- Remote workstations with multiple users and fixed storage that contains or process confidential protected health information, including modems, must be outfitted with appropriate hardware security and access restrictions.
- Workstations should be kept out of plain view when possible, in all other situations a property security measures will be taken.
- Appropriate security safeguards are to be employed when accessing the network or information from remote or offsite locations
- All Ăvysion Healthcare employees must adhere to the appropriate policies regarding the acquisition of software or commercial software licenses.

Taking work offsite must be approved by management

Term	Definition
Device	• Any workstation, laptop, home/personal computer, or mechanism used to directly or remotely access the network • Company issued portable hand held devices granted access to the company email system. • Company email will not be permitted on a device that is not owned by Ăvysion Healthcare Services.
Portable computing device	A computing device that is easily transported by hand.
Portable storage devices and media	Devices such as CDs, zip disks, DVDs and CD –RW drives that have the ability to store patient or business information.
Workstation	A terminal or personal computer that can store patient information, business information, access IT resources such as the Ăvysion Healthcare Services network and the Internet

.

8.0 Disaster Recovery

Purpose: It is the intent of this policy to describe the procedures for information recovery in the event of a disaster or extended interruption.

Policy: Ăvysion Healthcare Services is committed to remaining in business even in the event of a disaster or extend interruption. It is for this reason Ăvysion Healthcare Services has taken the time to develop a practiced logistical plan as to how recovery and restoration of partially or completely interrupted critical functions will occur within a predetermined amount of time.

Procedure: Ăvysion Healthcare Services has procedures in place for both business continuity and disaster recovery. Both procedures for Business Continuity Planning and Disaster Recovery Plans are regularly tested bi-annually.

Business Continuity Planning

Ăvysion Healthcare Services utilizes a remote back-up service for backing up information stored on our network shares, end-user computers and servers and (Including: payroll and employee specific, contractual and professional review information.)

- Retrieve files from the files back-up stored off site.
- Phone company will begin to re-establish communications.
- No more than one to three days to fully recover land lines.
- Utilize cell phones to contact employees and customers.
- Communication system for staff to contact their employees and customers.
- Could be a home or rental office.
- Re-direct mail and express deliveries to the temporary address.
- Utilize computer support from staff with laptops, home computers, rental agencies, etc,

Disaster Recovery Process

- Buy new equipment (hardware) or repair or remove viruses, etc.
- Call software provider and reinstall software
- Retrieve offsite storage discs
- Reinstall all data from back-up source
- Re-enter data from the previous week