

HIPAA SECURITY  
The Safeguarding of  
Electronic Protected Health Information - ePHI



**A Self Awareness Training Manual  
for Elim Park Computer Users**

# Hipaa: Whose responsibility?

- All Employees of Elim Park are responsible for securing the privacy and confidentiality of personal health Information relating to our Elim Park resident family.
- Employees who utilize information systems containing electronic Protected Health Information (ePHI) have additional responsibilities as noted herein.
- *(The Computer User employee must acknowledge receipt and self-study of this document by certifying to the Information Security Officer within one week of receipt, the final page of this presentation signed by the user.)*

# Sources of Hipaa Security Information

- **Hipaa Policies are stored in several locations as follows:**
  - **A) Information Systems Office (lower level)**
  - **B) Privacy Officers office**
  - **C) Director of Nurses**
  - **D) Chief Financial Officers Office**

# Means of Communication of Policies

**Elim Park uses the following for training purposes:**

- **Self Study (this document)**
- **Group training Sessions as needed**
- **Email communications as needed**
- **One on One as needed**

# Overview of Responsibilities

- **Security is everyone's responsibility**
- **Elim Park is mandated by the Government to protect the Health Information of those we serve at Elim Park, handling such Information in a “professional and caring and secure manner”.**
- **Protected Health Information (PHI) comes in various forms including (Verbal, paper, electronic)**

# Use of Information Systems

- **Employees must use Information systems for the conduction of Elim Park's business only.**
- **All information, data and files stored in the system are the sole property of Elim Park and must be protected according to established policies and practice.**
- **Abuse or unacceptable/inappropriate use of systems, and/or violations of security relative to PHI can result in disciplinary action up to and including possible termination, and/or criminal prosecution under the law.**

# Placement of Information Systems

- Computers screens must be positioned in a manner that precludes viewing from a public way.
- Printers, fax machines and other electronic devices must have at least one physical barrier to the public way.



# Computer Users

## Electronic ID policies

- **Each computer user will have a unique Username, and Password to authenticate to the network system.**
- **Depending upon Role, the user may be assigned a secondary Username and Password for access to particular health care programs and databases.**
- **In most cases, a user has custody of one machine. In some cases, many users will access one machine using the same Username and Password, In all cases, unique Username and Passwords will be required for medical programs specific to each user.**

# Computer Use Policies Cont'd

- **Users will be allowed 5 opportunities to log on to the network. Failure will result in a “lockout” period of 5 minutes.**
- **Network Passwords are good for 180 days after which an automatic message will inform the user to create a new password. (Passwords cannot be re-used until the third cycle of change)**
- **Passwords must be a minimum of 7 characters in length, be composed of three of the following 4 characters, with no character being used twice sequentially.**
  - **Upper case; lower case; numbers, or characters.**
  - **(The System will not accept passwords not meeting this criteria**

# Computer Use Cont'd

- Passwords may not include words found in an English dictionary, and shall not be shared.
- In addition, the words “Elim Park”, or ones “user name” cannot be used as a password. Examples of non-acceptable passwords: Elim12\*park; JAnderson#1; Mydogspot5; Dogspot##
- Passwords shall not be stored under keyboards, in desk drawers, or on monitors for others to see. If written, they must be placed in wallets or purses, and the password shall not be accompanied by any words such as “Elim Park Password”

# Computer Use – Cont'd

- **Desktop computers will “lock” after 15 minutes of activity, and default to a “screen saver” provided by Elim Park. Password must be re-entered to unlock the workstation.**
- **Data files created via Microsoft Office must be stored on the main servers. (Set to default to the file and print server). No ePHI data created shall be stored on the local computer.**

# Computer Use – cont'd

- **No data shall be placed on Floppy disks, Memory sticks, CD roms, or other non-authorized forms of backup.**
- **No “shadow” copies of ePHI are permitted, and no PHI data (paper or electronic) shall be removed outside the facility for any reason. (Special exceptions are allowed only with the approval of the PO and ISSO.)**
- **No installation of personal programs, or data is allowed, and no files of any kind shall be downloaded from the Internet without express permission of the ISSO.**

# Computer Use – Cont'd

- **Use of Modems:**

**Modems are used on certain Computers to transmit data from the facility to Vendors authorized to send and receive data into our network.**

**Modem users are required to place the Modems in the “off” position when not accessing or receiving data from a remote machine. A log sheet of “modem usage” is provided and required of all machines using modems.**

# Computer Use – Cont'd

- **Use of Modems – cont'd**
- **PcAnywhere is an authorized “dial-in” program which allows remote access trouble-shooting of vendor software as needed.**
- **A username and password is supplied to the vendor which authorizes the remote access. (See the ISSO if remote access is required)**

# Computer Use – Cont'd

- **Use of Email.**

- **Elim Park provides email for business use. Occasional personal use is permitted but shall not be abused.**
- **Email content shall be respectful, courteous, and otherwise proper at all times.**
- **Local Address Distribution lists are permitted to provide PHI to persons with “need to know”, but must be periodically pruned to protect the dissemination of PHI**
- **Non-business bulk email shall not be forwarded.**

# Computer use – Cont'd

- **Email cont'd**

- **Delete suspicious email when: the sender is not familiar to you, the email has attachments, and or has a message instructing the user to take action by deleting files, or sending the email to persons in your address book.**
- **Delete suspicious email from your “delete box” as well.**

**(Note: Email is scanned for Viruses before coming to the users mail box. The “delete” procedure is to err on the side of caution.)**

# Computer use – Cont'd

- **Email cont'd**

- **ePHI shall not be transmitted in the “message” section of email over the Internet.**
- **In the event that ePHI information must be transmitted to an external recipient, the data shall be faxed or sent by secure and traceable mail. If such avenues are not available, email may be used if the data is placed in a separate file, “attached” to the email and password encrypted before being sent.**

**The encryption password shall be communicated by phone to the recipient.**

# Computer Use – Cont'd

## Internet Usage

- **Elim Park provides broadband service to the Internet for business purposes.**
- **Abuse of the Internet for personal use is not allowed. Occasional use to check personal email, or travel plans etc., is allowed.**
- **The Internet shall not be used to access sites not in keeping with Elim Parks moral standards. Users failing to heed this restriction, will be disciplined, up to and including job termination.**

# Computer Use Monitoring

- **Elim Park utilizes an electronic monitoring function to maintain discipline in the use of Email and Internet.**
- **Elim Park retains the right to inspect Email and Internet Server logs to insure that policy is being respected.**

# Employees Team Security

- **Employees Reporting of Security Violations**

- **Employees must report actual or suspected security violations to immediate supervisor.**

**(Elim Park has a “no-retaliation” policy for reporting actual or suspected violations.)**

**Employees may use the “Corporate Compliance Suggestion Box” (located outside the office of the Privacy Officer) for reporting actual or suspected security violations.**

**Failure to report an actual violation may result in disciplinary action up to and including termination.**