FAIRHAVEN HIPAA ELECTRONIC SECURITY POLICY

(This document is an addendum to the "Internet, Intranet, and E-mail Acceptable use Policy")

I. POLICY ADDENDUM:

Employees are responsible for maintaining the physical security of computer resources under their control and for protecting the integrity and privacy of the data maintained on them by the appropriate use of lockdown devices such as, password controlled access, data encryption, virus protection software, and routine backup procedures. ***"Trumbull County Board of DD" reserves the right to inspect all data and to monitor the use of all its computer systems associated with patient information.*** Non-compliance with this policy addendum is subject to management review and action, up to and including termination of employment, vendor contract and/or legal action.

All workstations and or tablets with fixed storage that support the process of critical patient information must be equipped with security that secures hardware and/or restricts access to software and patient information.

All workstations and or tablets must be equipped with updated software for detecting the presence of malicious software (e.g., computer viruses), and must have current versions of anti-virus software enabled where applicable.

All workstations must be positioned or located in a manner that will minimize the exposure of any displayed patient or sensitive business information. When necessary, privacy screens should be deployed.

Tablets shall be equipped with 4G services in the event the device is either stolen or lost all data can be erased remotely via this service.

Users accessing electronic patient history information (ePHI) remotely shall employ the appropriate security safeguards set in place by the IT department. ONLY approved users shall have the ability to access ePHI remotely.

The Information Systems Department shall have sole discretion in determining which hardware, operating systems, and connectivity solutions will be supported. Users may not, independently install connectivity hardware or software to the computing resources.

User accessing any ePHI shall not email this information to their personal accounts. Nor shall flash drives be used to move data from one computer to another.

II. PURPOSE:

"***Trumbull County Board of DD***" is committed and required by law to provide a secure computer infrastructure to protect patient history information. Its computer systems hardware and software as well as the information and data carried by the system are the sole property of ***Trumbull County Board of DD***". Any misuse of these systems set in place will result in withdrawal of access to the network pending review. The intent of this policy is to:

- Ensure that each workstation / tablet has the necessary access controls to restrict unauthorized users and programs from accessing patient health or sensitive business information.
- Ensure that software on each workstation on the system (network) is internally compatible and will not lead to degradation of the system.
- Ensure that users are oriented and trained on workstation use and the maintenance of information integrity and privacy and resource security.
- Establish the security requirements for the appropriate use of mobile computing resources including laptops and/or tablets that access patient information or interface to the network.

III. SCOPE:

Employees, vendors, contractors or business associates who have access to patient information or business information stored on its computers or have access to its computer resources or network must sign into a business agreement with "***Trumbull County Board of DD***" where this applies.

IV. DEFINITIONS:

Workstation: A terminal or personal computer which has the capability to access or store patient information (including Protected Health Information as defined by HIPAA), IT resources such as the Internet and Intranet, and business information.

Portable-Computer Device: A portable-computing device is a computer that is easily transported by hand and has the ability to store patient information or business information. "Portable computing device" generally refers to laptop/tablet computers, but can include other emerging technologies that allow storage of and access to information, and that are capable of connection (physical or wireless) to the computer network, including connection to any server or workstation on the computer network.

Portable Storage Devices and Media: Devices which can store patient or business information and which are relatively portable such as disk drives, CD-RW drives, floppy disks, zip disks, CDs and DVDs, flash memory devices, etc. (These devices are strictly prohibited for use with "***Trumbull County Board of DD***" computer systems)

Electronic Patient Health Information (ePHI): Patient information, including demographic information, that:

A. Is created or received by a health care provider, health plan, employer or health care clearinghouse;
B. Relates to the past, present or future physical or mental health condition of a patient; the provision of health care to a patient; or the past, present or future payment for the provision of health care to a patient; and
C. Identifies the patient or can be used to identify a patient.

V. PROCEDURES

A. General

1. Users are required to log-off of applications containing patient information or sensitive business information before leaving their workstations.
2. User's shall save all work associated with ePHI to the network. In the event the user does not have access to the network they may store ePHI to the local TCBDD computer's hard drive ONLY.
3. In the event a critical document or file is inadvertently deleted, contact the Help Desk immediately. ***Do not continue to use the workstation or tablet.***
4. All tablets utilized for remote access must be secured (protected) when not in use. Proper security is dependent on risk factors and available resources at specific locations. Security may be provided by locking the equipment in a cabinet, desk, office, etc. Where such alternatives are not feasible, keeping the device out of sight in a desk or brief case may be appropriate.
5. Keeping information stored on a tablet device secure and current is the responsibility of the person who has the device in his or her possession and control. Those in possession are responsible for breaches of security related to devices in their possession and are required to report the device missing immediately.
6. Password Protection:
   All windows based workstations and tablets which access patient information or sensitive business information, are required to have enabled a password-protected screensaver. Any exceptions must be approved in writing. In cases where password protected screen savers are not available, non-password protected screen savers should be enabled. Users are authorized by this policy addendum to disable the screensaver protection in certain circumstances, for example, when computer support/repair personnel are expected. Department level procedures should define the allowable delay before automatic screensavers activate. That delay should be based upon a balance between operational needs and security risks. For example, consideration should be given to the:
   - number of users having access to the application,
   - number of patient records (high numbers are higher risk),
   - location (higher traffic or public would be high risk)
   - level of sensitivity of the information
     (HIV, oncology, performance evaluations, etc.)
7. All systems containing sensitive patient or business information should enable auto log-off capabilities if available. The delay should be determined based upon the risk criteria above.
8. Employees, physicians, volunteers, and outside vendors are required to have appropriate clearance prior to access to computer workstations.
9. Upon termination or change of job position, users will have network access removed or modified by the IT Department.
10. Where possible, workstations should be segregated based on function and access privileges as it pertains to patient information or sensitive business information.
11. The loss or theft of any portable computing device on which patient or sensitive business information is stored shall be immediately reported to Department Supervisor. The supervisor will contact the Information Security Officer.

12. Reframe from sending emails to internal and external individuals using full patient names (first and last name), instead use either the first letter of the first name and last name or first name and first letter of last name. (i.e. John D. or J Doe)

D. Remote Access

1. Access to "***Trumbull County Board of DD"*** computer systems from remote locations must be approved by the department supervisor, and the Information Systems Department. If a remote access system utilizes a VPN connection, it must be expressly configured to provide secure network access thru encryption.

End of addendum to "Internet, Intranet, and E-mail Acceptable use Policy"