Boston VA Research Institute, Inc.

Date: 5/24/2012

Legal Department

POLICY NO. 12-30

TITLE OF POLICY:

Written Information Security Policy (WISP)

1.0 PURPOSE

The Boston VA Research Institute, Inc.'s (hereinafter BVARI) purpose is to create an effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts in order to comply with the obligations under MA 201 CMR 17.00. The WISP sets forth BVARI's procedure for the electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts.

2.0 SCOPE

This policy applies to all protected personal information managed by BVARI or that BVARI supplies to third party vendors.

3.0 POLICY

3.1 Protected and Confidential Information access and storage

3.1.1 Access to personal information shall be restricted to BVARI employees user accounts only (i.e. only current employees of the BVARI shall have access to personal information). As such, confidential information stored on the BVARI network that is accessible only by the BVARI employee for his/her need to access to those matters. Similarly, physical confidential records are only accessible to BVARI employees who need access to those matters. The physical files containing confidential information are locked in cabinets with keys given to only BVARI Employees who need access to the information.

Furthermore, employees must not to leave documents containing personal information in plain view when away from their desks; such documents should be covered or turned upside down while an employee is away from his/her desk during business hours and when leaving in the evening. Employees must accompany visitors within the office at all times to prevent unauthorized access to personal data.

To ensure reasonable restrictions upon physical access to records containing personal information (taking into account the business needs of BVARI), the front door to the BVARI office remains unlocked during business hours. Outside business hours, the door is locked and the only access is

granted to BVARI employees by an electronic card pass. This ensures the physical security of all files and other records containing personal information.

3.1.2 Access to electronically stored personal information shall be electronically limited to those BVARI employees having a unique login ID, with a three letter complexity password. Electronic access to user identification after four unsuccessful attempts to gain access will be blocked and the Network Administrator needs to be contacted to gain access. Additionally, re-login will be required when a computer has been inactive for more than 15 minutes. BVARI implemented a secure method of selecting passwords by forcing users to change their passwords every 90 days. The same passwords may not be repeated within a 12 month period.

3.1.3 If protected or confidential information needs to be distributed outside of the domain boundaries, it must be distributed through a secure connection. A secure connection is required; a secure connection is defined as an encrypted connection and protected transfer site or, if e-mail is required, mail must be encrypted outside of the secure domain environment. In all instances if feasible, a facsimile is used to transmit protected data.

3.1.4 Employees who leave the BVARI, voluntarily or involuntarily, must return all records containing personal information, in any form, that may at the time of such departure be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

When an employee leaves BVARI, their physical and electronic access to personal information will be immediately blocked. Such departing employee shall be required to surrender all card keys and regular keys that permit access to BVARI's premises and confidential information. Moreover, such departing employee's remote electronic access to personal information will be disabled; e-mail access, internet access, and passwords will be invalidated.

3.1.5 Paper records containing personal information shall be disposed of only in a manner that complies with M.G.L. c. 93I. Specifically, paper records containing personal information shall be destroyed immediately by the use of BVARI's shredder.

3.2 Preventive measures

3.2.1 Anti-virus and anti-malware must be installed on all workstations and laptops. Update files will be automatically performed on a scheduled basis. The windows firewall or other software firewall must be enabled on all laptops and workstations.

3.2.2 Electronic critical files are being backed up on a daily basis and restores are tested once per month. All other files are backed up both onsite and offsite on a scheduled basis. The designated BVARI IT administrator will receive a backup report on a monthly basis indicating frequency and indicating areas where remediation is required.

3.2.3 Firewall firmware must be backed up after each change. All changes must be documented, including risk analysis, and all changes must be approved by the designated BVARI IT administrator.

3.3 Mobile storage and mobile devices

3.3.1 All mobile storage devices, such as portable drives, USB keys and other writable peripheral devices must be password protected or encrypted if they contain confidential or protected data.

3.3.2 All mobile devices for purposes of accessing and sending mail or file storage must be encrypted or protected through a PIN.

3.4 Issuance and return of IT equipment

3.4.1 All workstations, laptops, and other electronic devices will be newly installed with programs under this policy on issuance and will be a member of BVARI's domain. All standard applications will be installed and configured for use. All users will have required rights assigned and the systems will be fully password protected. Additional programs outside of the scope of this policy will need to be approved prior to installation.

3.4.2 Users are responsible for the removal of all private and confidential files prior to the return of any equipment. All confidential protected private information will be removed from the system and stored in secured shares or deleted.

3.5 Employee Training

3.5.1 Each new employee will be instructed in the handling of confidential and protected data.

3.5.2 Every employee needs to acknowledge knowledge of and adherence to the above policies in regards to confidential and protected information. This acknowledgement will be in the form of a signed document.

3.5.3 Once a year all employees will need to confirm their understanding of the WISP which includes their understanding of handling of confidential data. This training must be acknowledged by all employees.

3.6 Procedures in the event of breach

3.6.1 A breach is unauthorized and/or mistaken access to any confidential internal information for its guests or donors while that data or information is in the possession of BVARI its agents and employees. Such a breach would include a network or system intrusion including virus, malware or attack which results in the theft of protective personal information. It also includes loss or theft of physical documents containing protective personal information.

3.6.2 Employees are required to report any suspicious or unauthorized use of client information. Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an

immediate mandatory post-incident review of events and actions taken, if any.

3.6.3 If a breach occurs, it must be reported on discovery to Boston VA Research Institute, Inc. management. Boston VA Research Institute management will implement notification procedures to the Boston Police Department and The Office of the Attorney General. The person whose personal information has been compromised will be notified within 24 hours of discovery. There will also an immediate investigation in order to mitigate future events. Owner is Nancy Watterson-Diorio. Penalty is written warning for employee file.

3.7 Ownership of Security:

3.7.1 There will be a designated security officer responsible for the enforcement and maintenance of the above policies. Any exceptions to the above policies must be approved in writing by the security officer.

3.7.2 Any BVARI employee who violates this policy will be given a written warning

3.7.3 The BVARI security officer will annually review the WISP

3.7.4 3.8 **Vendors**:

3.7.5 Any and all vendors who utilizes any personal and/or confidential information shall provide a copy of their WISP for BVARI records.

4.0 DEFINITIONS

Term: Protected information is defined as:

First and Last Names with:

Social Security or other government ID number

Or

Financial account information including bank accounts, debit cards, and credit cards

5.0 RESPONSIBILITIES

5.1 BVARI Board of Directors: The BVARI Board of Directors is responsible for the overall policy, planning, and coordination of all BVARI activities within the VA Boston Healthcare System.

5.2 CEO: The BVARI CEO is responsible for developing, administering, and coordinating a business process that provides optimal internal controls for BVARI.

5.3 DIRECTOR OF OPERATIONS AND COMPLIANCE: BVARI's Department Director is responsible for ensuring that the BVARI employees follow the policies defined in the policy.

6.0 PROCEDURES

Any vendor who accesses Protected information as defined above, a copy of their WISP shall be provided to BVARI prior to transacting any business.

7.0 RELATED DOCUMENTS:

8.0 REVISION HISTORY

Revision Letter	Author	Revision Date	Description of Changes
A	Jeffrey Burd	08/12/2012	Original Policy
B			

Legal

POLICY NO. **12-30**
Date 5/24/2012

Transmittal Sheet

REASON FOR ISSUE:

SUMMARY OF CHANGES:

RELATED DOCUMENTS:

RESPONSIBLE OFFICER:
General Counsel

RECISSION:

RECERTIFICATION: This policy is scheduled for recertification on or before the last working day of May, 2015.

Nancy Watterson-Diorio

Chief Executive Officer

DISTRIBUTION Board of Directors, Date:

FLD: Sharepoint Server _____ E-mailed _____ to:

BVARI Staff, Stakeholders