Appendix C
SYSTEM SECURITY POLICY

Purpose
Security of electronic equipment and products is critical to the operation of the Vermont Department of Health (VDH). All persons with access to the equipment and services provided by the VDH have responsibility to assure protection from misuse and abuse. The purpose of this policy is to establish guidelines for the physical security of all the VDH's electronic files.

Definitions
Confidential: Information that is considered confidential. Such information includes *(but is not limited to)* hospital records, medical records, professional counselor records of the condition, diagnosis, care or treatment of a patient or former patient or a counselee or former counselee, including outpatient and past, present, or future payment for medical treatment. Such information should not be copied or removed from the organizational control without supervisor's authority. Security should be given the highest consideration in the design and management of an electronic data system involving protected health information.

Critical: Information that is considered critical to the VDH's ongoing operations and that could seriously impede them, if made public or shared internally. Such information includes accounting information, business plans, organizational tables, and highly sensitive data. Such information should not be copied or removed from the organizational control without supervisor's authority. Security should be very high.

Internal Use Only: Information not approved for general circulation outside the organization where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility. Examples include: internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.

Portable Devices: Laptops, electronic "Notepads", PDA's, keychain storage devices, tablet computers, smart phones, security tokens, etc.

Private Documents: Information designated as private, while still work-related. Such information would include: individual evaluations, memos to personnel office, etc. Security at this level is controlled but normal.

Public Documents: Information in the public domain: annual reports, press statements, media presentations, e-mail, etc. which have been approved for public use. Security at this level is minimal.

Policy
Granting Access

1. All requests for electronic system access must originate from the hiring authority.
2. All individuals will sign a confidentiality statement and return it to the hiring authority.
3. Upon granting access, the information technology staff will take the following steps:
    a. Assign the data user a unique user identification.
    b. Assign the data user an initial password/pass phrase.
    c. Provide user with a copy of the VDH Computer Password Policy (http://dii.vermont.gov/sites/dii/files/pdfs/System-Password-Policyv4.pdf).
    d. Provide user with adequate password/pass phrase training (http://dii.vermont.gov/sites/dii/files/pdfs/User-Password-Policy.pdf).

Servers

1. Computer servers will be located in areas where access is limited to authorized persons only. Unauthorized people will not be allowed in these areas without an escort. Areas in which unattended servers are located will be secured with locked doors (http://dii.vermont.gov/sites/dii/files/pdfs/Physical-Security-for-Computer-Protection.pdf).
2. The environment for computer equipment will conform to the manufacturers operating specifications for temperature and humidity.
3. Drinking and eating will be prohibited in the immediate vicinity of computer equipment.
4. All servers will be protected from power surges with an appropriate uninterruptible power source. That power source will provide enough capacity to either safely shut-down the equipment or switch to an alternative power source such as a generator in the event of a loss of power.
5. Unauthorized persons with a legitimate need (on behalf of the VDH), internal or external, will be required to be accompanied by an escort in order to gain access to areas containing confidential or critical information.
6. Servers that are connected to the Internet will be protected by a firewall.
7. A procedure for creating and maintaining backup media, both on-site and off-site must be in place and followed.
8. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons and backed-up on a periodic basis. All logs must be audited on a periodic basis.
9. Intrusion detection and network monitoring are both on 24 hours a day seven days a week basis and all attempted unauthorized access to the network should be logged and reported.
10. Security patches will be applied to servers at least monthly.

Virus Protection

1. Servers and workstations will be equipped with virus protection software.
2. Virus detection software will be configured to monitor at all times.
3. Virus definitions will be updated on a daily basis.

Workstations

1. Every effort will be made to make sure computer workstations will not be located in areas where unauthorized persons can view healthcare information.
2. If workstations are located in areas where unauthorized persons may be, those workstations must be “logged-out” when unattended.

Portable Devices

1. Portable devices are not to be left unattended in high-traffic public areas.

Destruction of Storage Media

1. Internal hard drives that contain confidential, critical, internal use only, and/or private information will be erased or removed by the network administrator before the equipment is removed from the premises.
2. External media such as CD’s, floppy disks, backup tapes, etc. will be destroyed before being discarded.

Approved Method of External Access

1. Healthcare information may not be accessed electronically by external parties without the permission of the Information Technology staff. The Information Technology staff must authorize both the method of such access as well as the information that will be accessed.

Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

-Source Vermont Immunization Registry Business Plan, March 2015