County of San Bernardino
Department of Behavioral Health

Data Integrity Policy

Effective Date	1/29/07
Approval Date	1/29/07

Allan Rawland, Director

Policy

It is the policy of the Department of Behavioral Health that the safety and integrity of client ePHI and other departmental confidential information is protected against unauthorized alteration or deletion of data, programs and files.

Local (site-based) Measures

Based upon a risk assessment, clinic or office supervisors must ensure the safety of internal, confidential, restricted, or critical information, including computer programs on network shares and storage media. Local (site-based) measures include the following expectations:

- Implement and regularly update anti-virus software on systems and network devices
- Establish policies and procedures for implementing new or upgraded applications and infrastructure environments from development through quality assurance testing to produce implementation
- Maintain a copy of tested production applications and specifications in a secure location, preferable in a geographically separate facility (or a copy of critical software source files maintained off-site)
- Establish authentication procedures for updates and patches. All new programs should be verified before installation

Virus Preventive Measures

System users will adhere to a pro-active preventative approach to eliminate virus infections. It is the responsibility of the system user to maintain use of tools and follow policies and procedures provided by Information Technology (IT) in order to minimize the risk of infection to the user's system, as well as to other systems with which it interacts.

Restrictions for Users

Users must abide by the following restrictions:

- Do not disable, interfere with the operation of, or tamper with the anti-virus software installed on any system controlled, managed, or connected to County or Department systems

  - A viral detection product will be provided, installed, configured and managed by Information Technology (or the proper authority, in the case of County maintained systems) for use on all systems as appropriate

- Do not download programs from public bulletin boards, Internet websites or any other media source including CD-ROMs without the written approval of the department's Security Officer and the Information Technology manager
  - Note that viruses are sometimes disguised as games or utilities

- Do not execute any new uninstalled software (e.g., .exe, .com, .bat or script file) without prior written approval of the department's Security Officer and the Information Technology Manager
  - Limit the installation of new software to applications intended for business operations
  - Minimize the exchange of executable code between systems whenever feasible (as when writing Microsoft Access macros)

- Do not place public domain or "shareware" programs in a common file server directory (i.e., "V" drive, department folders) that could be accessible to any other computer on the network, without written authorization from the Information Technology Manager

- Use only legitimate copies of software. Installing or knowingly using pirated software is strictly forbidden

- Write-protect removable media (floppy disks) when using or transferring data between systems. Media (such as floppies) that contain only read-only data files should also be write-protected. Any removable media, which must be written, can be susceptible to viruses by adding (unwanted) hidden files or replacing (with corrupt versions) existing files. No ePHI will be placed on any removable media such as CDs and floppy disks unless written authorization is obtain from the department's Security Officer and the Information Technology Manager

- Contact the "Helpdesk" immediately if a virus, worm, Trojan or other suspicious files are found or if a workforce member is unsure about or unable to verify that computer files are virus free. **Do not use the system under any circumstances until it is known to be virus-free**

- Be aware of the responsibility of all users to protect the physical security of all DBH systems, media and related devices. All systems will be secured as appropriate to prevent theft, inappropriate access, alteration, or destruction.

Anti-Virus Software

In general, workforce members will not need to be involved with the installation or upkeep of virus protection. The Information Technology unit will maintain such applications with the following requirements:

- Anti-virus software will require little or no user interaction and will automatically maintain and update itself as needed, or will be controlled and updated by IT
- Users must not disable any anti-viral software at any time
- Anti-virus software should be scanned for automatically and installed if not present on any system connected to the network either locally or remotely
- Anti-virus software and/or the network operating system will have automatic immediate central reporting ability and notification
- All systems will run a smart anti-virus behavior blocking device driver (not a TSR, not a resident scanner), when possible
- Users logging in should be checked to determine if an anti-virus device driver is running. If not, it will be automatically installed in their machines
- Monitor for and install all updates/patches immediately
- All systems should be scanned at log on
- Each user is responsible for protecting other users of DBH systems and technologies

Infection Control

The following infection control must be followed:

- If any virus is detected on a system component, the unit is to be powered down and the "Helpdesk" notified immediately
- Information Technology will disconnect the infected system from the network and perform the necessary steps to eradicate the virus and document the incident
- Information Management will review the incident report for follow-up