Computer and Network Appropriate Use Policy

Effective Date	10/05/2006
Revised Date	08/28/2023

DocuSigned by:
Dr. Georgina Yoshioka
7DF8077EEA674B2...
Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to utilize Behavioral Health and/or County electronic systems for legitimate department business purposes only.

Purpose

To provide DBH staff with information regarding the appropriate use of department systems including those network services provided by the County.

Definition(s)

Individually Identifiable Health Information (IIHI): Information including demographic information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of and identifies the individual, or to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Sanctioned Device: Any equipment, software, application, or electronic tools that have not been procured and/or approved by Information Technology (IT).

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information, that is linked or linkable to a specific individual.

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium (electronic, paper, microfiche, or verbal).

Staff/Users/Employees: Interchangeable terms used to reference DBH or other departmental employees, volunteers, work study individuals, contracted service personnel, vendors and others who have been authorized access to computers and/or computer lab facilities.

Systems: An all-inclusive term used to reference computers, workstations, desktops (physical and virtual), laptops, software applications, video-conferencing equipment, servers (physical and virtual), and networks or network services throughout this and related documents.

Continued on next page

General Information

County and/or department computer systems are provided to employees to assist them in the performance of their job duties. Using the systems for other than DBH business is prohibited.

Staff should have no expectation of privacy in anything they create, store, send or receive on a DBH system. All business conducted on departmental systems is considered the property of the department and therefore open to view and/or monitoring by authorized personnel.

Acceptable Uses

The following lists examples of acceptable uses of the DBH network:

- Communication and information exchange directly related to the directive or work tasks of the DBH;
- Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to DBH activities;
- Applying for or administering grants or contracts for DBH research or programs;
- Advisory, standards, research, analysis, and professional society activities related to the DBH governmental work tasks and duties;
- Announcement of new laws, procedures, policies, rules, services, programs, information, or activities, and
- All DBH business conducted electronically should occur via County owned servers and/or devices, use of personally owned devices must be approved by the IT department.

Prohibited Uses

Electronic media and communications shall not be used in any manner in violation of the law or County rules, policies, or procedures. Electronic media and communications shall not be used for any improper, illegal, offensive, or harassing purpose. Prohibited uses include but are not limited to the following:

- Use of the Internet or system resources for reasons other than for DBH business purposes;
- Downloading or storing applications, system software, audio, video, or picture files to department systems unless these files are required to perform operational responsibilities;

Continued on next page

Prohibited Uses, continued

- Accessing or sending any material or communication in violation of any federal, state, or local law, ordinance, or regulation;
- Installing or connecting any non-sanctioned device onto DBH systems or the County's network (excluding IT approved use of personally devices);
- Installing custom screen savers on DBH systems without written approval from IT;
- Storing electronic data without receiving prior authorization from IT to include PHI and/or PII, on:
  - Computer Disks (CD)s
  - Recordable (DVDR) and **DVD** Rewriteable (DVDRW) disks
  - A systems hard drive (drive C)
  - External/portable hard drives
  - USB flash drives
  - Any other devices manufactured for this purpose.

Note: Any external/portable hard drive or USB flash drive issued by IT must have as a minimum, 256-Bit encryption.

- Removing or manipulating any authorized software placed on DBH systems by IT;
- Copying operating systems, software, or utility tools from a DBH system for use on home computers or for personal gain;
- Modifying, revising, transforming, recasting, adapting, reverse-engineering, disassembling, or decompiling any software;
- Intentionally disrupting a network service;
- Downloading, uploading, using, or otherwise distributing copyrighted material without written permission or in violation of licensing agreements;
- Using work time and resources for personal gain, personal services, advertisement, or personal for-profit business interests;
- Posting or sending threatening or offensive messages;
- Downloading, uploading, transmitting, or otherwise distributing any content that violates any existing law, regulation, County policy, departmental or personnel rule;
- Downloading, storing, or sending inappropriate e-mails or other forms of electronic communication that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or otherwise in violation of County policy;
- Working on personal activities that incur additional cost to the department or interfere with a user's work performance;

Continued on next page

Prohibited Uses, continued

- Participating in chat room discussions, posting, or viewing electronic bulletin boards and social networking websites (Facebook, Instagram, etc.) unless doing so is a function of County responsibility;
- Using video and/or audio streaming and downloading technologies for non-County purposes;
- Misrepresenting, under any circumstances, an employee's identity, and
- Any action intended to accomplish or assist in unauthorized access to computer systems.

Information Technology Responsibilities

The IT department oversees the installation, maintenance, and monitoring of computer network systems within DBH. DBH-IT responsibilities include, but are not limited to, the following: Issuing unique system User Identifications (User ID) and complex passwords, which allow users access to applications, networks, and the Internet;

- Protecting the data and information stored on all system servers and ensuring that such data is recoverable and restorable in the event of damage or loss, including the development of a business contingency plan;
- Ensuring all County and department policies, Federal and State regulations, and HIPAA Security Rules within its area of responsibility are maintained, monitored, and exceptions are properly documented and reported;
- Controlling the rate of technology introduction and the types of technologies deployed within DBH, and
- Ensuring continued compliance with licensing laws.

IT will randomly scan for inappropriate file types; inappropriate files will be purged from the system without prior staff notification.

Staff Responsibility

DBH staff are responsible for ensuring use of system resources professionally, ethically, and lawfully as further defined in **County Policy 14-04 Internet/Intranet Use Policy** and in the **Internet Account Policy** (IT5003).

DBH staff are directly responsible for all actions resulting from the use of their User ID and password. User ID and password specifics are further defined in the **User ID and Password Policy** (IT5009).

Consequences of Violations

Staff violating the use of DBH systems as defined above or in any DBH or County policy may be subject to disciplinary action including and up to termination of employment. Deliberately performing acts that waste system resources or unfairly monopolize resources to the exclusion of others may affect the level of recommended level of discipline.

Continued on next page

Related Policy or Procedure

San Bernardino County Policy Manual:

- Electronic Mail (E-mail) Policy (14-01)
- Internet/Intranet Use Policy (14-04)
- Protection of Individually Identifiable Health Information (16-02)
- Protections of Individually Identifiable Health Information (16-02SP1)

DBH Standard Procedure Manual and Departmental Forms:

- Internet Access Policy (IT5003)
- Electronic Mail Policy (IT5005)
- Remote Access Policy (IT5006)
- Device and Media Controls Policy (IT5008)
- User ID and Password Policy (IT5009)

Reference(s)

- California Civil Code 56 et seq. (The Confidentiality of Medical Information Act)
- Code of Federal Regulations:
  - 42, Part 431.300, Section 2.1 et seq.
  - 45, Parts 160 and 164.
- Department of Behavioral Health Medi-Cal Privacy and Security Agreement
- Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)