County of San Bernardino
Department of Behavioral Health

Security of Protected Electronic Health Information Policy

Effective Date 10/5/06
Approval Date 10/5/06 **Allan Rawland, Director**

Policy

It is the policy of the Department of Behavioral Health (DBH) to implement administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information (e-PHI) that it creates, receives, maintains, or transmits. It is the responsibility of all care providers.

Purpose

To have a written policy in accordance with applicable federal and state laws governing the protection of health information and apply the policy to the following:

A. **Staff/Contract Agencies**- DBH regular employees, service contract providers, volunteers, interns, physicians and others granted authorized access to DBH protected health information regardless of medium.

B. **Clinical Information**- Generated in the context of patient care including, clinical assessments, client plans, results of laboratory tests, and the interdisciplinary notes detailing patient contacts. Such patient-related data may be available electronically, or in written form in standard medical records and patient charts. It may be available for individual patients or for groups of patients. Such information may reside in large central computer databases, such as those maintained by DBH and associated clinics where it can be made available electronically to peripheral workstations or to peripheral clinical databases maintained by individual departments.

C. **Information Systems and Technology devices used to process, store, and transmit information**- All hardware and/or purchased software of any kind including in-house developed programs are considered proprietary and the sole property of DBH.

Definitions

- **Hybrid Entity:** As defined in the HIPAA Privacy and Security Rules, is a "single legal entity", whose business activities include both covered and non-covered functions, which designate or one or more "health care components" in writing. The County is a hybrid entity under HIPAA and as such has designated certain departments of the County as its covered healthcare component.

- **Information User:** Any person authorized by the owner to access DBH data, information, or technology (regardless of the medium it is on or in).

- **Residual Risk:** The amount of risk remaining after a security control is implemented. Residual risk exists when a decision is made to accept a risk due to the cost of the control being high or the likelihood or impact of the threat being low.

- **Information Technology:** The custodian of data, information, and technology assets owned by DBH. Duties include:

  1. Creation and execution of instructions for collecting, processing and distributing data and information.

  2. Protection of data and information while it is being processed or stored on the central computers and to insure that such data is recoverable and restorable in the event of damage or loss, including the development of business contingency plans.

  3. Control of the rate of technology introduction and the types of technologies.

Safeguard Requirements

General Requirements- Safeguards to protect the confidentiality, integrity, and availability of information are determined through initial and periodic risk and security assessments conducted by Information System Department (ISD).

HIPAA-Defined Safeguard- These safeguards, as defined by the HIPAA Security Rule, require the establishment of policies, procedures and processes in order to comply with the Rules standards. These policies must interact as to not cause confusion or conflict with one another.

Secured Information- Confidential and protected health information, throughout its life cycle, will be protected in a manner consistent with its sensitivity and criticality (value) to DBH and its support functions, research activities, educational and instructional programs, and health care delivery services. This protection includes an appropriate level of physical and electronic security for the networks, facilities, equipment and software used to process, store, and transmit information. Information used in conducting DBH business must have adequate controls to protect that information from accidental or deliberate disclosure, damage, misuse, or loss. Only those with a need to know may view protected health information. Protected Health Information must be carefully handled and never left where unauthorized persons might see it.

Organized Health Care Arrangements (OHCA)

It is important to understand that all contracted health care providers and medical groups/corporations of DBH agree to abide by DBH policies as a prerequisite of participation in the DBH's OHCA. OHCA participants further agree to accept application of DBH's sanction policies to their personnel for violations of DBH privacy and security policies.

Department Responsibility

Department Security Official:
All policies related to information security should be reviewed at least annually or upon any breach or suspected breach of privacy or security and revised if necessary.

Program Managers and Supervisors:
Must ensure, via classroom attendance records, that workforce members and system/information users are trained with regard to and held responsible for protecting DBH e-PHI. In addition, they will be trained on an annual basis regarding compliance with policies, standards, and procedures governing its use.

All Staff:
Prevent unauthorized access of computer system.

DBH employees must:

- Create and maintain DBH e-PHI in a secure environment
- Evaluate DBH e-PHI and use cost-effective controls
- Use the access control system(s) provided to protect e-PHI residing on the central computer files
- Ensure the confidentiality, integrity and accuracy of DBH e-PHI
- Promptly report the compromise or circumvention of any safeguards
- Comply with established safeguards, as this is a condition of continued employment

Procurement/ Acquisition Requirements

- Information Technology will complete a Risk Assessment & Analysis of all information systems and/or technology devices to include, but not limited to; desktop computers, laptops, handheld computing devices, peripheral equipment, storage media, software and supporting infrastructure environments as part of the procurement/acquisition process to meet minimum safeguard specifications, defined by this and related privacy and security policies of the department

- All information technology and systems purchased after the effective date of this policy must comply with this and related privacy and security guidelines. Existing systems must be brought into compliance to the greatest extent possible pursuant to a completed system/application security risk assessment

Risk Assessment and Residual Risk

Risk Assessment- Information Technology will provide oversight in conducting risk assessments and analysis on all information technology systems, devices and related equipment (including purchases of new systems as part of the procurement process) on a periodic basis and update such assessments as needed in order to effectively manage the confidentiality, integrity and protection of electronic health information. The risk assessments should provide administration with enough information to make decisions about residual risk.

Residual Risk- Administration must determine the amount of residual risk to accept. DBH must utilize reducing and accepting risk in order to maintain compliance with regulations and best practices for information security.

Four Basic Ways to Address Residual Risk

Transferring	If Administration decides that the total or residual risk is too high; it may purchase insurance to offset any costs should the risk be realized. For a cost, which is less than the control, they are transferring the risk to the insurance company.
Rejecting	If Administration ignores the risk they are choosing to reject it.
Reducing	If Administration implements controls they are reducing the risk.
Accepting	If Administration decides to live with the identified risk, they are accepting the impact of it should it be realized.

Risk Management

Department managers, supervisors and Information Technology are responsible for prioritizing, implementing, and maintaining the appropriate risk-reducing measures identified from the risk analysis process. Implementation of security measures sufficient to reduce risks and vulnerabilities to information systems and resources to a reasonable and appropriate level are required in order to:

- Ensure the confidentiality, integrity, and availability of all sensitive information created, received, maintained, or transmitted
- Protect against any reasonably anticipated threats or hazards to the

security or integrity of such information

- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
- Ensure compliance with this policy by workforce members and medical staff

---

Workforce Security

The Department shall implement procedures regarding the interactions of all individuals authorized for system access with confidential and protected electronic health information that will ensure that such information is appropriately protected. See below table for typed of access and procedures:

- Access to e-PHI will be authorized by the security official, according to the minimum necessary access as determined by employee assignment, and requiring a background check. Department Managers/Supervisors will determine these needs for access. Access granted will be reevaluated for each change of role
- Access controls such as unique usernames will be established and enforced for each system and/or software application and maintained by Information Management
- Procedures for the timely termination of access will be developed and utilized for all terminating and terminated individuals regardless of their affiliation
- Procedures for authorizing and monitoring all access to systems from outside the Department will be developed and enforced. This includes access by authorized individuals from their homes or other remote locations

---

Personal Hardware/ Software Use

Personal hardware, technology devices or software are not allowed to be used or installed for any reason whether for personal or business operations or patient care or be connected in any way to the DBH information systems or network or be used for storage of DBH e-PHI information without prior written authorization from the DBH Business Applications Manager, even if not connected to the DBH network or computer systems. Only DBH authorized or controlled technology devices, computers and equipment may be connected to the DBH network or information systems for the creation, use or storage of client related e-PHI information.

Use of Removable Storage Media

Individuals who are authorized to access e-PHI maintained by the department may not store or off-load this information to any storage media (floppy disks, CD's, DVD's and/or internal/external drives attached to desktops, laptops, PDA's etc.) without the prior written permission of Department Security Official.

Enforcement / Workforce Sanctions (Disciplinary Action)

Failure of employees, contract providers, volunteers, interns and system and data users to safeguard information and assets as defined in this policy may subject the individual(s) to disciplinary action up to and including termination of employment or contract or expulsion from training programs. Supervisors and managers who fail to enforce this policy in its entirety will be reported to their immediate supervisor for disciplinary action. Violation of Department policies, State and Federal laws governing privacy and security of e-PHI may be applied to the organization and the individual. Sanctions include but are not limited to reprimand, termination, monetary penalties and incarceration depending upon the severity of the disclosure. Sanction must be documented and maintained for six years.

Monitoring of Use

Information Technology must implement procedures to regularly monitor records of information system activity, such as audit logs, access reports, and security incident tracking reports to identify discrepancies between policies and practices. A "system" normally includes "hardware, software, information, data, applications, communications, and people."

- Monitoring should be performed by use of the audit capabilities of the access control software system and through the internal creation and use of programs specific to this purpose as approved by Information Technology and the security official

- Upon notification of any abnormal activity, the information system/application owner/responsible department must review the incident and take appropriate action and follow-up

Data Integrity and Protections

All staff will protect the integrity of DBH electronic data. Back-up copies of e-PHI will be created regularly and stored off-site. Programs used on DBH computers must be approved by and installed by Information Management. Copies of database applications using and storing e-PHI will be created and stored by Information Management. Information Technology will maintain anti-virus software that monitor each computer at all times and log noted problems. Users must not disable or interfere with this software. Users will contact Information Technology when any sign of virus infection appears on their computers.

External Transmission of e-PHI

Information Technology will take all reasonable precautions to minimize the vulnerability of e-PHI data transmitted outside of the County network by using the appropriate data security tools. Electronic-PHI will not be transmitted or accessed from a home computer by DBH users using the County's e-mail connection to work. Electronic-PHI will not be transmitted outside of the DBH Domain unless it is protected.

Contingency Planning

Information Technology is responsible for establishing and annually reviewing plans for actions to be taken in the event that DBH computer systems are disabled or damaged by persons or natural disaster. This will include using stored back-up data and programs, access to facilities for repairs, temporary uses of non-DBH computers and devices, and any new security procedures that might be needed in such circumstances.

Training

The Department is responsible for providing training to all staff regarding e-PHI privacy and security issues, and to all new employees upon hire.

References

- **Health Information Portability Act Manual**
- **Security Management Process (Required) [45 C.F.R. § 164.308(a)(1)(i):** Implement policies and procedures to prevent, detect, contain, and correct security violations
- **Risk Analysis (Required) [45 C.F.R. § 164.308(a)(1)(ii)(A)]:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity
- **Risk Management (Required) [45 C.F.R. § 164.308(a)(1)(ii)(B)]:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with section 164.306(a)
- **Information System Activity Review (Required) [45 C.F.R. § 164.308(a)(1)(ii)(D)]:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
- **Evaluation Standard 45 C.F.R. § 164.308 (a)(8)**
- **Policies and Procedures C.F.R. § 164.316(a):** Outlines the requirements for developing security policies and procedures. Policies and procedures must be updated when there is a change in the law; an environmental or operational change that affects the security of the e-PHI; and/or a change in practices

---