	COUNTY OF SAN BERNARDINO **STANDARD PRACTICE**	**No. 14-03 SP 03** **PAGE** 1 **OF** 9 **EFFECTIVE DATE** June 10, 2016
POLICY: **SP:**	**HIPAA POLICY** **Administrative, Technical and Physical Safeguards**	**APPROVED** GREGORY C. DEVEREAUX Chief Executive Officer

PURPOSE

To document minimum administrative, technical and physical safeguards applicable to the County's Health Care Component (HCC) in order to minimize the risk of unauthorized access, use or disclosure of Protected Health Information (PHI).

DEPARTMENTS AFFECTED

All County agencies, departments, and Board-governed Special Districts that are determined to be covered by the Health Insurance Portability and Accountability Act (HIPAA).

DEFINITIONS

Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Covered Entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA covered transaction.

Disclosure: The release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

Electronic Protected Health Information (ePHI): Protected health information in electronic form.

Health Care Component: County departments or programs that meet the definition of a Covered Entity or Internal Business Associate.

Health Insurance Portability and Accountability Act (HIPAA): A federal law designed to provide privacy and information security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. (45 C.F.R. Parts 160 and 164)

Hybrid Entity: A single legal entity: (1) that is a Covered Entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates Health Care Components.

Internal Business Associate: A County department or program that provides services to another County department or program covered by HIPAA that if it was a separate legal entity would fall within the definition of a Business Associate.

Physical Safeguards: Physical measures, policies and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information (PHI): Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium (excludes individually identifiable health information in employment records held by the Covered Entity in its role as employer).

Technical Safeguards: The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Unsecured PHI: Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under 42 U.S.C. Section 17932 subdivision (h)(2).

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or internal business associate, is under the direct control of such covered entity or internal business associate, whether or not they are paid by the covered entity or internal business associate.

PROCEDURES

Departments within the HCC must comply with the minimum administrative, technical and physical safeguards detailed below. Departments shall implement reasonable and appropriate safeguards specific to their department that are in addition to and do not conflict with the safeguards contained in this Standard Practice (SP).

Administrative Safeguards

A. **Security Management Process**: HCC departments must comply with the following safeguards to prevent, detect, contain and correct security violations.

1. Risk Analysis: Departments shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the department. Departments shall conduct such a risk assessment of systems containing ePHI at the time of procurement and at any time there is a substantial change to the system thereafter. Departments shall conduct an overall assessment at a minimum every three (3) years.

2. Risk Management: Departments shall adopt and maintain a risk management plan sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the following:

   a. Ensure the confidentiality, integrity, and availability of all ePHI the department creates, receives, maintains, or transmits.

   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

   c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA.

   d. Ensure compliance with HIPAA by the department's workforce.

3. Sanction Policy: Employees who fail to comply with the security policies and procedures of the County and the department shall be disciplined in accordance with Human Resources policies and County Personnel Rules. Departments shall have policies and procedures that address the sanctions applicable to violations of HIPAA.

4. Information System Activity Review: Departments shall regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

B. **Assigned Privacy and Security Responsibility**: Departments are required to identify a privacy officer and a security officer within the department who are responsible for the development and implementation of the policies and procedures required by County Policy, Standard Practices and HIPAA for the Department.

C. **Workforce Security**: Departments shall implement policies and procedures to ensure that all members of the department's workforce have appropriate access to PHI, and to prevent those workforce members who should not have access from obtaining access to PHI.

1. <u>Authorization and/or Supervision</u>: Only those employees necessitating access to PHI to fulfill a job function shall be authorized to access PHI. Managers and/or supervisors are required to supervise employees granted access to PHI to ensure the employees are utilizing their access correctly and only for assigned job functions. Departments shall implement procedures for the authorization and/or supervision of workforce members who work with PHI or in locations where it might be accessed.

2. <u>Workforce Clearance Procedure</u>: Upon hire of an employee and at regular intervals thereafter, the department shall determine the appropriate level of access to PHI to be granted to the employee. Any workforce member must undergo a background check prior to being granted access to PHI. Only the minimum level of access shall be granted for the assigned job function. Employees are only authorized to view PHI pursuant to a stated job function and shall only view the minimum amount necessary to fulfill the job function. Departments shall implement procedures to determine that the access of a workforce member to PHI is appropriate.

3. <u>Termination Procedures</u>: Access to PHI shall be terminated promptly upon departure of an employee or when assigned job duties that no longer require access to PHI. Departments shall implement procedures for terminating access to PHI in such circumstances.

D. **Information Access Management**: Departments shall implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the HIPAA Privacy Rule.

1. <u>Access Authorization</u>: Each department must ensure that only workforce members who require access to information are granted access. Departments are responsible for ensuring that the access to information granted to workforce members is the minimum necessary required for individual job roles and responsibilities. Access to information must be granted upon a demonstrable and valid "need-to-know" basis and not merely by position or title. If the workforce member no longer requires access, the department must complete the necessary process to terminate access in a timely fashion. Departments must implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process or other mechanism.

2. <u>Access Establishment and Modification</u>: Departments shall establish and document authorizations granted for a workforce member's access to workstations, transactions, programs, processes and systems. Departments shall regularly review and modify a workforce member's right of access to any workstation, transaction, program, process or system that contains ePHI to ensure access remains necessary. Departments shall review access granted to all systems, programs, and processes containing ePHI at regular intervals to ensure only authorized individuals maintain access.

3. <u>Access of ePHI</u>: Workforce members are prohibited from accessing ePHI from a public computer, a public wireless network, or an unsecured wireless network, unless a secure process that has been authorized by the department is utilized. ePHI shall not be accessed from a personal mobile device unless a secured process that has been approved by the department is utilized. Departments shall implement policies and procedures to control access of workforce members' use of the San Bernardino County Outlook Web App (webmail), Virtual Private Networks (VPN) and other remote access technologies to prevent unauthorized access to ePHI from public and personal devices. Departments shall implement policies and

procedures concerning the telecommuting of workforce members, to ensure ePHI is accessed in a secure, authorized and appropriate manner.

E. **Privacy and Security Awareness and Training**:

1. Training*:* Before access is granted to PHI, workforce members shall receive training on the privacy and security requirements of HIPAA and the County and department policies established thereunder in accordance with Standard Practice 14-03 SP04.

2. Security Reminders: Departments shall conduct periodic security reminders for all workforce members granted access to PHI no less than every year.

F. **Privacy and Security Incident Procedures**: Departments shall implement policies and procedures for responding to privacy and security incidents. Policies must address incident reporting, mitigation, documentation, response timeframes and procedures, compliance with applicable state and federal reporting requirements, retention of reports and documentation, and sanctions.

G. **Contingency Plan**: Departments shall establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. HCC departments shall comply with the following:

1. Data Backup Plan: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

2. Emergency Mode Operation Plan: Establish procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

3. Disaster Recovery Plan: Establish procedures to restore any loss of data and normal business processes.

4. Testing and Revision Procedures: Implement procedures for periodic testing and revision of contingency plans.

5. Applications and Data Criticality Analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.

H. **Evaluation**: Departments shall perform a periodic technical and nontechnical evaluation of security controls and policies and procedures that affect the security of PHI and the systems that contain it.

Physical Safeguards

A. **Facility Access Controls**: Physical access to electronic information systems and facilities in which the electronic information systems are housed must be limited to only those authorized to access the system or facility.

1. Contingency Operations: Departments must establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2. Facility Security Plan: Departments must implement policies and procedures to safeguard their facilities and the equipment therein from unauthorized physical access, tampering, and theft. At a minimum the policies and procedures must include the following:

   a. Facilities containing PHI are secured through the use of entry by ID badge, key card or other secure method to prevent unauthorized access.

b. Keypads/cipher locks are changed periodically.

c. Computer server rooms are secured from unauthorized access. Access must be permitted and documented in such a way as to provide sufficient audit trail capability.

d. Workforce members shall not allow entry into a secure facility to an unauthorized individual.

3. Access Control and Validation Procedures: Departments must implement procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revisions. At a minimum the policies and procedures must include the following:

   a. Departments must ensure that workforce members surrender ID badges promptly after termination or upon departure from the department.

   b. Workforce members must report lost/stolen badges immediately and shall not share ID badges.

   c. Departments shall periodically review access granted to facilities to ensure access remains appropriate.

   d. Documentation of visitor controls, including the use of sign-in/sign-out sheets, physical escort of visitors through the facility and no visitors left unattended in areas where PHI is located or stored.

4. Maintenance Records: Departments must implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.

B. **Workstation Use and Security:** Departments must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. Departments must further implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. At a minimum departments must require:

1. Workstations must be used in an appropriate and authorized manner. Workforce members must use workstations to support clinical, research, education, administrative and other legitimate functions of the department.

2. Workforce members have no expectation of privacy when using department systems and workstations. The County may log, review or monitor any data contained within or transmitted by any County owned information system, technology device or equipment.

3. Access to workstations must be controlled by requiring authentication using a User ID and a password or an access device (e.g., token, fingerprint readers), unless specifically exempted and authorized by the department.

4. Workforce members must report suspected unauthorized access/use of a workstation or the loss or theft of a workstation immediately.

5. Workforce members must lock or log off of the workstation before leaving the workstation unattended for any period of time.

6. Workstations must be positioned or protected from view so that ePHI is not visible to unauthorized persons.

7. Workstations and peripheral devices must be secured in areas not accessible by unauthorized workforce members or other unauthorized personnel or individuals.

8. On a periodic basis the risk to workstations containing ePHI must be assessed to determine the level of physical protection required.

9. Portable workstations must be physically protected at all times, including while traveling.

10. PHI may not be stored on a portable workstation unless it is protected either through encryption or an equivalent protection method.

C. **Device and Media Controls:** Departments must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility. Media can be any storage device or medium which is used to store in any way ePHI, including, but not limited to, CDs, DVDs, thumbdrives, floppy disks, cell phones, wireless devices and external hard drives.

1. Disposal: Departments must implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored. At a minimum, ePHI on electronic media must be disposed of through: clearing (using software or hardware products to format or overwrite media in order to render ePHI indecipherable or inaccessible); purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains); or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

2. Media Re-Use: Departments must implement procedures for the removal of ePHI from electronic media before the media are made available for re-use. Prior to making storage devices and removable media available for reuse, workforce members must ensure that the device or media does not contain ePHI.

3. Accountability: Departments are required to maintain a record of the movements of hardware and electronic media. Departments must designate a person responsible for tracking the movements of hardware and electronic media containing ePHI within the department.

4. Data Backup and Storage: A retrievable, exact copy of ePHI, must be created when needed, before movement of equipment.

D. **Paper Document Controls**

Departments must implement policies and procedures to secure and protect paper documents containing PHI. Policies and procedures must address at a minimum, the following:

1. Storage of PHI*:* PHI in paper records must be secured at all times. PHI must be stored in a locked desk, filing cabinet, office or storage/file room. Keys for access to filing cabinets, desks, offices and storage/file rooms must not be left unattended on a desk or stored in a manner that is accessible to unauthorized persons. Individual shred boxes must be disposed of when leaving your work area.

2. Clean Desk Policy*:* Workforce members shall ensure that all PHI in paper and electronic form is secured in the work area when leaving the area for any amount of time and at the end of the day. All PHI must be removed from the desk and locked in a secure location, e.g. locked

drawer, file cabinet, or file room, unless located in a locked office or other approved secure area.

3. Printers and Faxes*:* Fax machines and printers must be kept in secured areas where information is not available to unauthorized workforce members or the public. Workforce members must verify the fax number with the intended recipient prior to sending PHI via fax. Fax machines and printers must be cleared regularly to ensure PHI remains protected and secured.

4. Mail*:* A secure courier with signature receipt must be utilized when sending large volumes of PHI. In addition, disks and other transportable media sent through mail or courier must be encrypted prior to sending.

5. Safeguarding PHI*:* PHI shall not be left unattended on desks or in unsecured areas, including conference rooms or public access areas. When traveling with PHI, PHI must not be left unattended or unsecured in checked baggage or in a public location. PHI should not be left unattended in a vehicle, however if necessary PHI may be secured in the trunk of a vehicle. PHI must not be left unattended in a vehicle overnight.

6. Destruction of PHI*:* PHI in paper form shall be disposed of by shredding the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed. Hard copies that contain PHI must be disposed of in containers designated for storage of such documents prior to destruction, e.g. shred bins. PHI deposited in a shred bin must be fully encompassed in the shred bin to prevent removal, and the shred bin must not be overfilled.

Technical Safeguards

A. Access Control: Departments shall implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. §164.308(a)(4). The policies and procedures shall at a minimum require the following:

1. Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.

2. Emergency Access Procedure: Establish procedures for obtaining necessary ePHI during an emergency.

3. Automatic logoff: Computer systems containing ePHI must be set to automatically log off after no more than 10 minutes of inactivity. Workforce members shall lock or log off a system containing ePHI whenever leaving the system unattended.

4. Encryption and Decryption: Implement a mechanism to encrypt and decrypt ePHI.

5. Password Management: Access to any workstation, program, process or system that contains ePHI shall be protected through the use of a unique User ID and password. Passwords shall not be common or easily identifiable (birthday, name, etc.). Passwords should not include dictionary words. Employees shall not share or make accessible User IDs or passwords. Passwords shall be changed no less than every 90 days. Departments must implement a lockout process after a specified number of failed attempts to access a workstation or system.

B. Audit Controls: Departments shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Departments shall implement procedures for monitoring log-in attempts and reporting discrepancies.

C. Integrity: Departments shall implement policies and procedures to protect ePHI from improper alteration or destruction.

1. Mechanism to Authenticate ePHI: Departments shall implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

2. Protection from Malicious Software: Departments shall implement procedures for guarding against, detecting, and reporting malicious software.

D. Transmission Security: Departments shall implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

1. Encryption Safeguards
   Departments shall use appropriate encryption to protect ePHI stored on portable devices or transmitted across an unsecured network such as the internet or wireless network in accordance with HIPAA regulations. Departments shall implement written policies and procedures for encrypting and decrypting ePHI as appropriate.

   a. *Encryption Standard*: ePHI must be secured using a Federal Information Processing Standard (FIPS) approved algorithm. In accordance with National Institute for Standards and Technology (NIST), whenever possible, Advanced Encryption Standard (AES) should be used for the encryption algorithm based on its strength and speed.

   b. *Email*: Email containing ePHI must be encrypted prior to sending outside of the County network.

   c. *Desktops, Laptops and Tablet Computers*: All County-owned desktops, laptops and tablet computers used to store ePHI must utilize Full Disk Encryption (FDE). Staff shall not store ePHI on personally owned devices.

   d. *Mobile Devices*: Departments must have policies, procedures and safeguards in place that address the use and security of County-owned and personal mobile devices. Mobile devices include, but are not limited to, smart phones, blackberries, phablets, personal digital assistants (PDAs) and smart watches.

   e. *Universal Serial Bus (USB) Drives, External Hard Drives, CDs and DVDs*: USB drives (also known as thumb drives, jump drives, flash drives), external hard drives, CDs and DVDs shall not be used to store ePHI unless the device or media is encrypted. The ePHI must be deleted or the device securely destroyed as soon as the ePHI is no longer required to be stored on the device or media.

   f. *Back-up Tapes:* Backup tapes used to store ePHI from servers must be encrypted. A secure accountability process must be implemented to store the tapes securely whether on or off site to prevent theft or loss of the tapes.

   g. *Remote Access:* All remote access into the department's network and systems must utilize an encryption mechanism to secure the connection and data from unauthorized access. Departments shall use standards such as a secure socket layer (SSL), Virtual Private Networking (VPN) or other equivalent alternative technology.

   h. *Wireless Networks*: Wireless networks used to transmit ePHI shall be secured using strong encryption standards. Wireless Equivalent Privacy (WEP) shall not be used as the encryption standard. Wireless networks used for guest or public access are exempt from this requirement if the network is segregated from secure wireless networks in order to prevent unauthorized access.

2. *Emails*: Departments shall adopt policies and procedures to protect PHI when transmitted via email. The following minimum requirements must be addressed:

   a. Departments must ensure an automated confidentiality notice appears on all emails.

   b. PHI must never be included in the subject line of an email and only the minimum amount necessary may be included in the body of an email.

   c. PHI sent outside the County network must be encrypted through a solution approved by the Information Services Department (ISD).

   d. Prior to sending PHI via email, the sender must verify the recipient's email address.

Retention: Documentation required for compliance with this SP shall be retained for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

This Standard Practice shall not be construed as relieving departments of their responsibility to develop full and complete departmental policies, procedures, and practices necessary to expand and tailor this overall County Policy to the particular needs of their departments.

LEAD DEPARTMENT
Human Resources