Better Health for All

COUNTY OF SANTA CLARA
Health System

DATE: February 10, 2023

TO: All Valley Health Plan Staff

FROM: Lisa Pfeifer, Chief Compliance Officer, DocuSigned by: Pfeifer, Lisa 49EB3E6DAB5A443...
County of Santa Clara Health System

SUBJECT: **Safeguarding and Protections for Data - Valley Health Plan**

REFERENCES: Health Insurance Portability & Accountability Act (HIPAA), Public Law 104-191
Privacy Rule (45 C.F.R. Parts 160 and 164, subpart A and E)
Security Rule (45 C.F.R. Parts 160 and 164, subpart A and C)
42 C.F.R. Part 2
HIPAA Enforcement Rule – Administrative Simplification
Civil Monetary Penalties 45 C.F.R. §160.400 *et seq.* and Criminal Penalties
45 USC, Section 1320d-6
American Recovery & Reinvestment Act – HITECH Act
California Constitution, Article I, Section 1
California Civil Code Section 1798 *et seq* Information Practices Act
California Civil Code Section 56.10-56.16, Confidentiality of Medical Information Act
California Welfare & Institutions Code Section 5328
California Health & Safety Code Section 1280.15
County of Santa Clara Health System Privacy Policies
National Committee for Quality Assurance (NCQA) and Health Equity Standards (2022)
CSCHS #585.17 Safeguarding Protected Health Information
CSCHS #585.26 Privacy Definitions

DEFINITIONS:
See *CSCHS Policy #585.26 Privacy Definitions.*

BACKGROUND
Valley Health Plan collects and maintains protected health information (PHI) and electronic protected health information (ePHI) data about its patients and plan members. HIPAA regulations, NCQA requirements and California state law limit the access, use, and disclosure of such PHI/ePHI by VHP workforce members. VHP has created policies and procedures to help workforce members secure and protect the PHI/ePHI of our patients and plan members.

Federal and state laws and regulations protect the confidentiality of PHI/ePHI data and specify when VHP can access, use, or disclose PHI/ePHI. In order to protect the privacy and confidentiality of our patients' and health plan members' PHI/ePHI and to comply with federal and state laws and regulations, all VHP workforce members are required to comply with the provisions of this policy.

POLICY

Valley Health Plan (VHP) is part of the County of Santa Clara Health System (CSCHS) and designated as part of the County of Santa Clara's Covered Entity. As such, VHP and its Workforce Members shall take reasonable steps as described in *CSCHS Policy #585.17 Safeguarding Protected Health Information*, and *CSCHS Policy #585.26 Privacy Rule Definitions,* to safeguard and protect all enrollee personal and protected health information (PHI), including identifying demographic information such as race/ethnicity, language preference, gender identity, sexual orientation data, and electronic PHI (ePHI) from any unlawful or unauthorized access, use or disclosure which otherwise may result in violation of the federal and state privacy regulations.

VHP Workforce Members and contractors must also reasonably safeguard PHI/ePHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required access, use or disclosure. PHI/ePHI that must be safeguarded may be in any medium, including paper, electronic, verbal, and visual representations.

VHP Workforce Members and contractors will prevent unauthorized access, use or disclosure of patient information by establishing and implementing appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical and personal information against unauthorized access, use or disclosure.

This policy outlines how VHP stores, disposes, reuses, and protects systems and devices (including, but not limited to diskettes, CD, tapes, mobile applications, portable drives, laptops, and secure portals) that contain PHI from unauthorized access; addresses permissible and impermissible use, disruption, modification, or destruction and to assure confidentiality, integrity, and limiting employee access and for terminating access of employees who are no longer authorized to have access.

PROCEDURE:

Responsible Party	**Action**
VHP Workforce Members	**PHI on Paper** Files and documents containing PHI must be adequately safeguarded against unauthorized access, use or disclosure. Safeguards include:

- **Storage:** Lock all files and documents being stored (short term and long-term storage) or develop reasonable procedures to minimize access to the PHI in such files and documents. Safeguards must include, but are not limited to:
  - Lock all lockable desks, file rooms, file cabinets, and open area storage systems.
  - For all desks, file rooms, file cabinets and open area storage systems that cannot be locked, develop reasonable procedures to minimize access to PHI.
- **Disposal/Destruction:** Label any storage area or container holding files and documents awaiting disposal or destruction. Safeguards must include, but are not limited to:
  - Ensure that desk-site waste/shred containers are appropriately labeled and disposed of on a regular basis.
  - Ensure that centralized waste/shred containers are clearly labeled, locked, and placed in a lockable storage room.
  - Ensure that all storage rooms containing PHI awaiting disposal are locked after business hours and whenever authorized staff is not present.

Verbal Communications of Data

Protect the privacy of verbal exchanges or discussions of PHI/ePHI (e.g., appointment reminder phone calls, etc.), regardless of where the discussion occurs.

- Discuss PHI only with those who have a need to know and are authorized to receive the information.
- Discuss PHI only in ways and places where patients, visitors and Workforce Members who are not involved in the patient's care are not likely to overhear. For this reason, public areas such as elevators and cafeterias are not appropriate for such discussions.
- Speak quietly and with awareness that PHI could be overheard.
- Use the minimum amount of information necessary for patient safety when calling out patient names in reception areas. For example, if feasible use only title and last name, or just first name.
- Minimize the amount of PHI disclosed when leaving appointment reminders or other types of messages for patients.

Visual PHI/ePHI

Take reasonable steps to ensure that visible PHI (e.g., patient charts, sign in sheets, whiteboards, etc.) are shielded from unauthorized use and disclosure, such as the following:

- **Computer screens.** Safeguards include, but are not limited to:
  - Use of privacy screens or other computer screen overlay devices that shield information on the screen from persons other than the authorized user.
  - Placement of computer workstations out of the visual range of persons other than the authorized user.
  - Clearing information from the screen when the computer workstation is not in use.
  - Lock-down of computer workstations when not in use.
- **Electronic and paper documents.** Ensure minimum necessary access to PHI/ePHI, including but not limited to, PHI/ePHI located on:
  - Desks;
  - Fax machines;
  - Photocopy machines;
  - Portable electronic devices (e.g., laptop computers, palm pilots, flash/jump drives, etc.);
  - Computer printers;
  - Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.);
  - Patient charts;
  - Sign in sheets;
  - Diskettes;
  - CDs;
  - Tapes;
  - Mobile applications; and
  - Secure Portals

Electronic PHI

- All electronic media (laptops, flash/jump drives, PDAs, etc.) must be loaded with the County encryption software to ensure the data is secure in case of loss or theft.
- Always secure electronic media if it is not in your possession. <u>Do not</u> leave PHI/ePHI or devices with PHI/ePHI in your car or trunk, lock it up securely when not in use, etc.

- PHI should never be stored on non-County owned computers, laptops, cloud drives or computer readable storage media or personal cloud drives.
- When ending a computer session, Workforce Members must wait for confirmation of the log-out command before leaving the workstation.

All CSCHS Workforce Members shall comply with applicable Health System policies and procedures related to the security of PHI and other confidential information maintained in electronic format.

Transporting PHI

All Workforce Members must get their manager's approval prior to transporting PHI/ePHI for work-related purposes.

- Workforce Members who must take PHI offsite to perform an authorized activity or duty shall use appropriate safeguards. The same requirements for protecting PHI onsite in the workplace apply when the information is offsite. Additional requirements apply to PHI taken offsite:
    - Workforce Members who take PHI offsite shall keep the PHI fully secured and in their physical possession during transit. Workforce Members shall never leave PHI unattended in any mode of transport, even if the mode of transport is locked. This does not apply to couriers who transport laboratory specimens from multiple client sites to the reference laboratory, as long as the specimens are transported in locked containers.

PHI taken offsite shall be secured at that location, stored in a suitable locked receptacle when not in use or unattended.

- Store all forms of media containing PHI/ePHI (paper format or encrypted electronic media) in a locked case or tote.
- Keep laptops or mobile devices and all media containing PHI/ePHI in your personal possession during transport.
- <u>Do not</u> leave laptops or other mobile devices unattended.

Staff Can Use and Disclose a Members' PHI for Treatment, Payment, and Health Care Operations

Use and disclosure includes face-to-face communications, faxed communications, telephone communications, and possibly email communications. These disclosures of PHI are permissible as long as staff takes proper measures to safeguard the information consistent with this policy. VHP does not create a significant amount of PHI, as most PHI is generated as a result of a Provider visit or a hospitalization. All eligibility and enrollment data is PHI as are grievance documents, provider dispute records, authorizations, claims and other VHP documentation needed to perform its duties. Access and use of this information is only to perform required functions by authorized VHP staff.

1. **Disclosures outside VHP:** Staff may disclose PHI outside of VHP for purposes of treatment, payment, or healthcare operations. This includes disclosures to business associates who have a current contract with the County to perform a function or service on behalf of VHP. Consultants may have limited access, but they are required to identify what type of data they need in the contract and sign a business associate agreement that outlines the restrictions for their use and access to PHI.
2. **Uses within VHP:** Staff can discuss a member's PHI with co-workers within VHP if such use is consistent with their professional duties and the co-worker has a professional need to know the information.

All other disclosures must be specifically authorized by the member or approved by VHP Compliance Department and/or County Counsel.

Impermissible Uses of Data

Impermissible Uses: Any uses of data not explicitly listed above or approved by Compliance and/or County Counsel would be considered impermissible use. Impermissible use includes but are not limited to underwriting, denial of services, coverage, and benefits.

Issued: 2/10/2023

Revised: