POLICY AND PROCEDURE	
TITLE: Safeguarding Protected Health Information/ Personally Identifiable Information	
DEPARTMENT POLICY OWNER: Compliance	**POLICY #:** HPA42
IMPACTED DEPARTMENT: Check all departments impacted by this policy	
☐ Administration ☐ Claims ☐ Compliance ☐ Customer Service ☐ External Affairs ☐ Facilities ☐ Finance	☐ Human Resources ☐ Information Technology ☐ Marketing ☐ Medical Management ☐ Provider Networks ☐ Project Management x ALL
EFFECTIVE DATE: 05/15/2019	**REVIEW/REVISION DATE:** 04/19, 12/20, 04/21
COMMITTEE APPROVAL DATE: PRC: 05/19, 07/20, 04/21 Compliance Committee: 07/19	**RETIRE DATE:**

PRODUCT TYPE:	REPLACES:
Medi-Cal	IT15 – Protection for Workstation and Electronic Access IT18 – Application Logging Procedure IT21 – Device and Media Controls IT22 – Maintaining Integrity and Security of ePHI IT33 – Use of Electronic Mail (email) IT34 – System Monitoring and Activity Review IT203 – Safeguarding ePHI HPA06- Administrative Safeguards for PHI HPA26- Use and Disclosure of PHI HPA27 Disclosure for Judicial Proceedings HPA28 Disclosure for Law Enforcement Purposes HPA29 Disclosure for Specialized Government Functions HPA30 Disclosure for Health Oversight Activities HPA31 - Protection of Protected Health Information Belonging to Terminated or Deceased Member HPA32 Disclosure to Personal Representatives HPA33 Verification of Identity for Disclosure of PHI HPA36 Disclosure of Member PHI HPA38 Disclosure to workers compensation carriers HPA39 De-Identification of PHI

I. PURPOSE

The Health Plan of San Joaquin (HPSJ) shall reasonably safeguard protected health information (PHI) contained in member records from any intentional or unintentional use or disclosure not permitted under the Health Insurance Portability

and Accountability Act (HIPAA) Privacy and Security Rule and Confidentiality of Medical Information Act (CMIA). This Policy and Procedure (P&P) addresses privacy and security controls implemented to safeguard this confidential information.

II. POLICY

A. This HPSJ implements administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS, in compliance with 45 CFR sections 164.308, 164.310, 164.312 and 164.502(f), and to prevent use or disclosure of PHI other than as provided for by this Agreement (DHCS Contract Exhibit G, Provision C.2).

B. HPSJ may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances, per 45 C.F.R. § 164.508(b)(4).

C. The HPSJ will control access to PHI and ensure it is handled in an appropriate manner. Violations of this policy shall be reported to the Compliance Department either in person, via email or anonymously as described in Policy and Procedure (P&P) CMP01 Response and Prevention of Compliance Violations.

D. The HPSJ may disclose to a family member, of a deceased HPSJ Member, who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity

E. Members have the right to revoke an Authorization, provided that the revocation is in writing, except to the extent that the HPSJ has already acted based on the Authorization.

F. The HPSJ shall comply with the Department of Health Care Services (DHCS) Contract to, “use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of DHCS, provided that such use or disclosure would not violate the HIPAA regulations” (DHCS Contract Exhibit G.III.A).

G. The Chief Compliance Officer is responsible for ensuring that non-routine

disclosures of PHI, including sensitive services, are permissible and necessary. HPSJ licensed health care personnel are aware of activities in which they are permitted under HIPAA to disclose PHI without permission from the member

H. Electronic Communications and Transmissions

1. The workforce must encrypt email messages containing Confidential Information before transmitting.
2. The workforce must use an encrypted tunnel or Virtual Private Network (VPN) or protocols such as Secure File Transfer (SFTP) or Secure Socket Layer (SSL) when transmitting Confidential Information over a public network (i.e., the Internet).

I. Electronic Media and Storage

1. HPSJ prohibits storing PHI/ePHI on local desktop hard drives.
2. HPSJ must encrypt ePHI stored on portable devices and media (i.e., laptops, portable storage, and tapes).
3. HPSJ must encrypt hard drives containing ePHI when encryption is appropriate and reasonable. In situations where HPSJ, after careful assessment and consideration, determines that encryption is not appropriate or reasonable, HPSJ must implement an alternative safeguard that provides the same level of protection as encryption.
4. HPSJ must govern the movement of hardware, storage, and electronic media containing ePHI.
5. HPSJ must sanitize electronic media containing ePHI prior to reuse.
6. HPSJ must sanitize or physically destroy electronic media containing ePHI prior to disposal.

J. HPSJ's encryption approaches and procedures must use a FIPS 140-2 compliant encryption algorithm.

K. Audit Logging and Review

1. HPSJ must log or record activities of information systems that create, receive, maintain, or transmit ePHI.
2. HPSJ must periodically examine activity and audit logs of information systems that create, receive, maintain, or transmit ePHI.

L. Computers and Electronic Devices

1. Computers and electronic devices that create, receive, maintain, or transmit ePHI must

    a. Include protection from malicious software including applicable critical OS patches, service packs, or service updates.

    b. Have encrypted hard drives or be protected by compensating controls that provide equivalent protection as encryption.

    c. Automatically lock after a period of inactivity.

    d. Be limited to Users and processes with the minimum privileges necessary to fulfill their duties or functions.

2. HPSJ must regularly maintain network-connected computers or electronic devices including the application of critical security patches within 30 days of notification by the IT Security or the vendor. HPSJ applies other patches not designated as critical on a normal maintenance schedule, which may depart from the above.

III. PROCEDURE

A. The Chief Compliance Officer (Privacy officer) and Security Officer shall be responsible for the administrative safeguards of PHI/ePHI.

a. Hardcopy documentation which contains PHI.
    i. Documents containing PHI will be stored in locked cabinets or secure locations, in work areas.
    ii. Large amount of documentation containing PHI will be mailed in a secure format with tracking and signature requirements. This information will be maintained and stored in compliance with the record management retention program.
    iii. Permanent destruction of documentation with PHI is carried out in accordance with P&P CMP02 Records Management and Retention.

b. Oral communications
    i. PHI will only be discussed in appropriate work areas, not in collective public/areas.
    ii. HPSJ Member interviews and discussions will be conducted in secure areas (such as, but not limited to Member rooms may be used).

c. Electronic Communications and Transmissions

i. Electronic Messages (email)

1. HPSJ uses email encryption methods (i.e., using the "Send Secure" desktop Outlook or "Protect" Office 365 Outlook buttons) to encrypt emails to recipients outside of the hpsj.com domain.

2. Users refrain from including PHI in the subject field of an email.

3. The enterprise email system reviews and evaluates outbound email messages against a set of PHI criteria and automatically encrypts any unencrypted message matching such criteria.

ii. HPSJ uses encrypted tunnels or protocols such as VPN, SSL, or SFTP for electronic communications or transferring files containing ePHI over public networks. When vendors or partners are not equipped to support SFTP, HPSJ uses applications such as PGP (Pretty Good Privacy) to encrypt the file before transferring over an unencrypted tunnel.

iii. HPSJ workforce and vendors/partners use VPN or Citrix during any remote user interactive sessions that transmit ePHI over public networks.

iv. Web applications use Transport Layer Security (TLS) to ensure authentication and integrity of ePHI transferred over HTTP as HTTPS.

d. Electronic Media and Storage

i. IT Operations has procedures to ensure that portable media automatically encrypts stored data.

ii. When storing of ePHI is necessary, Users store ePHI to network drives.

iii. IT Operations disables USB ports on desktop computers.

iv. Users may request the ability to write to Portable Storage with approval and in accordance with this policy

v. IT Operations issues USB drives that automatically encrypt to users authorized to have their USB drive enabled.

vi. HPSJ records the receipt, deployment, and destruction of all electronic media containing ePHI as specified in the IT Operations standards and procedures.

vii. HPSJ sanitizes or securely erases electronic media containing ePHI prior to re-use in a different system or by a different owner, in accordance with IT Operations standards and operating procedures.

viii. HPSJ securely destroys, prior to disposal, all electronic media containing (or suspected of containing) ePHI by physical destruction or by sanitizing i n accordance with the IT Operations standards and operating procedures.

e. Encryption

i. HPSJ has mechanisms to encrypt and decrypt information whenever deemed appropriate.

ii. HPSJ uses the following factors to assess the appropriateness and reasonability of encrypting Data-at-rest:

1. The application's ability to function on a server with an encrypted disk drive
2. The ability of the application or server to support mechanisms to encrypt/decrypt data
3. The impact of encryption on the application's performance and functionality
4. The cost of additional resources to implement or support encryption

iii. In situations where HPSJ determines that encrypting Data-at-rest is not reasonable or appropriate, HPSJ implements all or a combination of the following compensating controls:

1. House servers in secure server rooms or data centers
2. Log all access to the server rooms or data centers

3. Follow security best practices for hardening servers
4. Implement Intrusion Detection and Prevention (IDS/IPS) or Data Loss Prevention (DLP) systems.

f. Audit Logging and Review

i. HPSJ Information systems log or record activity such as failed authentication attempts, configuration changes, process startup, shutdown, or restart, and malware or suspicious activity detection.

ii. HPSJ has mechanisms to review logs for unauthorized access.

g. Computers and Electronic Devices

i. HPSJ safeguards Information Resources that have access to Confidential Information using perimeter security devices such as firewalls.

ii. IT distributes computers with the ability to write or access Portable Storage disabled.

iii. Computers include software to protect against malicious software (i.e. anti-virus software) and mechanisms to install new releases of the Operating System (OS) security and critical updates.

iv. IT has P&Ps for vulnerability and patch management. The HPSJ risk- based approach for prioritizing critical patches ensures timely and appropriate application of patches that address application, system, and network device vulnerabilities.

v. Computers and electronic devices with access to ePHI automatically enable a password-protected screen saver after 10 minutes of inactivity (idle time).

h. Obtaining an Authorization from a Member or Personal Representative

i. Upon receiving a request as described in III.A., Members are required to complete an Authorization. The Member may submit the Authorization via mail or complete it at an HPSJ office. HPSJ Workforce may obtain the Authorization from Intranet/Forms/HIPAA.

An Authorization must be a separate document and may not be combined with any other type of form.

ii. Authorization will only be mailed to the Member at the address currently maintained in our Member database. Mailing an Authorization to an alternative address is strictly prohibited.

iii. When completing an Authorization form at an HPSJ office, the Customer Service Workforce member asks the HPSJ Member for photo identification and documents in a call log.

iv. Personal Representatives of non-SPD Members must submit or show proof of their legal authority to complete an Authorization for the Member as described in policy HPA32 Disclosure to Personal Representative. Examples of valid proof include: birth certificate of a physically or mentally disabled Member demonstrating that the Personal Representative is the parent, court or county documents indicating that the Personal Representative is permitted to seek and obtain medical care for the member, power of attorney granting the Personal Representative the right to act on behalf of the member, or caregiver Authorization Affidavit citing the Personal Representative as the caregiver.

i. SPD Members are not required to complete an Authorization form in the case of physical or mental incapacity. Staff may utilize data submitted by DHCS and stored to identify a Personal Representative. All other proof must be approved by the Compliance Department.

j. In the event HPSJ must seek an authorization from the Member or Personal Representative, HPSJ personnel will complete all sections of the Authorization form before providing to the Member or their Personal Representative for signature.

k. In the event that HPSJ seeks the authorization from the Member or Personal Representative, a copy of the signed authorization will be provided to the Member or Personal Representative. In cases where the Member or Personal Representative seeks the authorization, a copy may be provided on request.

l. The HPSJ may disclose the PHI of a deceased individual in the following instances.

i. In the case of deceased Members, for PHI requested within 50 years of the Member's death, the HPSJ shall considers an executor,

administrator, or other person who has authority to act on behalf of the deceased member as their personal representative. Such representatives must provide legal documents supporting their legal authority.

ii. To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.

iii. For research that is solely on the PHI of decedents.

iv. To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

v. To a family member or other person who was involved in the individual's health care or payment for care prior to individual's death, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the HPSJ.

m. Review of Authorizations

i. All submitted HPSJ Authorization forms are reviewed by the Customer Service Department prior to using or disclosing a Member's PHI in the manner indicated on the Authorization form.

ii. All non-HPSJ Authorization forms are reviewed by the Compliance Department prior to using or disclosing a Member's PHI in the manner indicated on the Authorization form. An Authorization is deemed defective and invalid under any of the following circumstances:

1. The Authorization is requesting that the Member's PHI be disclosed for purposes unrelated to the administration of the Medi-Cal program.

2. The Authorization form was signed by the Personal Representative of a minor, e.g., parent, but PHI can only be used or disclosed with the minor's permission as defined under the State of California Family Code.

3. Any elements on the form are incomplete.

4. The expiration date has passed or an expiration event is known by HPSJ to have occurred.

5. A valid Authorization was later revoked by the Member.

6. Any material information provided in the Authorization form that is known by HPSJ to be false.

iii. Any restrictions or prohibitions noted by the Member or their Personal Representative, including those related to sensitive services, are documented by the Compliance Department under the Personal Representatives and Alert sections of the Member Module.

n. Revocation of an Authorization

i. A Member, or Personal Representative, has the right to revoke an Authorization at any time. The revocation must be requested in writing.

ii. The HPSJ takes all necessary steps to honor and comply with a revocation unless the HPSJ has taken action in reliance thereon.

o. Documentation

i. The Member, or Personal Representative, is provided with a copy of a signed Authorization form when HPSJ solicits the Authorization.

ii. The Compliance Department retains all valid or invalid Authorization forms, and any subsequent revocations.

iii. Authorization forms and revocations are retained in accordance with CMP02 Records Management and Retention.

iv. Specialized Government Functions

v. Requests are reviewed and responded to by the Compliance Department.

vi. Accepted requests are limited to those authorized by 45 CFR 164.512(k).

vii. The Compliance Department verifies the officials who request access to Member PHI while on the HPSJ premises by asking for appropriate identification.

viii. The Compliance Department mails materials in response to officials in an envelope marked “confidential”, or via fax

B. ATTACHMENT(S)

A. Glossary of Terms Link

C. REFERENCES

a. 45 CFR Part §160 and §162
b. 45 CFR 164.308 (a)(1)(ii)(D) - Information System Activity Review
c. 45 CFR 164.310(d)(1) – Device and Media Controls
d. 45 CFR 164.310(d)(2)(i) - Disposal
e. 45 CFR 164.310(d)(2)(ii) – Media Re-use
f. 45 CFR 164.310(d)(2)(iii) – Accountability
g. 45 CFR 164.312(b) - Audit Controls
h. 45 CFR 164.312(e)(1) – Transmission Security
i. 45 CFR 164.312(e)(2)(i) – Integrity Controls
j. 45 CFR 164.312(e)(2)(ii) – Encryption
k. 45 CFR 164.312(a)(2)(iv) – Encryption and Decryption
l. 45 CFR 164.502(f)
m. CA Civil Code 56 (CMIA)
n. CMP01 Response and Prevention of Compliance Violations
o. CMP02 Records Management and Retention
p. Compliance (Internal Audit and Risk Management) Program Plan
q. DHCS Contract Exhibit G, Provision C.2.
r. FIPS PUB 140-2 – Security Requirements for Cryptographic Modules
s. Health Information Technology for Economic and Clinical Health Act (HITECH Act)
t. HPA08 Mitigation
u. HPA33 Verification of Identity
v. HR11 Corrective Action
w. IT33 Email
x. NIST Special Publication (SP) 800-53 Revision 4, Security, and Privacy Controls for Federal Information Systems and Organizations

D. REGULATORY AGENCY APPROVALS

Per HPSJ's agreement with The Department of Health Care Services (DHCS), HPA42 is approved for implementation due to being under review past 60 days.

E. **REVISION HISTORY**

STATUS	DATE REVISED	REVISION SUMMARY
Proposed	01/31/2019	Combined content from existing policies and added content to align with the HIPAA Security Rule
Finalized	04/02/2019	Approved by PSOC
Revised	01/13/20	Added Policy and Procedures Glossary
Revised	02/10/20	Combined HPA06 administrative safeguards and portions of HPA31 Protection of PHI for deceased members into IT203. Policy title changed from IT203 to HPA42, moving policy owner from IT to Compliance. Incorporated and updated purpose, policy and procedure.
Revised	02/25/20	Formatting and header changed.
Revised	12/11/20	Combined policy HPA26 into HPA42. AG
Revised	04/05/21	Reviewed policy for accuracy.