POLICY AND PROCEDURE	
Policy # and TITLE: HPA07 Reporting and Mitigating Suspected Privacy & Security Incidents and Breaches	
Primary Policy owner: Compliance	**POLICY #:** HPA07
Impacted/Secondary policy owner: Select the department(s) that are responsible for compliance with all, or a portion of the policy or procedure as outlined	
1) ☒All Departments 2) ☐Accounting & Finance (FIN) 3) ☐Administration (ADM) 4) ☐Care Management (CM) 5) ☐Claims (CLMS) 6) ☐Community Marketplace & Member Engagement (MAR) 7) ☐Compliance (CMP and HPA) 8) ☐Configuration (CFG) 9) ☐Cultural & Linguistics (CL) 10) ☐Customer Service (CS)	11) ☐Facilities (FAC) 12) ☐HEDIS/NCQA (QI) 13) ☐Human Resources 14) ☐Information Technology / Core Systems (IT) 15) ☐Pharmacy (PH) 16) ☐Project Management Office 17) ☐Provider Contracting (CONT) 18) ☐Provider Services (PS) 19) ☐Quality Management (QI) 20) ☐Utilization Management/ BH (UM)
PRODUCT TYPE: ☒Medi-Cal	**Supersedes Policy Number:** HPA08

I. PURPOSE

To outline the reporting and mitigating processes for handling Privacy or Security Incidents, Breaches of Protected Health Information/Personal Information (PHI/PII), and/or other unauthorized access, use, or disclosure of PHI/PII.

II. POLICY

A. San Joaquin County Health Commission ("Commission"), operating and doing business as Health Plan of San Joaquin and Mountain Valley Health Plan ("Health Plan") must immediately report suspected or confirmed Privacy or Security Incidents, Breaches of PHI/PII, other unauthorized access, and unauthorized use or disclosure of PHI/PII (collectively known as "HIPAA Incidents") to regulators as required by the Health Insurance Portability and Accountability Act (HIPAA),

Privacy, Security and Breach Notification Rules, 45 CFR Parts 160 and 164, California Civil Code sections 1798.29, and contractual or regulatory requirements.

B. The Privacy Officer or designee and/or IT Security Officer must report HIPAA Incidents to the Privacy and Security Oversight Council (PSOC) as well as to the appropriate federal and state agencies.
C. The following are ways to report an incident: SharePoint link, supervisors, managers, or Executive Team, Compliance Team Members, via fax, via email, via phone, anonymously, or through physical onsite Compliance boxes.
D. The Health Plan must provide written reports of unthwarted HIPAA incidents to DHCS in accordance with this policy.
E. Suspected HIPAA Incidents will be reported to DHCS by the Health Plan using the DHCS Portal. The Health Plan will notify individual Members whose PHI/PII has been or believed to have been accessed, acquired, used, or disclosed as a result of a breach, determined by DHCS.
F. The Health Plan must not require individuals to waive their rights as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits. [1]
G. The Health Plan must delay notification if a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security. [2]
H. The Health Plan's Program Integrity Unit provides oversite and enforcement of this policy under supervision of the Privacy Officer and It Security Officer.
I. The Compliance Officer and Privacy Oversite Counsel reviews this policy annually and revises as necessary.

III. PROCEDURE

A. Discovery

A breach must be treated as discovered as of the first day when the breach is suspected or known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is a Health Plan Workforce member or other agent of The Health Plan.

---

[1] 45 CFR § 164.530(h)
[2] 45 CFR §164.412

1. The Health Plan's Workforce must report any HIPAA Incidents immediately after discovery, via the following methods:
    a. Report directly via the Share Point Link which is the online reporting application that links to https://secure.compliance360.com.
    b. Report directly to the Workforce member's supervisor, manager, or member of the Executive Team.
    c. Report directly to The Health Plan's Privacy Office or Security Officer.
    d. Report directly to any of the Compliance Management Team members.
    e. Report via email PIU@HPSJ.com.
    f. Report via fax (209) 762-4721.
    g. Report via the anonymous online reporting application at Syntrio: Llighthouse Reporting
    h. Report via the physical Compliance boxes located within the Health Plan's facilities.
    i. Report via the Compliance Hotline 1-800-822-6222.
    j. Management Team members.
2. The Health Plan's Department(s) and Workforce shall immediately report to the Compliance Department using one of the described methods listed above, upon the discovery of a suspected Privacy or Security Incident or Breach. Failure to report will constitute a violation of P&P.
3. The Health Plan's Workforce is required to work with the Compliance Department to investigate and remediate the HIPAA Incidents upon request and adhere to the following requirements.
    a. Adherence to the processes and timeline outlined in the "Service Level Agreement for Privacy Incidents Remediation Requirements" during the investigation period.
    b. Adherence to the remediation roles and responsibilities outlined in the Desk Level Procedure Compliance and Business Owners Remediation Process for Privacy Incidents.
    c. The failure to comply with may result in applicable disciplinary

actions per HPA09 HPSJ Workforce Sanctions.

4. Providers, Contractors, Subcontractors, Downstream Subcontractors, including Business Associates (Collectively known as "Third-Party") shall immediately report:
    a. Via email notification incidents@dhcs.ca.gov. The Third-Party is required to carbon copy to The Health Plan's PIU inbox piu@hpsj.com in the same email.
    b. Via a phone call (866) 866-0602
    c. When either Portal reporting or phone call method is used, the Third-Party is required to send an immediate communication providing the same information related to the incident via the Health Plan's PIU inbox piu@hpsj.com email address.
5. Third-parties Requirement to Report
    a. More detail is covered on third-party reporting obligations in HPA05 – Business Associates.
    b. The Health Plan informs and educates third parties' reporting obligations as outlined in the BAA.
    c. The Health Plan reports on behalf of Third Parties, the Incident to DHCS, within 24 hours when it is aware of such Incident, should the Third-Party fail to report timely.
    d. The Health Plan also fulfills subsequent reporting requirements should the Third-Party fail to adhere to the subsequent reporting requirements.
    e. The Third-Party's failure to adhere to the regulatory reporting requirements as outlined in the BAA may result in actions assessed by the Health Plan which may include up to termination of contract.

B. The Health Plan Member Reporting

1. A member may file a HIPAA violation complaint with a Customer Service representative via telephone or mail. The address and phone number are provided on the Notice of Privacy Practices. They may also submit through our public website Syntrio: Lighthouse Reporting.
2. The Health Plan processes the complaint in the same manner as

described in this Policy.

C. Reporting of HIPAA Incidents to Regulators

1. The Health Plan's Compliance Department, must investigate notify, and report the discovery of HIPAA Incidents in accordance with the following guidelines:
2. Breach:
    a. The Compliance Department must notify DHCS **immediately** through the DHCS Portal upon the discovery of a security breach of PHI/PII in computerized form if the PHI/PII was, or is reasonably believed to have been, acquired by an unauthorized person, or upon the discovery of a suspected privacy or security incident that involves data provided to DHCS by the Social Security Administration.
    b. Notify the DHCS Contract Manager, DHCS Privacy Officer and DHCS Information Security Officer utilizing the DHCS Privacy Incident Report (PIR) template.
3. Suspected HIPAA Incident:
    a. Notify, **within 24 hours,** through the DHCS Portal of any suspected privacy or security incident, intrusion, or unauthorized access, use or disclosure of PHI or PII in violation of the 2024 DHCS Contract between the Health Plan and DHCS.
4. Investigation:
    a. Upon discovering a HIPAA Incident, the Compliance Department initiates the investigation immediately.
    b. Submit investigation updates through the DHCS Portal within **72 hours** of discovery.
    c. Submit the complete PIR details through the DHCS Portal within **ten (10) working days** of the discovery of the breach or unauthorized use or disclosure. If more time is needed to complete the investigation, then the Health Plan will request an extension from DHCS and during the extension period submit weekly updates to DHCS until the investigation is complete. Upon discovery of a HIPAA Incident, The Health Plan must take:
        i. Prompt corrective action to mitigate any risks or

damages involved with the breach and to protect the operating environment.

ii. Any action pertaining to such unauthorized disclosure is required by applicable federal and state laws and regulations.

5. Notification of Members:
    a. The Health Plan must notify each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.
    b. The notifications must be made without unreasonable delay and in no event later than 60 calendar days after discovery of a breach.
    c. DHCS must review and approve the content of the notification.
6. Notification of Media:
    a. Media notification is required for Breaches for unsecured PHI involving more than five hundred (500) individuals.
    b. The notifications to the media must be made without unreasonable delay and in no event later than sixty (60) calendar days after the discovery of a breach.
7. Notification of Department of Health and Human Services (DHHS)Secretary, Office of Civil Rights:
    a. Notification of the DHHS Secretary is required for Breaches of unsecured PHI involving more than five hundred (500) individuals.
    b. For Breaches of unsecured PHI involving less than five hundred (500) individuals, The Health Plan must maintain a log or other documentation of such breaches and no later than sixty (60) days after the end of each calendar year, provide the log to the DHHS Secretary.

D. Determining which HIPAA Incidents are Reportable versus Non-reportable to DHCS.
    1. All reasonably confirmed breaches must be reported to DHCS, however, not every HIPAA Incident is a breach. There are three exceptions:

a. Unintentional acquisition, access, or use
b. The inadvertent disclosure to an authorized person
c. The inability to retain PHI.
d. The "HPSJ PIR Decision Tree" is a guideline to determine which privacy or security incidents should be classified as reportable versus non-reportable to DHCS.

E. Law Enforcement Delay

1. If a law enforcement official states to the Health Plan that a notification, notice, or posting required would impede a criminal investigation or cause damage to national security, the Health Plan must:

a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the period specified by the official; or
b. If the statement is made orally, the Health Plan will document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement. [3]

IV. ATTACHMENT(S).

A. DLP - *Compliance and Business Owners Remediation* Process for Privacy Incident.
B. DHCS Medi – Cal Managed Care Plans Definitions (Exhibit A, Attachment I, 1.0 Definitions)
C. DHCS Privacy Incident Report
D. Glossary of Terms Link
E. Medi-Cal Managed Care Contract Acronyms List (Exhibit A, Attachment I, 2.0 Acronyms)
F. SLA for Privacy Incidents Remediation Requirements

V. REFERENCES

A. 45 CFR Parts §160, §162 and §164.412
B. California Civil Code §56 - §56.37 Confidentiality of Medical Information

[3] 45 CFR §164.412

Act

C. CMP01 Response and Prevention of Compliance Violations
D. CMP DP009 Privacy Incident Intake and Reporting
E. DHCS Contract Exhibit G
F. HPA01 Privacy and Security Oversight Council (PSOC)
G. HPA09 HPSJ Workforce Sanctions
H. HPSJ Business Associate Agreement
I. HPSJ PIR Decision Tree
J. Medi-Cal Notice of Privacy Practices
K. Privacy Incidents FAQs
L. SLA for Privacy Incidents Remediation Requirements

VI. REVISION HISTORY

*Version 001 as of 01/01/2023

Version*	Revision Summary	Date
000	03/03, 07/03, 04/05, 01/09, 05/09, 06/12, 09/14, 11/18, 06/20, 07/20, 12/20, 2/21, 11/21, 10/22, 12/22, 2/23	N/A
001	Moved HPA07 onto new 2023 template	03/21/2023
002	Inputted information about SLA for Privacy Incidents Remediation Requirements under section B. Reporting of Privacy or Security Incidents or Breaches to the HPSJ	05/23/2023
003	Revised procedure for Business Associates to report breaches.	07/14/2023
004	Per 2024 DHCS Contract, added language about business associates mitigating breaches and security incidents in policy.	08/30/2023
005	Formatted content for readability.	9/21/2023
Initial Effective Date: 04/14/2003		

VII. COMMITTEE REVIEW AND APPROVAL

Committee Name	Version	Date
Compliance Committee	005	12/7/2023
• Privacy & Security Oversight Committee (PSOC)	005	11/7/2023
• Program Integrity Committee		
• Audits & Oversight Committee		
• Policy Review	005	11/15/2023
Quality and Utilization Management		
• Quality Of Care		
• Grievance		

VIII. REGULATORY AGENCY APPROVALS

Department	Reviewer	Version	Date
Department of Healthcare services (DHCS)	N/A	N/A	N/A
Department of Managed Care (DMHC)	N/A	N/A	N/A

IX. APPROVAL SIGNATURES

Signature	Name Title	Date
	PRC Chairperson	
	Policy Owner	
	Department Executive	

Signature	Name Title	Date
	Chief Executive Officer	

*Signatures are on file, will not be on the published copy