PRIVACY & PHYSICAL SECURITY POLICY

Calendar Year 2026

PNS | Pacific Neuropsychiatric Specialists

Contents

I. INTRODUCTION & OVERVIEW

PURPOSE

The purpose of this policy and procedure is to outline procedures for PNS's Privacy, Confidentiality, and Physical Security and best practices shared throughout the company to minimize the risk of and/or avoid breaches of confidential information and comply with federal and state privacy and confidentiality regulations.

GOALS

The Privacy & Physical Security Policy is designed to protect sensitive patient and organizational data while ensuring compliance with applicable laws and regulations. The goals of this policy are as follows:

- Protect Patient Privacy and Confidentiality by ensuring that all patient health information, including personal, medical, and treatment data, is protected from unauthorized access, use, or disclosure.
- To comply with all relevant federal, state, and local laws, regulations, and industry standards, such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and any applicable state privacy laws.
- To implement security measures and controls to prevent unauthorized individuals from accessing, altering, or disclosing Protected Health Information (PHI), ensuring that only authorized personnel have access based on job responsibilities.
- To foster an organizational culture where all employees and stakeholders are aware of the importance of privacy, confidentiality, and security, and are trained to adhere to security protocols, practices, and the organization's policies to prevent breaches.

APPLICABILITY AND SCOPE

This policy applies to all employees, contractors, and guests of Pacific Neuropsychiatric Specialists.

This policy is intended to encompass all incidents which may significantly impact business operations for Pacific Neuropsychiatric Specialists. This policy and procedure applies to all protected member information (PHI) and Personally Identifiable Information (PII), in any form (digital, softcopy, or hardcopy) and to all employees, contractors, and affiliated personnel within PNS who are involved in handling any data. When encountering a situation that has not been expressly addressed in this document, employees shall use good judgment, and the guiding principles outlined in this policy.

POLICY REVIEW & MAINTENANCE

The PNS Compliance Department shall review and modify this policy and procedure (when necessary) on an annual basis. Any suggestions, comments, or questions should be directed to the PNS Compliance Department.

II. DEFINITIONS

HIPAA Privacy Rule: Set of standards within HIPAA that address the use and disclosure of individuals' health information (PHI) by organizations subject to the Privacy Rule (e.g., covered entities) as well as standards for individuals' privacy rights to understand and control how their health information is used.

Protected Health Information (PHI): Any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

Personally Identifiable Information (PII): Any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Covered Entity: As defined by HIPAA rules, fall within 3 specific categories:

- Health plans
- Health care clearinghouses
- Health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

Business Associate: As defined by the Health Information Portability and Accountability Act (HIPAA) Privacy Rule, this is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

Need-to-Know-Basis: Also known as the "**Minimum Necessary Rule**," refers to providing only the information that is required to complete a necessary task.

Treatment: the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

Payment: For the purposes of this policy, this is related to activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Healthcare Operations: For the purposes of this policy, 'Healthcare Operations' include any of the following activities: quality assessment and improvement activities, including case management and care coordination; competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; specified insurance functions, such as underwriting, risk rating, and reinsuring risk; business planning, development, management, and administration; and business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

Personal Representatives: The person who has the authority to make health care decisions on behalf of the patient.

Sensitive Services: Medical care services related to mental health, reproductive health, sexually transmitted infections, substance use disorder treatment, and other services where disclosure of information could lead to harm or distress (in alignment with California AB1184).

Clean Desk Policy: PNS policy that requires desks be free of all paperwork when the desk is left unattended.

Head of Compliance: For the purpose of this policy, the 'Head of Compliance' is the individual designated by PNS oversee, implement, and manage the organization's comprehensive Compliance Program. This individual serves as the primary authority for ensuring that all clinical and administrative operations align with federal and state regulatory requirements, as well as internal ethical standards.

III. REFERENCES

- Health Information Portability and Accountability Act (HIPAA) Privacy Rule
- Health Information Portability and Accountability Act (HIPAA) Security Rule
- Health Information Portability and Accountability Act (HIPAA) Breach Notification Rule
- PNS Telework Policy
- PNS Telehealth Policy
- PNS Clean Desk Policy

IV. TRAINING

- **Initial Training:**
  - All employees and relevant personnel must receive HIPAA training (including training on the proper handling of PHI) either through in-person instruction during new-hire orientation or as assigned through PNS' Learning Management System (LMS) within the first 90-days of hire.

- **Refresher/Ongoing Training:**
  - All employees and relevant personnel must receive HIPAA training (including training on the proper handling of PHI) on an annual basis through PNS' Learning Management System (LMS).

- **Document Retention:**
  - Documentation of education/training activities shall be retained for a period of no less than ten (10) years.

V. POLICY

A. **PNS Commitment to Compliance with Privacy, Confidentiality, and Security.**

1. It is critical that the Company maintains the confidentiality of PHI and other information that is deemed confidential by other laws. Confidential PHI may be information in any form, e.g., written, electronic, oral, overheard, or observed. Access to all information is granted on a need-to-know basis.
2. During daily work, an employee may be exposed to information that is considered strictly confidential.
    a) This information should only be used for the treatment, payment, or healthcare operations related to a patient.
    b) This information should not be discussed with anyone, including: other clients, co-workers, other families, family, or friends.
    c) An employee must be alert to others overhearing professional discussions regarding confidential information and employees should refrain from having such conversations where they can be unintentionally overheard.

B. **Designation of a Privacy Officer**

1. Pacific Neuropsychiatric Specialists will designate a Privacy Officer whom is responsible for ensuring that a healthcare organization complies with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule.
2. The Privacy Officer may be the Head of Compliance or designee.
3. The Privacy Officer's responsibilities include:
    a) Developing and implementing policies
    b) Providing training on HIPAA privacy requirements and procedures to applicable staff
    c) Regularly reviewing policies and procedures to ensure compliance with HIPAA and other privacy/confidentiality regulations
    d) Managing inquiries and complaints about patient privacy rights
    e) Investigating incidents where PHI may have been breached and reporting breaches as necessary
    f) Ensuring that patients' rights are protected in accordance with state and federal laws.

C. **Document Safeguarding**

1. All documentation or notes containing PHI must be properly filed in locked drawers or file rooms when not actively in use.
2. Documentation containing PHI that is not required to be archived, per PNS policy, must be disposed using shred bins or shred machines placed through the office. Documentation containing PHI must never be disposed of in trash cans inside or outside of the office.
3. Employees are not permitted to take documentation containing PHI outside of the office without express written permission from management unless job responsibilities of the employee require the use of PHI outside of the office.

D. **Remote Access Safeguards to PHI**

1. Refer to PNS Telework Policy, PNS Telehealth Policy, & PNS Clean Desk Policy.

E. **Enforcement**

1. Any employee that does not report a violation of HIPAA or other privacy/confidentiality regulations, policies, etc., will be subject to the disciplinary policy up to termination.
2. Unnecessary, inappropriate, or otherwise unlawful disclosure of confidential information is grounds for disciplinary action up to and including termination.
3. Sharing, disclosing, not properly disposing, or posting any documentation including PHI will result in disciplinary action up to termination.
4. All employees are responsible for reporting any violations of HIPAA or other privacy/confidentiality regulations, policies, etc., by themselves or others, to their immediate manager/supervisor or to the Head of Compliance (either directly or through the compliance hotline) within 1 business day. An employee will not be subject to retaliation for any report of wrongdoing made in "good faith" regarding a violation of another employee. An employee's report shall be kept anonymous whenever possible.

F. **Employee Separation**

1. All business records provided to employees or in an employee's possession must be returned to the Company upon termination of employment or immediately upon request by management.

G. **Employee Training Requirements**

1. All employees hired and/or subcontracted by PNS and conducting business on behalf of PNS must complete company approved HIPAA training at the time of hire and annually thereafter.
2. All employees must sign a Confidentiality Agreement upon hire (prior to receiving access to PHI/PII) and attest/sign a Confidentiality Agreement annually thereafter.

H. **Subcontractor Requirements**

1. Upon execution of a Business Associate Agreement, PNS must receive attestation form from subcontractors confirming all employees complete HIPAA training annually and allow for record audits if requested by PNS to confirm compliance.
2. Upon receipt of the attestation the form will be filed with the subcontractor's contract files and held for a minimum of ten (10) years.

VI. PROCEDURE

A. Encrypting PHI for E-mail

1. If it is required in your normal duties to send PHI by e-mail you must follow the below steps:
    a) Open a new e-mail.
    b) In the subject line type the word ***ENCRYPT***. Your subject line can include a subject, but no PHI is allowed within the subject line.
    c) Compose your e-mail as normal.
    d) Press Send.

2. An e-mail will be sent to the specified recipients. In the e-mail sent, there will be an individual link for each recipient to click. The recipient will be required to create a password to access the PNS e-mail server to review the e-mail.

B. Encrypting Data Files for Storage Devices:

1. The applications needed for properly encrypting files to 256-bit encryption are not generally installed on employee's computers. Employees that require the encryption of a file that will be stored on a CD DVD Media Storage Device, or any other hardware, must receive management approval. Management will give the request to IT, who will prepare the files to ensure the data is encrypted properly.

C. Shredding (Destroying Physical/Hardcopies) of PHI

1. All physical documentation containing PHI that is no longer needed (and has been approved to be destroyed) should be disposed of by placing the documents in bins located around the office (that are similar to the bins in the picture to the right).

2. Prior to destruction, take special care to ensure that the document containing PHI is not required to be retained (e.g., documents identified as evidence or are required to be kept/maintained due to court order).

D. System Password Security

1. At no time should you share your password with any employee including your manager, supervisor, or IT. You will be asked to change your network password at a set interval. To change your password manually follow the below steps:
    a) When logged into windows hold Control + Shift + Delete.
    b) Click on ***Change Password***
    c) Enter your old password.
    d) Enter your new password twice.
    e) Click the button to save your password.

2. Note: The above method for changing your password is to change your ***network*** password. Changing your password across other systems may have different steps unique to that system. If you have questions about changing the password within a specific system, please contact your supervisor or place a ticket with the IT Helpdesk.

E. Leaving Workstations Unattended

1. Whenever you leave your desk, your workstation must be handled by following these steps:
    a) Press Control + Alt + Delete on your keyboard.
    b) Click on "***Lock This Computer".***
    c) Lock all loose documents in a locked drawer.
        (1) PNS adheres to a '**Clean Desk Policy**.' If you plan to leave your workstation for break, lunch, or for the day you must store all PHI in appropriate designated storage areas. No loose documents/paperwork of any kind should be left on your desk when left unattended.

F. Office Visitors

1. PNS offices (including administrative headquarters, outpatient clinics, rehab facilities, clinical research, etc.) will have non-employees enter the premises, which may include patients/clients, vendors, or company partners. All visitors in each office will be recorded in a visitor log. The visitor logs are kept for 1 year. The following procedures must be followed for any person not holding a company-issued an identification badge:
    a) The visitor must sign in on the visitor log located at the front desk of each office.
    b) The visitor must sign the Visitor Facility Access Waiver
        (1) This visitor may sign the document once, which would be kept active for a period of 12 months. After the 12-month period, the waiver expires and the visitor must sign a new form.
        (2) Visitors that are guests of patients can have their form kept in the patient documents area of the EMR.
    c) The employee must notify the clinic manager of the visitor presence.
    d) Once the visitor has completed their visit, they must sign out from the visitor log.

G. File Cabinets and File Drawers

1. The company only provides locked access to employees with specific job responsibilities. If provided a key lock, it is the employees responsibility to ensure all files are locked up when not in use and the following process is followed:
    a) Employees shall analyze the documents to ensure extended use is necessary to fulfilling their role.
    b) Employees shall confirm that a designated filing location has not already been established for the documents; if so, the employee should use the designated location, unless it is not reasonably located to the employee's workstation.
    c) Employees should retain documents in their locked space for no more than two (2) business days. If it has been longer than two (2) business days, and there is no designated filing location, the employee must speak to management for authorization to keep the files at their desk, or to establish a filing location for the documents.

H. Physical Locks

1. Generally, employees are not granted access to physical keys to open doors to the office or doors within the office. If authorized to possess a key you must follow the below

procedures:

a) Keep your key in a safe location when not in use.
b) Lock doors behind you or at the end of the day where necessary. Rooms with confidential files or computer equipment (servers, hard drivers, etc.) must be locked at all times when not in use.
c) Notify leadership immediately if a key is lost or stolen.

I. Signing into Restricted Areas

1. Some areas of the office may be accessible to employees but are restricted to logged entry. Examples: file rooms, sever rooms, etc. Employees accessing these areas must follow the below procedure:
    a) When entering a restricted area, you must always sign in using the sign in log listing the time you arrived and your purpose for accessing the room.
    b) You must close the door behind you.
    c) Only access those files or equipment that are required for the task you are completing.
    d) You must log the time you are leaving the restricted area in the log. If equipment or files were removed, you must log it.
    e) Close the door behind you as you leave.

J. Use of Fax Machines

1. When using a fax machine to transmit PHI, it is important to follow the steps below to minimize the potential for unnecessary disclosures of PHI:
    a) **Sending a Fax:**
        (1) Sending party to verify the recipient's fax number and should use preprogrammed numbers where possible to minimize dialing errors.
        (2) Sending party to confirm that the recipient is authorized to receive the PHI and inform them of the impending transmission.
        (3) Sending party shall always use a fax cover sheet that includes a confidentiality notice stating that the information is protected health information and that unauthorized access or use is prohibited.
        (4) Sending party shall transmit only the minimum necessary PHI required for the intended purpose.
        (5) Use secure fax machines that are located in areas with controlled access to prevent unauthorized viewing of PHI (compliant with description in subsection F below).
        (6) Verify the successful transmission of each fax containing PHI by checking the confirmation report.
        (7) When applicable, contact the recipient to confirm that the fax was received in full and without issues.
        (8) If the recipient is unable to confirm the reception of the fax, the sending party shall notify their supervisor immediately.

b) **Fax Physical Security**
   (1) Ensure that fax machines used for transmitting or receiving PHI are in secure locations accessible only to authorized personnel.
   (2) Regularly check the fax machine for any uncollected documents and promptly secure any received faxes containing PHI.

c) **Retention and Disposal**
   (1) Store faxed documents containing PHI according to the PNS record retention policy.
   (2) Properly dispose of any paper containing PHI that is no longer needed by shredding or using other secure disposal methods by placing the documents in the designated disposal containers throughout the office.

d) **Incident Reporting**
   (1) Immediately report any faxing errors or breaches of PHI to the Head of Compliance. Follow the PNS Disaster Recovery Plan (DRP), or any other applicable incident management policies to mitigate any potential harm and comply with breach notification requirements.

e) **Destruction of Fax Documents**
   (1) Received faxes should be kept only as long as necessary. After the appropriate time period of maintenance of the records has expired, the fax documents should be destroyed by being placed in the marked PHI documentation disposal locations to be shredded.
   (2) Prior to destruction, take special care to ensure that the document containing PHI is not required to be retained (e.g., documents identified as evidence or are required to be kept/maintained due to court order).

K. Risk Assessments for Suspected Impermissible Acquisitions, Uses, or Disclosures of Protected Health Information (PHI)

1. Any employee or contractor who suspects an impermissible acquisition, use, or disclosure of PHI must immediately report the incident to the Head of Compliance.

2. **Initial Investigation**:
   a) The Head of Compliance, in collaboration with the PNS IT Team and relevant department heads, will conduct an initial investigation to gather facts and determine if a potential breach has occurred.

3. **Risk Assessment:**
   a) The Head of Compliance will conduct a risk assessment using the following criteria to evaluate the incident:
      (1) Nature and Extent of PHI Involved: Identify the type of PHI involved, including any identifiers and the likelihood of re-identification.
      (2) Unauthorized Person: Determine who received or accessed the PHI without authorization.
      (3) Acquisition, Use, or Disclosure: Assess whether the PHI was actually acquired or viewed, and the extent of the impermissible use or disclosure.
      (4) Mitigation Efforts: Evaluate any steps taken to mitigate the potential risk

to PHI, including measures to prevent further unauthorized access or use.

b) Based on the risk assessment, determine the probability that the PHI has been compromised.
   (1) If the risk assessment indicates a low probability of compromise, document the findings and rationale for not proceeding with breach notification.
   (2) If the risk assessment indicates a significant probability of compromise, follow the breach notification procedures.

4. **Documentation**:
   a) Document all findings, risk assessment criteria, and conclusions, including any actions taken to mitigate risks. Maintain these records in accordance with the PNS' documentation retention policies.

5. **Disclosure & Corrective Actions:**
   a) If a breach is determined to have occurred, follow the notification steps and procedures described for Internal Reporting and Review and External /Regulatory Reporting (below), which includes notifying affected individuals, the Office of Civil Rights (OCR), the Department of Health and Human Services (HHS), our healthcare clients, and potentially the media, as required by HIPAA.
   b) Implement corrective actions to prevent future occurrences, which may include revising policies and procedures, retraining staff, and enhancing security measures.

L. Processing PHI-Related Complaints

1. **Complaint Submission**
   a) Individuals may submit PHI-related complaints anonymously through multiple avenues:
      (1) Navex EthicsPoint
         i. PNS.ethicspoint.com
         ii. PNSMobile.ethicspoint.com (mobile phone or tablet)
      (2) Phone: (833) 498-6793

   b) Via the Head of Compliance
      (1) Email: QualityCompliance@PNSOC.com
      (2) By phone: (714) 545-5550
      (3) In person

   c) Complaints should include the complainant's contact information (unless complainant wishes to remain anonymous), a detailed description of the incident, the date and time of the incident, and any other relevant information.

2. **Acknowledgment of Complaint**
   a) **Timely Response**: The Head of Compliance or designee will acknowledge receipt of the complaint within five (5) business days.
   b) **Initial Assessment**: The Head of Compliance or designee will evaluate if the complaint is a violation of PHI-related policies or HIPAA regulations.

3. **Investigation Process**
    a) **Designation of the Investigation Team**: The Head of Compliance, or designee, will lead the investigation, involving other relevant departments as necessary.
    b) **Collection/Review of Data**: The investigators shall gather all relevant information, including reviewing records, conducting interviews, and examining any related documentation.
    c) **Determination of Validity**: After collecting data, the investigation team will conduct an initial assessment of the collected material to determine whether there was a violation of PHI policies or HIPAA regulations.
    d) **Full Review of Data**: The investigation team shall conduct a thorough review of all data collected and prepare a summary report of the investigation process, any applicable findings, and recommendations for corrective actions to be taken.

4. **Investigation Follow-up/Close-out**
    a) **Findings and Recommendations**: Based on the investigation, the Head of Compliance (or designee) will present the findings to the PNS Executive Team and/or Compliance Committee and provide recommendations for corrective actions.
    b) **Communication with Complainant**: If appropriate, the complainant will be advised of the investigation's outcome and any actions taken, while maintaining confidentiality as required.
    c) **Corrective Actions**: Implement corrective actions to address any identified issues, which may include remediation on policies/procedures, policy revisions, or an enhancement to existing internal controls.

5. **Non-Retaliation**
    a) **Protection for Complainants**: All individuals will be assured that they will not face retaliation for filing a complaint in alignment with PNS policies, and state/federal regulations. Any form of retaliation is strictly prohibited and will be subject to disciplinary action up to and including termination of employment.

6. **Internal Reporting and Review**
    a) **Reporting Frequency**: The Head of Compliance will provide regular reports on the status and outcomes of complaints to the PNS Executive Leadership Team and/or Compliance Committee.
    b) **Policy Review**: This policy will be reviewed annually and updated as necessary to reflect changes in regulations, technology, and organizational practices.

7. **External/Regulatory Reporting**
    a) **Reporting Applicability:** The Head of Compliance (or designee) will consult with legal counsel and senior management to determine if the complaint meets the threshold for reporting to regulatory agencies.

8. **Report Overview**
    a) **Required Information**: A detailed report shall be created containing the following information:
        (1) Description of the breach or complaint.
        (2) Date and time of the incident.
        (3) Types of PHI involved.
        (4) Number of individuals affected.
        (5) Steps taken to investigate and resolve the breach.
        (6) Description of the corrective actions implemented.

9. **Supporting Documentation**: Include any relevant supporting documents, such as internal investigation reports, risk assessments, and communication with affected individuals.

10. **Cooperation with and Notification to Regulatory Agencies**
    a) PNS shall cooperate with regulatory agency complaint investigations and compliance reviews, including permitting access to facilities, records, and other sources of information.
    b) **HIPAA Breach Notification Rule**: If it is determined that the incident involved a breach involving 500 or more individuals, PNS shall report the incident to the Office of Civil Rights (OCR) and the Department of Health and Human Services (HHS) within 60 days of discovery. For breaches involving fewer than 500 individuals, the Head of Compliance shall maintain a log and submit the information on an annual basis.

        (1) Submission of information regarding a data security breach to the HHS Secretary is required by 45 CFR 164.408.

        (2) **Notification/Incident Submission**: Use the HHS breach reporting portal to submit the report (URL below): https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?facesredirect=true

        (3) **CA State Regulations**: PNS shall comply with California state-specific reporting requirements by submitting the report to the relevant state regulatory agency.
            i. Submission of information regarding a data security breach is required by California Civil Code s. 1798.29(e); California Civil Code s. 1798.82(f) ii. **Notification/Incident Submission**:

        Use the CA state breach reporting portal to submit the report (URL below):
        https://oag.ca.gov/privacy/databreach/report-a-breach

    c) **Other Regulatory Agencies**: If the complaint involves other regulations (e.g., FTC, OCR), Head of Compliance is to ensure reports are submitted to the appropriate agencies following their specific guidelines.

11. **Notification to Affected Individuals**
    a) **Timely Notification**: Notify affected individuals as required by HIPAA and other relevant regulations, providing details about the breach, potential risks, and steps taken to protect their information.
    b) **Methods of Notification**: Use appropriate methods such as written notices, email, or media announcements, depending on the size and scope of the breach.

12. **Follow-Up Actions**
    a) **Implement Corrective Measures**: Ensure all corrective actions identified during the investigation are implemented promptly.
    b) **Training and Awareness**: Provide additional training to staff as needed to prevent future incidents.

13. **Ongoing Compliance Monitoring**: Regularly monitor compliance with PHI protection policies and procedures to identify and address any Vulnerabilities.

M. Patient's Rights for Inspecting, Amending, and Obtaining PHI

1. **Processing Patient Requests for Amendment of PHI**
    a) **Submission of Amendment Requests**
        (1) Patients must submit requests for amendment in writing.
        (2) The request must include the patient's name, contact information, a description of the information to be amended, the reason for the amendment, and any supporting documentation.

    b) **Acknowledgment of Request**
        (1) **Timely Response**: The Head of Compliance will acknowledge receipt of the request in writing within 10 business days.
        (2) **Record of Request**: Document the receipt of the request and the date it was received.

    c) **Review and Evaluation**
        (1) **Verification**: Verify the identity of the individual making the request to ensure they have the right to request an amendment.
        (2) **Consultation**: Consult with the healthcare provider responsible for the entry to determine whether the amendment is appropriate based on the patient's medical record and supporting information.
        (3) **Criteria for Amendment**: Amendments may be appropriate if the information is inaccurate or incomplete. Requests may be denied if the information is accurate and complete, was not created directly by PNS, or is not part of the patient's designated record set.

    d) **Decision and Notification**
        (1) **Decision Timeframe**: PNS to confirm their decision regarding the amendment request within 60 days of receipt. If more time is necessary, PNS shall inform the patient in writing, explaining the reasons for the delay and the expected decision date, which shall not exceed an additional 30 days.
        (2) **Approval of Amendment**: If the amendment is approved:
            i. **Amend the Record**: Make the appropriate amendments to the

PHI and any other records that contain the amended information.

ii. **Inform the Patient**: Notify the patient in writing that the amendment has been accepted.

iii. **Inform Others**: With the patient's agreement, notify relevant persons or entities who have received the PHI and may have relied on the inaccurate or incomplete information.

(3) **Denial of Amendment**: If the amendment is denied:

i. **Provide Explanation**: Send a written denial to the patient, including the reason for the denial and information on how to submit a statement of disagreement.

ii. **Right to Disagreement**:
Inform the patient of their right to submit a statement of disagreement and the process for doing so.

iii. **Rebuttal Statement**: Inform the patient that PNS may prepare a rebuttal statement to the disagreement and how the patient can receive a copy.

(4) **Additional Documentation**:

i. PNS shall create documentation of the titles or persons or departments responsible for receiving and processing all PHI amendment requests.

ii. This documentation shall be maintained and stored securely for a time period for no less than ten (10) years.

e) **Statement of Disagreement and Rebuttal**

(1) **Inclusion in Record**: Include the patient's statement of disagreement and the PNS' rebuttal (if any) with the patient's medical records.

(2) **Future Disclosures**: Ensure that any future disclosures of the disputed PHI include the request for amendment, the denial, the patient's statement of disagreement, and PNS' rebuttal.

2. **Patient's Right to Inspect and Obtain Copies of Their PHI**

a) Patients have the right to inspect and obtain a copy of their PHI maintained in the designated record set, with certain exceptions as permitted by law.

b) **Request for Access**

(1) **Submission of Request:**

i. Patients must submit a written request to inspect or obtain a copy of their PHI to the Compliance Department.

ii. Requests may also be submitted electronically through the PNS Go app, where available.

(2) **Verification of Identity:**

i. The Compliance Department must verify the identity of the individual making the request before providing access to PHI.

c) **PNS Response to Request**

(1) **Timeliness:** The PNS Compliance Department will respond to requests for access within 30 days of receipt. If the requested information is not readily accessible, an extension of up to 30 additional days may be granted. The patient will be notified in writing of the extension and the reason for the delay.

(2) **Denial of Access:** Access may be denied in certain circumstances, such as when disclosure could endanger the life or physical safety of the individual or another person, or when the PHI contains references to another person (unless such person is a healthcare provider) and access would reasonably likely cause substantial harm. Denials will be provided in writing, including the basis for the denial and information on how to appeal the decision.

d) **Provision of Access** (1) **Inspection:**

(1) Patients may inspect their PHI in person by scheduling an appointment with the Compliance Department. A staff member will supervise the inspection to ensure the integrity of the records.

(2) **Copies:**

i. Patients may obtain copies of their PHI. Fees for copying, mailing, or other supplies may apply as permitted by law. The fee schedule will be made available to patients upon request. ii. If the PHI is maintained electronically and the patient requests an electronic copy, the Quality Assurance Department will provide the information in the electronic form and format requested, if readily producible, or in a mutually agreed-upon format.

e) **Documenting & Tracking Requests:**

(1) A log shall be kept by the Compliance Department documenting any requests to inspect and copy their PHI and will include the date the request was received and the date it was completed.

i. This log shall be kept for each health plan and will be available for review upon request by each health plan.

3. **Patient's Rights to Request to Restrict the Use and Disclosure of PHI**

a) **Receipt of Restriction Request:**

(1) Patients must submit restriction requests in writing to Pacific Neuropsychiatric Specialists.

i. Patients may use forms provided by their legal representative at the discretion of PNS' management team.

(2) Forward all written requests to the Head of Compliance or designated person responsible for handling PHI restrictions immediately upon receipt.

b) **Acknowledgement of Request:**

(1) Acknowledge receipt of the restriction request in writing to the patient within 10 business days.

(2) Inform the patient that their request is under review and will receive a response within 30 days.

c) **Review of Restriction Request:**

(1) The Head of Compliance, in consultation with Executive Management and relevant PNS department leadership, will review the request to determine its feasibility.

i. Considerations may include the impact on the patient's care, legal obligations, and administrative bandwidth when evaluating the request.

d) **Decision on Request:**

(1) **Approval**: If the request is deemed reasonable and does not interfere with treatment, payment, or healthcare operations (TPO), the request shall be approved with the decision documented and sent to the patient in writing.

(2) **Denial**: If the request is not reasonable or would impede essential operations, the request shall be denied. PNS management to provide a written explanation to the patient, including the reason for the denial, within 30 days.

e) **Implementation of Approved Restrictions:**

(1) PNS management shall update the patient's record in the designated record set to reflect the approved restriction.

(2) All relevant workforce members and business associates shall be notified of the approved restriction to ensure compliance.

(3) Maintain documentation of the restriction request, the decision, and any related communications in the patient's record.

f) **Ongoing Monitoring and Compliance:**

(1) Ensure that all workforce members are aware of and comply with the approved restriction.

(2) Conduct periodic audits to ensure adherence to the restriction and to address any issues promptly.

g) **Revocation or Modification of Restrictions:**

(1) Patients may request to revoke or modify their restriction request in writing at any time.

(2) Follow the same review and implementation process for revocations or modifications as outlined above.

(3) Document any changes and communicate them to all relevant parties.

h) **Emergency Situations:**

(1) In an emergency where the restricted PHI is necessary to provide treatment, the restriction may be temporarily lifted to ensure patient care. The patient will be informed of this action as soon as reasonably possible.

i) **Documenting & Tracking Requests:**

(1) A log shall be kept by the Compliance Department documenting any requests to restrict use and disclosure PHI and will include the date the

request was received and the date it was completed.

(2) This log shall be kept for each health plan and will be available for review upon request by each health plan.

N. Amending Protected Health Information (PHI) in a Designated Record Set When Informed of an Amendment by Another Covered Entity

1. **Receipt of Amendment Request:**
   a) When another covered entity (Health Plan) informs Pacific Neuropsychiatric Specialists of an amendment to a member's PHI, the request must be forwarded immediately to\ the Quality Assurance team or the designated team responsible for handling PHI amendments.
   b) PNS to verify the identity of the requesting entity and ensure the request is legitimate. The request must be in writing and specify the information to be amended.

2. **Review of the Amendment Request:**
   a) The Head of Compliance (or designee) will review the amendment request to determine if the PHI in question is part of the designated record set.
   b) PNS management to confirm that the amendment request is relevant to the PHI maintained by PNS.

3. **Decision on Amendment:**
   a) If the PHI is found to be part of the designated record set and the amendment request is valid, proceed with making the amendment.
   b) If the amendment request is not valid or if the PHI is not part of the designated record set, notify the requesting entity in writing, providing the reasons for denial. This response must be sent within 60 days of receipt of the request.

4. **Making the Amendment:**
   a) Document the request and the decision to amend in the individual's record.
   b) Amend the PHI in the designated record set as requested. Ensure that the amendment is clearly marked and dated.
   c) Maintain the original information along with the amended information to preserve the integrity of the record.

5. **Notification of Amendment:**
   a) Inform the requesting covered entity (health plan) that the amendment has been made.
   b) Notify any other parties who may have relied on the unamended PHI (e.g., business associates, other healthcare providers) if the amendment affects the information they have.

6. **Documenting & Tracking Requests:**
   a) A log shall be kept by the Compliance Department documenting any requests to amend PHI and will include the date the request was received and the date it was completed.
   b) This log shall be kept for each health plan and will be available for review upon request by each health plan.

O. Confidential Communications for Sensitive Services

1. **Overview:**
    a) California Assembly Bill 1184 (also referred to as CA Civil Code 56.107) requires health plans and insurers to accommodate requests from subscribers or enrollees to receive communications related to sensitive services through confidential means.
    b) ***Sensitive services*** refer to medical care related to the following categories:
        (1) mental health
        (2) reproductive health (which may include the identification/treatment of sexually transmitted infections (STI's), substance use disorder treatment, and other services where disclosure of information could lead to harm or distress).

2. **Request for Confidential Communications by Patients:**
    a) During call intake by PNS Call Center Representative (CSR), if services requested by a patient meet the requirements for sensitive services (listed above), the CSR shall inform patient of their right to request confidential communications at the time of scheduling or through written notice.
        (1) All confidential information shall be sent directly to the protected individual (member) by phone, email, and physical address(es) provided by the protected individual.
        (2) Disclosure of information deemed confidential under this section other than the protected individual shall only be granted if part of the treatment, payment, or healthcare operations related to the individual or if a signed release is completed and submitted to PNS by the protected individual.

    b) PNS will accept requests for confidential communications in writing, over the phone, or electronically. Ensure the request specifies the desired method of communication (e.g., alternate address, email, phone call).

3. **Documentation of Request:**
    a) CSR to record the request in the patient's Medical Record (MR), noting the preferred method of communication.
    b) PNS to ensure that this information is easily accessible to all (and only) appropriate personnel involved in the patient's transportation and care coordination.

4. **Confirmation of Request:**
    a) Send a written confirmation to the patient acknowledging receipt of their request for confidential communications within 10 business days.
    b) Clearly outline how their request will be accommodated and provide contact information for further inquiries.

5. **Implementation of Confidential Communications:**
    a) CSR's to update all systems and records to reflect the patient's preferred communication method.

b) CSR's to ensure that all communication regarding the patient's transportation for sensitive services is conducted according to their request. This includes:
    (1) Using alternate addresses or phone numbers.
    (2) Ensuring that email communications are sent to the designated email address.
    (3) Avoiding any mention of sensitive services in communications to third parties.

6. **Patient Communication:**
    a) PNS to maintain open communication channels with patients regarding their rights under AB 1184 and the process for requesting confidential communications.
    b) PNS to provide patients with a clear process for updating their communication preferences or revoking their confidential communications request.

P. Personal Representatives

1. **Personal Representatives of Living Members**
    a) PNS will recognize personal representatives as required by the HIPAA regulations.
    b) A personal representative is the person who has the authority to make health care decisions on behalf of the patient.
        (1) A family member or caregiver should not be assumed to be the Personal Representative of the patient, unless the individual meets the criteria described in this policy.
        (2) A personal representative may include:
            i. The patient's adult child, spouse, or other member of the patient's family, a close friend or any individual power of attorney authorized to make medical decisions for a patient.
            ii. Health care surrogate decision makers, guardian(s), or other court-appointed representatives.
        (3) Prior to the designation of a patient's personal representative, PNS must obtain written documentation to validate this request.

    c) When a patient contacts PNS by phone, the CSR (or other PNS staff) should request 2 identifiers, which include their name (first and last), date of birth, their home address, phone number to confirm their identify to be able to access their account.
        (1) If a patient's representative (including family members) request information, the patient must verify that the requesting party has the authority to receive PHI on their behalf by:
            i. coming to the telephone and providing temporary verbal authorization; or
            ii. sending an email with written authorization.

    d) **Exceptions & Additional Considerations:**
        (1) In cases where there is no written documentation of authorization and patients cannot provide incidental verbal authorization to authorize the family member to access their data, PNS should not grant access to that individual's data to their family member.

i. In these cases, PNS should refer the requesting party to their health plan for further action.

(2) If the patient is an adult or emancipated minor who lacks decisional capacity as documented in their health records, PNS must make a reasonable inquiry as to the availability and authority of a Personal Representative.

(3) If a patient is incapacitated (but not confirmed to be deceased), a Personal Representative may sign any form, or receive PHI concerning the patient on behalf of the individual.

(4) If a PNS staff member believes that disclosing information to a person identified as patient's personal representative may endanger the patient, they must notify their supervisor AND Head of Compliance before refusing to disclose information.

2. **Personal Representatives of Deceased Patients**
   a) Any individual requesting information about a deceased member will be referred to the health plan to obtain that information.
   b) PNS shall not provide information about a deceased member directly to any non-member.

VII. ENFORCEMENT

A. <u>Policy Enforcement: Privacy & Security Standards</u>

1. Mandatory Compliance & Scope
   a. All PNS staff, including clinicians, administrative staff, contractors, and Business Associates, are required to adhere to the Privacy and Security policies of Pacific Neuropsychiatric Specialists (PNS). Compliance is a condition of employment or contractual engagement.

B. <u>Oversight and Audit Authority</u>

1. The Head of Compliance is granted the authority to conduct regular, unannounced audits of all systems and physical spaces. Enforcement activities include:
   a. Electronic Access Logs: Periodic review of Electronic Health Record (EHR) audit trails to ensure "Minimum Necessary" access and detect "snooping" (unauthorized viewing of records without a clinical or business need).
   b. Physical Inspections: Verification of "Clean Desk" standards and secure storage of sensitive psychiatric files.
   c. Network Monitoring: Review of remote access logs and VPN usage to ensure compliance with California-specific encryption standards.

C. <u>Violation Categorization & Disciplinary Framework</u>

1. PNS reserves the right to apply disciplinary measures based on the severity of the violation, the sensitivity of the exposed data, and the intent of the individual. Under California CMIA, the organization and individuals may also face civil or criminal penalties.

a. Category 1 (Unintentional/Procedural): Accidental lapses (e.g., leaving a computer unlocked or failing to secure a file).
    1) Response: Mandatory re-training and a formal verbal warning.

b. Category 2 (Negligent/Repeated): Repeated procedural failures or accessing PHI without a clear "Need to Know" but without malicious intent.
    1) Response: Written warning, suspension of remote access privileges, and/or performance improvement plan.

c. Category 3 (Malicious/Willful): Intentional data theft, selling PHI, "snooping" into high-profile or personal records, or sharing credentials.
    1) Response: Immediate termination of employment and notification to the appropriate Licensing Boards and potentially the California Attorney General.

D. <u>Mandatory Reporting & "Safe Harbor"</u>

1. Under HIPAA and California Breach Notification Laws (Civil Code 1798.82), any workforce member who discovers a potential breach is legally required to report it to the Head of Compliance within one (1) hour.
    a. Non-Retaliation: PNS maintains a "no-retaliation" policy for employees who report security vulnerabilities or potential breaches in good faith.
    b. Self-Reporting: While violations are subject to review, prompt self-reporting that mitigates a breach will be considered a significant mitigating factor during disciplinary review.

E. <u>Personal Liability & Legal Sanctions</u>

1. Workforce members are advised that violations of California's CMIA or federal HIPAA regulations may result in:
    a. Civil Penalties: Fines ranging from $100 to $250,000.
    b. Criminal Charges: For the intentional and/or commercial misuse of psychiatric data.
    c. Professional License Review: Reports made to the Physician Assistant Board (PAB), Medical Board of California, or Nursing Board.

[END OF POLICY]