INTERNAL HIPAA PRIVACY & BREACH RESPONSE SOP

Policy Owner: Privacy Officer
Applies To: All workforce members (employees, contractors, interns, volunteers)
Effective Date: January 17, 2026
Review Cycle: Annual or upon regulatory change

---

1. Purpose

This SOP establishes internal controls to:

- Protect Protected Health Information ("PHI")
- Ensure compliance with HIPAA, HITECH, and state law
- Define workforce responsibilities
- Provide a clear, documented breach response process

---

2. Scope

This SOP applies to:

- All PHI (electronic, paper, verbal)
- All PCG systems and vendors
- All workforce members
- All locations and remote work environments

---

3. Definitions

- **PHI:** Individually identifiable health information
- **ePHI:** PHI stored or transmitted electronically
- **Breach:** Impermissible use or disclosure of PHI that compromises privacy or security
- **Business Associate:** Third party that creates, receives, maintains, or transmits PHI on PCG's behalf

---

4. Roles & Responsibilities

Privacy Officer

- Oversees HIPAA compliance
- Investigates incidents and breaches
- Coordinates breach notification
- Maintains documentation

Workforce Members

- Access PHI only as necessary
- Report suspected incidents immediately
- Complete HIPAA training annually

IT / Systems Administration

- Maintain technical safeguards
- Support investigations
- Implement corrective actions

---

5. PHI Access & Minimum Necessary Rule

- Access to PHI is **role-based**
- Workforce members may only access PHI required to perform job duties
- Access rights are reviewed:
  - Upon hire
  - Upon role change
  - Upon termination

---

6. Administrative Safeguards

PCG maintains:

- HIPAA training upon hire and annually
- Confidentiality agreements
- Workforce sanction policy for violations
- Written policies and procedures
- Vendor risk assessments and BAAs

---

7. Physical Safeguards

- Secure office access
- Locked filing cabinets
- Screen privacy practices
- Clean-desk policy
- Secure disposal of paper PHI (shredding)

---

8. Technical Safeguards

- Unique user IDs and strong passwords
- Multi-factor authentication where available
- Encryption of data in transit (where supported)
- Automatic logoff
- Audit logs
- Secure cloud-based EHR (TheraPlatform)

---

9. Approved Systems & Vendors (HIPAA-Aligned)

PCG uses the following HIPAA-aligned systems under Business Associate Agreements:

- **TheraPlatform** – EHR, scheduling, billing, client portal
- **Twilio** – Secure SMS and voice communications
- **LeadConnector** – Intake workflows, CRM, messaging

Use of unapproved systems for PHI is prohibited.

---

10. Incident & Breach Identification

Workforce members must report immediately if they observe:

- Lost or stolen devices
- Mis-sent emails or texts
- Unauthorized access
- Phishing or hacking attempts
- Improper disposal of PHI

Reports must be made **within the same business day** to the Privacy Officer.

---

11. Breach Response Procedure

Step 1: Containment

- Secure systems
- Revoke access if needed
- Prevent further disclosure

Step 2: Investigation

- Identify what happened
- Determine PHI involved
- Identify affected individuals
- Assess risk using HIPAA’s 4-factor test

Step 3: Risk Assessment Factors

1. Nature and extent of PHI
2. Unauthorized person involved
3. Whether PHI was acquired or viewed
4. Mitigation steps taken

---

12. Breach Notification

If a breach is confirmed:

- Notify affected individuals **within 60 days**
- Notify HHS OCR as required
- Notify state authorities if applicable
- Document all actions taken

---

13. Documentation & Record Retention

PCG maintains:

- Incident logs
- Risk assessments
- Training records
- Breach notifications
- Vendor BAAs

Records are retained for **at least 6 years**.

---

14. Sanctions & Enforcement

Violations may result in:

- Retraining
- Disciplinary action
- Termination
- Legal consequences

---

15. SOP Review & Updates

This SOP is reviewed:

- Annually
- After any material breach
- Upon regulatory change