	Training: Provider Training - HIPAA Privacy, Security & Information Protection Requirements	Policy and Procedure#:	TRN009
		Version:	1.0
		Effective Date:	1/28/2026

Document Information			
Department	**Division**	**Document Type**	**Document#**
Compliance	Training	Training	009

Revision History				
Version	**Description of Change**	**Author**	**Review Date**	**Revision Date**
1.0	Original/ Initial Version	Brittney Green	01/28/2026	N/A

1. PURPOSE

This Policy establishes the requirements for all contracted providers regarding:

- Protection of Protected Health Information (PHI)
- Protection of Electronic Protected Health Information (ePHI)
- Cybersecurity safeguards
- Release of Information standards
- Breach notification obligations
- Fraud, waste, and abuse related to information misuse

This Policy replaces the *HIPAA and Information Security Guidance for Providers* and serves as the governing compliance requirement for participation in The Holman Group provider network.

2. REGULATORY AUTHORITY

Providers must comply with:

- HIPAA Privacy Rule (45 CFR §164.500 et seq.)
- HIPAA Security Rule (45 CFR §164.302 et seq.)
- HIPAA Breach Notification Rule (45 CFR §164.400–414)
- HITECH Act (2009) and 2013 Omnibus Rule
- Knox-Keene Health Care Service Plan Act
- DMHC confidentiality requirements
- California Confidentiality of Medical Information Act (CMIA)
- Department of Insurance standards (where applicable)
- NCQA Information Integrity & Delegation standards

3. APPLICABILITY

This Policy applies to:

- Covered Entities
- Business Associates
- Subcontractors with access to PHI/ePHI

Per 45 CFR §160.103:

Covered Entities include:

- Health care providers
- Health plans
- Health care clearinghouses

Business Associates include:

Any person or entity that performs functions involving PHI on behalf of a covered entity, including:

- Third-party claims processors
- CPAs
- Attorneys
- Utilization review consultants
- Health care clearinghouses
- Translation services
- Accreditation bodies

Providers must execute compliant Business Associate Agreements (BAAs) as required by 45 CFR §164.504(e).

4. DEFINITIONS

4.1 Protected Health Information (PHI)

Individually identifiable health information that:

- Exists in paper, electronic (ePHI), or spoken form
- Relates to physical or mental health
- Relates to provision of care
- Relates to payment for care

Examples include:

- Lab results
- Therapy session details
- Radiology reports
- Appointment dates/times
- Invoices
- History & physical reports
- Patient identifiers

4.2 Personal Identifiers

Examples include:

- Name
- Medical Record Number
- Social Security Number
- Account Number
- License number
- IP address
- Health plan number
- DOB
- Email address
- Biometric identifiers

- Photographs
- URLs

5. HIPAA PRIVACY RULE REQUIREMENTS

Providers must protect PHI in all formats:

- Electronic
- Spoken
- Paper

Members have rights to:

- Access records
- Request amendments
- Restrict disclosures
- Receive alternate communications
- Obtain accounting of disclosures
- File complaints

Providers must apply the minimum necessary standard.

6. RELEASE OF INFORMATION (ROI)

6.1 Authorization Requirements

In most cases, a formally documented authorization must be obtained prior to releasing PHI.

Authorization must comply with state and federal law.

6.2 Identity Verification

Before making verbal disclosures:

- Verify name
- Date of birth
- Member number
- Address

6.3 Special Protections

Federal law provides heightened protection for:

- Substance use disorder records
- Mental health records

6.4 Permitted Disclosures Without Authorization

PHI may be disclosed without authorization:

- When required by law
- To public health authorities (FDA, CDC)
- For abuse or domestic violence reporting
- For law enforcement
- For suspicious death
- For workers' compensation
- For disaster relief
- To avert serious threat

- For health oversight activities

7. HIPAA SECURITY RULE REQUIREMENTS

Providers must implement safeguards ensuring:

- Confidentiality
- Integrity
- Availability

7.1 Administrative Safeguards

- Workforce training
- Security policies
- Risk assessment
- Incident management
- Sanction policy
- Workforce access management

7.2 Technical Safeguards

- Encryption
- User access controls
- Firewalls
- IDS/IPS
- SIEM monitoring
- Anti-malware
- Multi-factor authentication
- Penetration testing
- Vulnerability management

7.3 Physical Safeguards

- Secure facilities
- Clean desk policy
- Screen positioning
- Secure record transport
- Locked vehicles when PHI present
- Secure disposal

8. CYBERSECURITY THREATS

Providers must remain vigilant against:

- Hacking
- Malware
- Ransomware
- Phishing
- Social engineering
- Data leakage
- Privilege escalation
- Insider threats
- Natural disasters

9. USER ACCOUNT & PASSWORD SECURITY

Providers must:

- Maintain unique user IDs

- Prohibit password sharing
- Implement strong passwords
- Use multi-factor authentication
- Prevent unauthorized access
- Restrict use of USB devices
- Prevent installation of unauthorized software

Workforce members are responsible for activity under their credentials.

10. EMAIL, FAX & INTERNET SECURITY

Email

- Encrypt PHI sent externally
- Verify recipient email
- Avoid suspicious links
- Include confidentiality disclaimer
- Use work email for business only

Fax

- Avoid faxing PHI when possible
- Verify number before sending
- Do not include PHI on cover sheet
- Report misdirected fax immediately

Internet & Social Media

- Do not post work-related PHI
- Do not store PHI on web-based file sharing sites
- Do not use work email for personal applications

11. TRANSPORTING & DISPOSING OF PHI

When transporting records internally:

- Secure physically
- Carry close to the person
- Use designated containers
- Ensure names are not visible

Externally:

- Locked briefcase
- Locked vehicle
- Store in trunk or floor behind seat

Disposal:

- Shred paper PHI
- Sanitize electronic media
- Secure destruction procedures

12. BUSINESS CONTINUITY & DISASTER RECOVERY

Providers must maintain:

- Business Continuity Plan
- Disaster Recovery Plan
- Backup and recovery procedures
- Communication plans

---

13. BREACH NOTIFICATION REQUIREMENTS

Per 45 CFR 164.402: *Impermissible use or disclosure of unsecured PHI is presumed a breach unless low probability of compromise is demonstrated.*

Risk assessment must consider:

- Nature and extent of PHI
- Unauthorized recipient
- Whether PHI was viewed/acquired
- Mitigation efforts

13.1 Provider Reporting Requirement to Holman

Providers must report to The Holman Group:

- Potential exposure of PHI/ePHI
- Theft of equipment
- Unauthorized password use
- Unauthorized network access
- Lost/stolen PHI
- Security policy violations
- Suspected breaches

Reporting timeframe: Without unreasonable delay and no later than 2 calendar days after discovery.

Report to:

Email: ComplianceTeam@holmangroup.com
Mail: Compliance Department, P.O. Box 8011, Canoga Park, CA 91309
Phone: 800-321-2843

14. FRAUD, WASTE & ABUSE

Providers must not:

- Bill for services not rendered
- Alter claims for higher reimbursement
- Misuse codes
- Bill for medically unnecessary services

Medi-Cal/Medicaid fraud is a criminal offense and may result in:

- Imprisonment
- Significant fines
- Civil liability
- Suspension from government programs

15. SANCTIONS

Providers must implement a sanction policy for workforce violations.

Sanctions may include:

- Coaching/ Training
- Written warning
- Contract termination
- Regulatory reporting

---

16. TRAINING REQUIREMENTS

Providers must:

- Conduct HIPAA training upon staff hire
- Conduct annual refresher training with staff
- Maintain documentation
- Ensure business associates are trained

17. HOLMAN OVERSIGHT

Holman may:

- Request documentation of compliance
- Conduct audits
- Review breach documentation
- Require corrective action
- Terminate contracts for non-compliance

18. PROVIDER ATTESTATION REQUIREMENT

As part of network participation, providers must:

- Attest to receipt of this Policy
- Confirm understanding of HIPAA obligations
- Confirm implementation of safeguards
- Confirm understanding of reporting obligations
- Submit attestation within five (5) days of receipt

Approval Authority	Signature	Date
Brittney Green	Brittney Green	01/28/2026