

HIPAA: Safeguarding & Understanding Privacy

Overview: What is HIPAA?

HIPAA (Health Insurance Portability and Accountability Act of 1996) is a federal law designed to:

- Improve the efficiency of the U.S. healthcare system.
 - Ensure **privacy and security** of individuals' medical information.
 - Provide **portability** of health insurance for working Americans.
-

Key HIPAA Components

- **Privacy Rule:** Protects the confidentiality of PHI.
 - **Security Rule:** Sets standards for securing electronic PHI (ePHI).
 - **Fraud Prevention:** Addresses healthcare fraud and abuse.
-

What is PHI?

PHI is any health information that:

- Is created or received by a healthcare provider, plan, or clearinghouse.
- Relates to past, present, or future physical/mental health.
- Identifies or can reasonably identify an individual.

Common PHI Identifiers (common if receiving services):

- | | |
|---|---|
| 1. Names | 6. Medical record numbers |
| 2. Addresses | 7. Financial account info |
| 3. Dates (birth, admission, discharge, death) | 8. Photos |
| 4. Phone numbers | 9. BSU numbers |
| 5. Social Security numbers | 10. Email, IP addresses, biometric data, etc. |
-

HIPAA in Lifesharing

PHI may be used for:

- **Treatment:** Providing care.
 - **Payment:** Billing and insurance. Navigating/enrolling in waiver services.
 - **Operations:** Training, reporting, transporting PHI, etc.
-

HIPAA Compliance Best Practices

General Guidelines

- Access PHI only on a **need-to-know** basis.
- Keep PHI **confidential and secure**.
- Understand that **violations** can lead to:
 - Civil/criminal penalties
 - Job loss
 - Reputational damage

Safeguarding PHI

- **Oral:** Speak quietly, avoid public areas, don't use names unnecessarily.
 - **Written:** Lock files, shred documents, avoid using bulletin boards or whiteboards for PHI.
 - **Electronic:** Secure computers, check printers/fax machines, report misdirected emails/faxes. Encrypt email communications.
-

HIPAA Breaches

A **breach** is any impermissible use or disclosure of unsecured PHI. This includes:

- Employee errors
- Third-party access
- Cyberattacks (e.g., ransomware)

All affected individuals must be notified, and agencies must follow breach reporting policies.

Social Media Risks







Avoid sharing any PHI on:

- Social Media / Facebook / Instagram / X (personal or agency pages)
 - YouTube
 - Any public platform
-

Everyday Life & HIPAA

- HIPAA allows PHI use for treatment, payment, and operations.
 - Lifesharing must balance **community inclusion** and **privacy**.
 - Example: Sharing health updates with a pastor or celebrating achievements must be done with **consent** and awareness of HIPAA rules.
-

Scenarios for Practice

- Introducing a resident in public
 -  Use a first name basis – This is Amy, she is a young woman joining us.
 -  Share too much info – This is Joe Schmoe. He is 57. Born on 4/3/1971
- Sharing health updates with volunteers
 -  Short, sweet & vague - Doing better. Feeling better. Back to work.
 -  Oversharing – Diagnosed with anxiety. Now takes lorazepam at night.
- Leaving PHI in public places
 -  Double check settings following meeting/appts. – Gather all papers & shred at a secure location if not needed
 -  Improper Disposal – Throwing PHI in a public trash container

- Misplacing notes with health data
 - 👍 Carry sensitive information in a sealed bag – Tommy’s Support Briefcase
 - 👎 Comingle family health information in one place – Junk drawer approach
-

Conclusion

To stay compliant:

- Limit PHI access to those who need it.
 - Keep all PHI identifiers secure.
 - Follow agency HIPAA policies.
 - Know how to report a breach.
-

Fraud, Waste & Abuse: Training Guide for Lifesharing

What is Fraud, Waste, and Abuse (FWA)?

- **Fraud:** Intentional deception or misrepresentation for personal or financial gain.
Example: Billing for services not provided or falsifying documentation.
 - **Waste:** Overuse or misuse of services or resources, not necessarily intentional.
Example: Providing more services than necessary or duplicating services.
 - **Abuse:** Practices that are inconsistent with sound medical or business practices, leading to unnecessary costs.
Example: Charging for services that are not medically necessary or not following proper billing procedures.
-

How FWA Applies to Lifesharing Providers

Lifesharing is a Medicaid-funded service in Pennsylvania that supports individuals with intellectual disabilities by placing them in family homes. As a provider, you are considered a **Medicaid provider**, and therefore subject to both **state and federal FWA regulations**.

Key Responsibilities:

1. Accurate Documentation

- Document all services provided, including dates, times, and nature of care.
- Ensure timesheets and progress notes are truthful and complete.

2. Billing Integrity

- Only bill for services actually provided.
- Avoid duplicate billing or billing for services not authorized in the individual's plan.

3. Training Requirements

- Lifesharing providers must complete **annual FWA training** as part of compliance with the **Centers for Medicare & Medicaid Services (CMS)** and **Pennsylvania Department of Human Services (DHS)** guidelines.
[\[q1.amerihe...ipcare.com\]](#), [\[pa.performcare.org\]](#)
- Training includes recognizing, preventing, and reporting FWA.

4. Reporting Suspected FWA

- You are **legally obligated** to report any suspected fraud or abuse.
 - Reports can be made to the **Office of Inspector General (OIG), DHS Bureau of Program Integrity**, or your Managed Care Organization (MCO).
-

Examples Specific to Lifesharing

- **Fraud:** Submitting daily notes for stipend reimbursement when the individual was on a home visit.
 - **Waste:** Repeatedly purchasing supplies that are not used or needed.
 - **Abuse:** Providing services outside the scope of the Lifesharing agreement or failing to meet health and safety standards.
-

Best Practices for Compliance

- Attend all required FWA and compliance trainings.
 - Maintain clear, timely, and accurate records.
 - Understand the individual's **Individual Support Plan (ISP)** and follow it closely.
 - Ask questions if you're unsure about billing or documentation procedures.
 - Use official reporting channels if you suspect misconduct.
-

Where to Report Suspicions of FWA

RHD Internal

1. Program Leadership – Amy Rush – 484-294-1873
2. RHD Regional Director – Jessical Holdsworth – 267-300-8517
3. Compliance Email Box – RHDcares@rhd.org

External

1. Pennsylvania Department of Human Services (DHS)

- **Fraud Tip Hotline:** 1-844-DHS-TIPS (1-844-347-8477)
- **Online Reporting:** [DHS Report Fraud Page \[oig.hhs.gov\]](https://oig.hhs.gov)

- **What to Report:** Suspected fraud in Medicaid, SNAP, cash assistance, or other public assistance programs.
-

2. Medicaid Fraud Control Section (MFCS) – PA Office of Attorney General

- **Phone:** 1-717-783-1481
 - **Email:** mfcsintake@attorneygeneral.gov
 - **Online:** [Medicaid Fraud Reporting \[friendship...ousepa.org\]](https://friendship...ousepa.org)
 - **What to Report:** Fraud by Medicaid providers, abuse/neglect of care-dependent individuals.
-



Tips for Reporting

When reporting, try to include:

- Names and contact info of individuals or providers involved
- Dates and times of incidents
- Description of the suspected fraud or abuse
- Any supporting documentation (e.g., billing records, communication logs)