CareCertify LLC

Behavioral & Mental Health Training Series

BH-08

Client Rights, Confidentiality & Data Privacy

Participant Guide

Behavioral & Mental Health Training Series · Audience: ARMHS · CTSS · Behavioral Aides · MH Practitioners · Case Managers · CE Hours: 1.0

Rights and Privacy Are the Foundation of Trust

People seeking mental health and substance use care share some of the most sensitive information about their lives, and they do it trusting that their rights will be honored and their privacy protected. Chapter 245I sets out client rights, and a web of laws protects their data. Honoring both is the foundation of trust — and the law.

This guide covers client rights, the confidentiality laws (including the extra-strict 42 CFR Part 2 for substance use), when sharing is and isn't allowed, and everyday privacy habits. When in doubt about sharing information, the safe answer is to check first.

Learning Objectives — by the end of this module you will be able to:

- Summarize client rights under Chapter 245I
- Explain confidentiality and the laws that protect client information
- Identify when information can and cannot be shared
- Describe releases of information and mandatory exceptions
- Apply everyday privacy practices

Section 1: Client Rights Under Chapter 245I

Chapter 245I sets out the rights of clients receiving mental health services, including the right to be treated with dignity and respect, to participate in their own treatment and planning, to give informed consent, to refuse services and be told the consequences, to privacy and confidentiality, to be free from abuse and neglect, and to voice grievances without retaliation. Clients must be informed of their rights, and staff must honor them.

Section 2: What Confidentiality Means

Confidentiality means protecting client information and sharing it only as permitted by law and with proper authorization. In behavioral health, even the fact that someone is a client can be protected information. Confidentiality applies everywhere — in conversation, documentation, phone calls, and online — and it's both an ethical duty and a legal requirement.

Section 3: The Laws That Protect Client Data

Several laws protect client information. HIPAA sets federal health-privacy standards. The Minnesota Health Records Act (Minn. Stat. 144.291–144.298) governs how Minnesota health records are released. The Government Data Practices Act (Minn. Stat. ch. 13) covers government-held data. And 42 CFR Part 2 gives extra-strict protection to substance use disorder treatment records. You don't need to be a lawyer — you need to know that information is protected and to follow your agency's policies.

Section 4: 42 CFR Part 2 and Substance Use Information

Substance use disorder treatment records receive extra federal protection under 42 CFR Part 2. In general, you cannot disclose — or even acknowledge — that someone is in substance use treatment without specific written consent, beyond limited exceptions. Because many behavioral health clients have co-occurring substance use, be especially careful with any information touching substance use, and follow your program's Part 2 procedures.

Section 5: Releases of Information

Sharing client information with people outside the treatment team usually requires the client's signed release of information (ROI), which specifies what can be shared, with whom, and for how long. Share only what the release authorizes, and verify before disclosing. Within the treatment team, share on a need-to-know basis to coordinate care.

Section 6: Mandatory Exceptions to Confidentiality

Confidentiality is not absolute. Mandatory exceptions include reporting suspected maltreatment of vulnerable adults or children, situations involving a serious risk of harm to the client or others, certain court orders, and emergencies. These safety obligations can require disclosure. Know your reporting duties (covered in BH-10), tell clients at the start about the limits of confidentiality, and follow agency policy.

> **Don't promise total secrecy**
>
> Tell clients up front that you'll protect their privacy but must act on safety — like risk of harm or abuse. Never promise to keep a safety concern secret.

Section 7: Everyday Privacy Practices

Most privacy breaches are everyday slips: discussing a client in a hallway or on social media, leaving a screen or chart visible, or sharing on the phone without verifying who's asking. Protect privacy with simple habits — don't discuss clients in public, secure records and devices, log off, verify identity before disclosing, and share only on a need-to-know basis.

Section 8: When in Doubt, Check First

When you're unsure whether you can share information, the safe answer is to pause and check with your supervisor or agency policy before disclosing. A wrongful disclosure can't be taken back, and it can harm the client and break the trust that treatment depends on. Protecting privacy is protecting the person.

Key Terms

Term	What it means
Confidentiality	Protecting client information and sharing only as the law allows.
HIPAA	Federal law protecting health-information privacy.
MN Health Records Act	Minnesota law governing release of health records (144.291–144.298).
42 CFR Part 2	Federal rule giving extra protection to substance use records.
Release of information (ROI)	A signed authorization specifying what may be shared, with whom.
Mandatory exception	A situation (like abuse or serious harm) that can require disclosure.

Check Your Understanding

1. Name three client rights under 245I.
2. Why is even confirming someone is a client sometimes protected?
3. What is special about 42 CFR Part 2?
4. What does a release of information specify?
5. Name two mandatory exceptions to confidentiality.

What's Next

> **Looking ahead**
>
> Next, BH-09: Documentation & Progress Notes covers writing the records that support treatment and meet 245I standards.