A FREE GUIDE FOR BEHAVIORAL HEALTH PRACTICE OWNERS

When A Clinician Leaves

How To Protect Your Clients' Records

Clinicians move on. It's a normal part of running a group practice. This plain-English guide walks you through what to do before, during, and after a clinician's last day, so your clients' most private information stays where it belongs.

Inside:

- The setup that makes every departure easier
- What to do when a clinician gives notice
- A two-page last day checklist you can use right away
- What to do about personal laptops and phones
- A quick self-check: could you handle a departure tomorrow?

BigU COMPUTERS

(570) 340-0800
bigucomputers.com

INTRODUCTION

Why This Matters

Clinicians leave. They start their own practices, move, change careers, or retire. Some clients will choose to follow them, and that's their right.

The harder question is what happens to everything else: the notes, intake forms, emails, text messages, and files that clinician could reach. In many practices, nobody can say for sure where all of it lives, or whether access has truly been shut off.

Your practice is responsible for protecting that information, even after the person who created it walks out the door. HIPAA, the federal health privacy law, expects practices to have a process for ending access when someone leaves.

How To Use This Guide

1. **Before Anyone Gives Notice**
   The setup that makes every future departure simpler.
2. **When A Clinician Gives Notice**
   The weeks between the announcement and the last day.
3. **The Last Day Checklist**
   Two pages you can print and work through.
4. **The Personal Laptop Problem**
   What to do when client work happened on personal devices.
5. **After They're Gone**
   The first week, the first month, and every time after.

This guide is general information, not legal advice. Talk with your attorney and your licensing board about your specific situation.

PART 1

Before Anyone Gives Notice

The easiest departure is the one you prepared for long before it happened. These steps take some effort once, and then every departure after gets simpler.

1. **Keep a list of every system**
   Your electronic health record (EHR), email, file storage, telehealth platform, phones, fax, texting and reminder tools, billing, and anything else a clinician can log into.

2. **Give everyone their own login**
   Shared logins make it impossible to shut off one person without disrupting everyone else.

3. **Use practice accounts only**
   Client communication belongs in practice email and practice phone lines, never personal email or a personal cell number.

4. **Turn on sign-in verification**
   A code sent to a phone or app, in addition to the password, protects accounts even if a password leaks.

5. **Manage every device used for client work**
   Practice-owned or personal, any device that touches client information should be set up so you can lock it or remove practice information from a distance.

6. **Put it in writing**
   Agreements with employees and contractors should state that client records belong to the practice, and how practice information and equipment are returned. Have your attorney write or review this language.

7. **Write your departure checklist now**
   Start with Parts 3 and 4 of this guide, so someone other than you can run it.

PART 2

When A Clinician Gives Notice

Most departures are friendly. Treat these steps as good housekeeping, not suspicion. They protect your clients, your practice, and the colleague who is leaving.

1. **Plan client transitions the right way**
   Follow your ethics code and licensing board's expectations for continuity of care. Clients choose where they go next.

2. **Keep records with the practice**
   If a client follows the clinician, their records transfer through a signed release handled by the practice. They are never copied over by the departing clinician.

3. **Get notes finished**
   Ask for all progress notes to be completed and signed before the last day. Unsigned notes are much harder to resolve later.

4. **Inventory what they can reach**
   Using your system list, write down every account, device, and shared password this clinician has access to.

5. **Watch for unusual activity**
   Large downloads, file exports, or email rules that send messages to a personal address are worth a quiet look.

6. **Pick the moment access ends**
   Decide exactly when access will be shut off, usually at the close of the last day, and who will do it.

7. **Plan the goodbye message**
   Decide what clients, referral sources, and staff will hear, and prepare an email auto-reply that points people to the practice.

PART 3 · CHECKLIST 1 OF 2

The Last Day: Accounts

Work through this at the agreed time. Check off each item and keep these pages with your records.

- [ ] Deactivate their EHR account. Deactivate rather than delete, so notes and history stay intact.
- [ ] Reset their email password and sign them out of every device.
- [ ] Remove their phone from sign-in verification on every account.
- [ ] Set an auto-reply and send new email to a colleague or the practice manager.
- [ ] Check for rules that forward email to outside addresses, and remove them.
- [ ] Remove access to shared files and folders, and move anything they created into practice ownership.
- [ ] Close or transfer their telehealth account.
- [ ] Remove them from billing, fax, texting, and appointment reminder tools.
- [ ] Change every shared password they knew, including front desk computers and office Wi-Fi.

PART 3 · CHECKLIST 2 OF 2

The Last Day: Phones, Devices, And The Office

- [ ] Reassign their phone extension and voicemail box. Review saved voicemails for client information.
- [ ] Turn off any call forwarding to their personal cell phone.
- [ ] Collect practice laptops, phones, keys, badges, and door codes.
- [ ] For personal devices used for client work, remove practice apps and information (see Part 4).
- [ ] Update your website, online directory listings, and staff lists.
- [ ] Write down what was done, when, and by whom.

Document Everything

If questions ever come up, a dated, signed checklist shows that you acted promptly and responsibly.

Completed by _____

Date and time _____

PART 4

The Personal Laptop Problem

This is the part that keeps practice owners up at night. When a clinician uses their own laptop or phone, client information can end up in downloads folders, email apps, text messages, and photo libraries.

If It Has Already Happened

- Ask directly and kindly. Request that they delete all practice information and sign a short statement confirming they did. Your attorney can draft it.
- If the device was set up for practice management, remove practice apps and information from a distance.
- Change passwords on every account the device could reach, so saved logins stop working.
- Review recent account activity for large downloads or unusual sign-ins.
- If you believe client information was exposed, talk with your attorney about whether breach notification rules apply.

Going Forward

- Provide practice-owned devices for client work whenever you can.
- If personal devices are allowed, require them to be set up so practice information lives in a separate, protected space that can be removed without touching personal photos or files.
- Keep client files in your EHR and practice storage, never saved directly to a device.

PART 5

After They're Gone

The last day isn't quite the end. A little follow-through over the next few weeks closes the gaps that checklists miss.

The First Week

- Review sign-in activity on key accounts for anything unusual.
- Confirm auto-replies and call routing are working.
- Make sure no client messages or voicemails are going unanswered.

The First Month

- Keep their email account for a set period, then archive it according to your record keeping policy.
- Update your system list and departure checklist with anything you missed.
- Remind your team that shared passwords have changed.

Every Time

- Ask what made this departure easy or hard, and fix the hard parts before the next one.

> **A departure handled well** protects your clients, your practice, and the colleague who left. It also shows your team that the practice takes client trust seriously.

QUICK SELF-CHECK

Could You Handle A Departure Tomorrow?

Answer honestly. Nobody sees this but you.

1. Could you list every system a clinician can log into?	☐ Yes	☐ No
2. Do all clinicians use practice email, never personal email, for client communication?	☐ Yes	☐ No
3. Does every person have their own login, with no shared passwords?	☐ Yes	☐ No
4. Can you lock or remove practice information from every device used for client work, including personal ones?	☐ Yes	☐ No
5. Do your agreements with clinicians state that client records belong to the practice?	☐ Yes	☐ No
6. Could you shut off all of one clinician's access in under an hour?	☐ Yes	☐ No
7. Would you know if someone downloaded a large number of client files?	☐ Yes	☐ No
8. Do you have a written departure checklist that someone other than you could follow?	☐ Yes	☐ No

7 to 8 yes

You're in strong shape. Keep your lists current.

4 to 6 yes

You have a foundation, with a few gaps worth closing soon.

0 to 3 yes

You're not alone, and this is fixable. Start with Part 1.

WANT A SECOND SET OF EYES?

Let's Make Your Next Departure The Easy Kind

Big U Computers has spent years supporting behavioral health and drug and alcohol programs in Pennsylvania. Today we help group practices across the Lehigh Valley protect every client record and keep clinicians focused on their clients, not their computers.

Here's How It Works

1. **Schedule a free Practice Protection Review**
   A relaxed conversation about how your practice works.
2. **Get a clear roadmap, in plain English**
   What's working, what isn't, and what to fix first.
3. **Lead with confidence**
   Knowing your clients' trust is protected.

Book your free Practice Protection Review
bigucomputers.com/behavioral-health-it-services

(570) 340-0800

"Our agency relies heavily on him..."

Mary Lyn Cadman, MSW, LSW, Administrator/CEO, CMSU Behavioral Health and Developmental Services

We Won't Hold You Hostage	Personal Service	Peace Of Mind	No Geek-Speak