



Infinity Technologies

HIPAA INSIDER THREAT CHECKLIST: PROTECT YOUR PRACTICE FROM INTERNAL SECURITY RISKS

PREPARED BY INFINITY TECHNOLOGIES -
REGISTERED PROVIDER ORGANIZATION (RPO)

Insider threats come from employees, contractors, or business partners who misuse their access to patient data. Use this checklist monthly to spot potential risks before they become breaches.

Technology & System Access

Red Flags:

- ☐ Multiple failed login attempts from the same user
- ☐ Downloading or printing large amounts of patient data
- ☐ Staff accessing patient records outside their job duties
- ☐ Staff working unusual hours with heavy system activity
- ☐ Employees looking up their own medical records or those of family/friends

Patient Data Handling

Red Flags:

- ☐ Taking patient files home or off-site
- ☐ Taking photos of computer screens or patient records
- ☐ Sharing patient information on social media
- ☐ Accessing records of patients they're not treating
- ☐ Discussing patient cases in public areas (hallways, cafeteria, parking lot)

Workplace Behavior Changes

Red Flags:

- ☐ Frequent disputes with supervisors or coworkers
- ☐ Financial stress or personal problems affecting work
- ☐ Employee expressing anger about workplace policies or pay
- ☐ Bragging about having access to "important" or "celebrity" patient files
- ☐ Making concerning comments about "getting back at" the organization

Prevention Best Practices

Monthly Review Tasks:

- ☐ Update staff training on data protection policies
- ☐ Check who has access to patient data systems
- ☐ Review unusual login activity or access patterns
- ☐ Test your incident response procedures
- ☐ Verify that terminated employees no longer have system access

Ongoing Protection:

- ☐ Provide regular HIPAA training and updates
- ☐ Conduct annual background checks for staff with data access
- ☐ Create clear policies for handling patient information
- ☐ Maintain detailed logs of who accesses patient records
- ☐ Establish anonymous reporting channels

What to Do If You Spot Warning Signs:

Immediate Steps:

- Don't confront the employee directly
- Document what you observed with dates and details
- Preserve evidence like screenshots or access logs
- Report to your supervisor or compliance officer

Your Reporting Options:

- Direct supervisor or manager
- HIPAA compliance officer
- HR department
- Anonymous reporting hotline (if available)
- Practice owner or administrator

Don't ignore potential warning signs.
It's better to report a false alarm than miss a real threat.

Need Help?

If you've identified potential insider threats or want to strengthen your practice's security:

Contact Infinity Technologies for expert HIPAA compliance guidance and security solutions tailored to healthcare providers.

While this checklist helps support HIPAA compliance, it should not be used in place of professional security assessment or legal advice.