HIPAA, Privacy & Cybersecurity Checklist

For Assisted Living Communities and Skilled Nursing Facilities

Angela Gillis, Sorticulture Systems

A note on assisted living vs. skilled nursing: skilled nursing facilities are generally HIPAA covered entities, because they typically conduct standard electronic transactions such as claims. Assisted living communities should confirm their own covered-entity status. But, every item on this list protects resident information either way.

Start This Week

☐ Write down where resident information shows up, and who can touch it.

Supports: Security Rule required risk analysis (45 CFR §164.308(a)(1)(ii)(A)), the first input to a real risk analysis.

Why it matters: Duplicate or mismatched resident records are linked to an estimated 2,000 preventable deaths a year nationally. You cannot catch a wrong chart if you do not know what you are tracking in the first place.

☐ Turn on multi-factor authentication (MFA) for email and remote access.

Supports: Security Rule access control and technical safeguards (45 CFR §164.312(a)).

Why it matters: Most account break-ins start with a stolen password. MFA stops the break-in even when the password is already out there. Applies to any system that holds electronic resident information.

☐ Remove system access the same day someone leaves: staff, agency, or contractor.

Supports: Security Rule workforce security / termination procedures (45 CFR §164.308(a)(3)(ii)(C)).

Why it matters: In May 2025, nineteen skilled nursing facilities paid $1.56 million collectively to HHS-OIG for a related access-control failure: not checking who still had access. It also builds staff trust: clear rules mean no one is stuck using someone else's login just to get through a shift.

☐ Post a "hang up and call back" notice near every resident-facing phone.

Supports: Not a specific HIPAA citation. It is a practical fraud-prevention step that protects the same information HIPAA covers.

Why it matters: Resident-facing phones give scammers a direct path to residents, bypassing many of the safeguards staff would normally provide. A simple "hang up and call back" rule interrupts the pressure and urgency scammers rely on and gives residents and staff a clear next step: end the call and use a known, trusted number to verify who is calling.

☐ Train staff to recognize and report a scam call.

Supports: Security Rule security awareness and training (45 CFR §164.308(a)(5)); Privacy Rule training requirement (45 CFR §164.530(b)).

Why it matters: Seniors lost $7.7 billion to scams in 2025, up 59% in a single year, more than any other age group. Staff who can spot a scam call protect residents and families directly, not just your compliance file.

☐ Log every records request the day it comes in.

Supports: Right of Access (45 CFR §164.524): a 30-day deadline, with one 30-day extension allowed if written notice is given.

Why it matters: This is the single most active area of federal HIPAA enforcement right now. It is also a trust habit: a family that gets an answer on time trusts you more than one left waiting.

The Next 3 to 6 Months

☐ Complete a full, documented risk analysis, built from what you wrote down in week one.

Supports: Security Rule required risk analysis (45 CFR §164.308(a)(1)(ii)(A)), the single most-cited requirement in federal HIPAA enforcement.

Why it matters: This is the foundation everything else on this list sits on. It turns "we believe we are compliant" into "we can show we are."

☐ Test that your backup actually restores, and write down the downtime plan.

Supports: Security Rule contingency planning (45 CFR §164.308(a)(7)).

Why it matters: When systems go down, staff lose real-time access to allergies, medication lists, and care plans. This is a care-quality issue in the moment, not only a cybersecurity one.

☐ Review every real vendor for a signed Business Associate Agreement (BAA).

Supports: Business associate provisions (45 CFR §164.502(e), §164.504(e)).

Why it matters: A 2026 hospital breach affecting 18,600 patients came through a third-party vendor, not the hospital itself. Vendors are a documented, common point of failure. This is also your payer-trust item: answer a payer's security question that day.

☐ Build out full training: HIPAA, privacy, and cybersecurity.

Supports: Security Rule and Privacy Rule training requirements (45 CFR §164.308(a)(5), §164.530(b)).

Why it matters: Employees are one of the strongest protections residents have against scams, privacy violations, and security incidents: but only if they know what to recognize and what to do next. Training should give staff clear, practical responses to suspicious calls, phishing, requests for resident information, inappropriate disclosures, lost devices, misdirected messages, and other situations they are likely to encounter.

This checklist is educational, not legal advice. For guidance specific to your organization, consult your attorney.

SESSION FEEDBACK

HIPAA, Privacy, and Cybersecurity in Assisted Living and Skilled Nursing Facilities — Angela Gillis, Sorticulture Systems

Please complete and hand in before you go. Thank you.

Your name: _____

Facility: _____

Your email: _____

The most valuable idea I learned today, and how I'll use it:

_____

_____

One suggestion to make this session better:

_____

PLEASE CHECK ANY THAT APPLY

☐ Send me the electronic checklist from today.

☐ I'd like to refer Angela to speak at another organization or conference.

☐ Add me to your email list for your monthly newsletter for HIPAA and privacy tips.