centrexIT

AI and the Vulnerable Elder

A pocket guide for elder-serving organizations and the older adults in their care.

THE FIVE RULES FOR THE AI ERA

If you remember nothing else, remember these.

1. **The voice is no longer proof.**
2. **Caller ID is no longer proof.**
3. **Polished writing is no longer proof.**
4. **Urgency is a warning sign.**
5. **Verification is the new trust.**

WHAT TO NEVER SHARE WITH AI

Treat public AI tools like a stranger in a public room.

- Social Security number
- Medicare number
- Bank or credit card information
- One-time passcodes or passwords
- Date of birth or home address
- Medical records or prescription details
- Photos of IDs or insurance cards
- Family emergency details
- Security questions or recovery answers
- Caregiving and travel schedules

If you wouldn't say it out loud at the bank, don't type it into ChatGPT.

THE FAMILY VERIFICATION PROTOCOL

Six rules every family should agree on — before they need them.

1. **Family safe word.** A pre-agreed phrase used only when verifying urgent requests.
2. **Hang up and call back.** Use a known number, not the one you were called from.
3. **Second-person check.** Verify any emergency with a second family member.
4. **Never share codes.** One-time passcodes, account numbers, or passwords — ever.
5. **No remote access.** Never install software because someone called you.
6. **No secrecy around money.** If it's secret, it's a red flag.

WHEN SOMEONE HAS BEEN SCAMMED

Shame is the scammer's second weapon. Fast reporting is part of recovery.

SAY	AVOID
"This was designed to trick people."	"How did you fall for this?"
"You are not the only one this has happened to."	"Why did you send the money?"
"The faster we know, the more options we have."	"You should have known better."

centrexIT

centrexIT

FOR ORGANIZATIONS THAT SERVE OLDER ADULTS

The Provider Side of Elder AI Safety

You can't credibly counsel elders on AI safety if your own organization is leaking their data.

THE PROVIDER CHECKLIST

What every elder-serving organization needs.

- Written AI acceptable use policy for staff and volunteers
- Enterprise AI tiers — no-training guarantees and audit logs
- Encryption at rest and in transit on all client data
- Multi-factor authentication on every account
- Role-based access control — least privilege
- Quarterly phishing simulations and training
- Vendor due diligence on every tool touching client data
- Written incident response plan reviewed annually
- Verification protocol for staff impersonation attempts
- Periodic data inventory — know where everything lives

WHERE SENSITIVE ELDER DATA ACTUALLY LIVES

Exposure doesn't always come from a hack. It often comes from a well-meaning staff member or volunteer pasting client information into the wrong tool.

- Case management systems
- Email & attachments
- Donor databases
- Board member devices
- Shared drives & cloud
- Volunteer spreadsheets
- Transportation rosters
- Staff laptops & phones
- Intake forms (paper & digital)
- Meal delivery lists
- Third-party vendor systems
- AI prompts & chat histories

ASSESS YOUR ORGANIZATION

Elder AI Risk Snapshot

Free 2-minute self-assessment. Score your AI risk across data governance, staff use, and client vulnerability. No email required.

centrexit.com/tools/elder-ai-risk-snapshot

THE FULL TOOLKIT

10 Resources, One Page

Provider checklists, family verification scripts, AI policy templates, and incident response cards — all in one place for staff and clients.

centrexit.com/elder-ai

WANT A SCORE INSTEAD?

The Elder AI Risk Snapshot is a free 2-minute self-assessment that scores your AI risk across data governance, staff use, and client vulnerability — and tells you which of the items above to prioritize.

Go to centrexit.com/tools/elder-ai-risk-snapshot

YOU CALL. WE ANSWER. IT WORKS