PRIVACY AND SECURITY GUIDE · 2026

Are Your Call Recordings Secure?

Why recordings are personal information, how they leak, what the NDB scheme requires, and the eight controls that close the gaps.

> Every recorded call is a **file of personal information**: names, addresses, account details, and too often card numbers or health details. Under APP 11 it has to be protected, and destroyed once it is no longer needed.

What the law expects (APP 11)

- **11.1** Protect it from misuse, loss and unauthorised access
- **11.2** Destroy or de-identify it when no longer needed
- **11.3** Technical and organisational measures (2024 reforms)
- Health providers are covered whatever their size

Five ways recordings leak

- Shared admin logins
- Files downloaded and emailed
- Former staff who can still listen
- Kept forever "just in case"
- Breaches at the provider

If a recording escapes (NDB scheme)

1. **Contain:** remove access, delete stray copies, change passwords.
2. **Assess:** within 30 days, work out which recordings and what they held.
3. **Notify:** the OAIC and affected people if serious harm is likely.
4. **Review:** fix the cause so it cannot happen again.

Card details

PCI DSS does not allow card security codes to be stored after authorisation, including in audio recordings. Use a payment link, keypad payment or a recording pause.

Eight controls that close the gaps

Control	In practice
Named logins only	No shared admin account
Access by role	Few people can hear everything
Stronger sign-in	Multi-factor or passwordless, device approval
Retention schedule	Written periods, deleted on time
Fewer copies	Share inside the system, not by email
Access trail	Who listened to what, and when
Same-day offboarding	Leavers signed out on their last day
Know where it lives	Country of storage and every copy

Ask your phone provider

- [ ] Where are recordings stored, and who else holds copies?
- [ ] Are they encrypted in transit and at rest?
- [ ] Who at the provider can access them?
- [ ] Can recordings be deleted automatically after a set period?
- [ ] Can access be limited by user, with a record of listens?
- [ ] What sign-in protection is available?
- [ ] Can recordings go to our own storage?
- [ ] How and when will you tell us about a breach?

General information

Based on OAIC and PCI Security Standards Council guidance as read in November 2026. Not legal advice.

Uniden Voice

Australian owned, hosted and supported in Australia. Recordings and AI summaries in the call log, offsite storage in your own OneDrive or Google Drive, CRM integrations, passwordless sign-in and device approval. Book a demo at unidenvoice.com/get-started/book-a-demo or call 1300 881 662.