Resource:

Ideas about Vulnerabilities—and Safeguarding Organizational Ombuds (OO) Confidentiality and Independence When Collecting and Using Data to Illuminate OO Value

2026

Note: Please see these ideas as brainstorming rather than legal or technical advice. Each ombuds has their own practice and organization so generalities may not be useful to everyone. The world we live in is changing very fast. In addition, many portions of this "working draft" were generated by AI. (AI-generated sections are signified with red headings or text.) Because AI may provide inaccurate, inadequate, quickly out-of-date, and even offensive information, please consider ideas here only as a starting point for your own research. And please do critique and share good ideas.

This working draft consists of six sections:

I. Introduction
II. Reviewing Confidentiality Vulnerabilities re: OO Data
III. Reviewing Core Principles in Ombuds De-identification
IV. Not Using Dates or Masking Dates in a Database or Checklist
V. Understanding Confidentiality in Cloud Storage
VI. An AI-Generated Privacy Snapshot About Surveys for Ombuds

I. Introduction

We are continually learning of organizational ombuds colleagues who believe their data were inadvertently made available or moved—or hacked or copied—or copied and keyword searched—or demanded—from inside or outside their organizations. We present some ideas for gathering and keeping operationally useful data that illuminate OO value, with less risk, from inside and outside your organization. Several ideas relate to keeping data that would not likely betray personal identities even if leaked. (See the Checklist articles in the Resource Repository.) Some points relate to a detailed database and personal notes.

Here are some past-history concerns: People overhearing an office visit or phone calls, picking up or reading papers from a desk, or gaining access to one's computer or, in some cases, being given access after a subpoena. Therefore, OOs have been taking names and email addresses and phone numbers out of our records.

Our additional new concerns are many. AI is changing the landscape—and the airwaves.

All digitized data that are online—theoretically—can be accessed and recorded in transit. **(And of course your database also could be subpoenaed even if offline.) While no method is entirely foolproof, two reasonable approaches to collecting, using, and keeping data without endangering the International Ombuds Association (IOA) Standards of Practice are: 1) Keep it "air-gapped"—i.e., entirely offline—and routinely delete or shred it, or 2) collect and use and keep only those data that both illuminate Ombuds value and effectiveness *and* are IOA Standards of Practice compliant.**

Transgressors can be inside or outside the organization, individuals or groups or foreign nations or competitors interested in phone calls or written communications or the OO database. They might be interested in just one case, for example, like a plaintiff suing the organization—or ill-wishers who record a lot of organizational traffic to be searched…days or even years later.

All the privacy concerns of the past still exist, and some now are amplified by AI. AI can record enormous

amounts of data and then do *keyword searches* and *"interrogations" of ideas.*[1] In addition, data that are successfully stolen can be *altered*—to *add or delete* numbers*, words, and images—or otherwise misused.*

These points mean that Ombuds need to consider how they accept data, collect and assess data, and how they store and use and communicate data.

1. **Step One in data collection: Ask your constituents (in general) what they might wish to know and list what you wish to know about your practice**. Do you have any need to keep names and other identifiers? If so, can you keep identifiers only in a paper calendar, keep notes on paper—and then shred, routinely?

2. **Read this International Ombuds Association blog post from 2025, by Reese Ramos:**
   The Evolving AI Reality and Confidentiality in the Ombuds Practice.

3. **Read the AI-generated advisories about OO data vulnerabilities, and OO responses, that are included in this memo.**

4. **Consider using only your *own* electronic equipment and apps**, if you are going to accept or collect data online. (And even if you are not going to *collect* data through electronics, you may decide that you need to own some of your own electronics anyway.) Relevant devices include your phone(s), calendars, VOIP, computer, use of interpreters, AI assistance apps like chat and generative AI, translators, Zoom, Meet, etc. If you do not want others to be able to access data from your use of electronic equipment, at least set controls to no recording where possible and check the app meticulously for other privacy safeguards. For each device you use, consult experts and perhaps use AI to find out how to minimize threats to of confidentiality.

5. **Please consider researching the confidentiality issues associated with keeping an office calendar** and choose the calendar system that best fits your practice and organization and needs for confidentiality.

6. **Consider keeping your ombuds data at home on a dedicated computer that is not online. Or at the office on a dedicated computer that is not online**. Consider keeping *paper* notes about issues, Most Serious Cases, etc., at the office—and take them home and shred them on a regular basis. Share data with your office colleagues on hand-carried hard drives.

7. **For relatively safe (and quick) input:** Consider an Outcomes Checklist about achievements, where you can track, in very general terms, some outcomes of your work as you become aware of them—and a weekly Friday Checklist about your functions, issues, risks, visitor choices, etc. See the Resource Repository Index for articles about these two checklists.

8. **For small caseloads, consider keeping all the data yourself, name-free, in a private place, on paper**. And shred according to an explicit policy.

---

[1] **Interrogating a text by AI goes beyond keyword searching. It involves using AI technologies to understand and analyze the text more deeply:**
Natural Language Processing (NLP): AI uses NLP to comprehend language, context, and semantics.
Extraction and Summarization: Extracts key information and may summarize content.
Sentiment Analysis: Determines the sentiment or emotional tone of the text.
Pattern Recognition: Identifies patterns or themes within the text
Contextual Understanding: AI considers the context to provide more nuanced responses.

9. **For the OO Office Database and especially for large caseloads, consider consulting with a cyber expert about anonymizing your database.** Some OOs have neglected to *remove or mask the dates* when they have helped a visitor. Investigate the possibilities for masking dates that apply to your own situation.[2] This will help to discourage anyone from trying to use your database to find what you what you were doing and with whom you were meeting, on a certain day.

   In a large database, consider collecting *non-identifiable* demographics and geographics (location) about both your initial visitors and any respond*ent* visitors (e.g., alleged offenders). For example, tag initial visitors and respond*ent* visitors with their major job cohort, large organizational units (e.g. Faculty, School of Business) and geographics (e.g., name of country, name of bureau or agency or School). And consider not using such tags unless the units are very large.

10. **If you keep data about respon*ders* (those that help with a case), track just their general function:** e.g., Admin Staff or Leadership, Compliance Officer.

11. **Do consider tracking many issues in a large database** —so you can clump and cross-tabulate issues—*but consider doing so in databases where the dates are masked, the data are on your own dedicated computer—and offline.*

12. **Collect data from organizational engagement surveys** that include your office. (Ask to have your office included in these surveys where relevant).

13. **Collect data about the use of your website, and feedback** from presentations and letters, interviews, and articles, etc.

14. **Collect data from your own surveys in ways whereby you keep no lists of survey recipients**. For example, attach the survey URL to your signature when you reply to initial visitors, alleged offenders and responders. If you see people in person, offer self-addressed paper forms to them as they leave. Consider using survey platforms that are unlikely to compromise confidentiality and use all their safeguards. (As a starting point, see the section of this article on survey platforms.)

II. Reviewing Confidentiality Vulnerabilities re: OO Data

Reported by AI in 2026, with assists by Mary Rowe

A. Initial contact and scheduling

1. **Incoming phone calls to make appointments**
   - Landline or VoIP calls can be recorded by the carrier, employer systems, or call-recording features on either party's device, or by hacking.
   - Call metadata (numbers, times, duration) sit with telecom providers and can often be obtained by subpoena, with low thresholds in many jurisdictions.
2. **Emails used to request appointments**

[2] Dates can be "masked" in many ways by transforming them, so they are no longer directly identifying but still analytically useful. Consult the expert or AI of your choice about other ways of masking dates.

- Email content and metadata are stored on institutional and cloud servers, vulnerable to admin access, misconfiguration, breaches, hacking and subpoenas.
- Built-in “smart features” (auto-draft, classification) may send content to third-party AI services unless disabled.

3. **Web forms or online intake tools**
   - Data pass through web servers, logs, and application databases; insecure configuration can expose them to hacking or insider access.
   - If hosted by a vendor (case-management SaaS), provider staff or law enforcement can potentially access data via legal process to that vendor.
4. **Text/SMS, messaging apps (WhatsApp, Teams, Slack, etc.)**
   - Messages may be stored unencrypted on devices and in cloud backups; providers can be compelled to disclose some data by subpoena or warrant, depending on jurisdiction and encryption. Hacking.
   - Screenshots or forwards by the other party (visitor, manager) can create uncontrolled copies with no expectation of confidentiality.

B. In-person and live meetings

5. **Conversations in shared physical spaces (hallways, lobbies, cafés)**
   - Others can overhear names, issues, or the fact of contact with the ombuds if conversations occur where colleagues or bystanders pass.
   - Cameras or microphones in “smart” buildings or security systems may incidentally capture audio or video.
6. **Meetings in the ombuds office or conference rooms**
   - Visitors or others may intentionally or unintentionally record using phones, laptops, wearables (smartwatches, eyeglasses, earbuds) or built-in meeting-assistant apps.
   - Building security systems or IT monitoring may log door access and room bookings, revealing who met with the ombuds even if content is not recorded. Hacking.
7. **Hybrid or virtual meetings (Zoom, Teams, Meet, etc.)**
   - Platform features like AI companions, auto-transcription, or recording may be enabled by default and store transcripts and summaries in the vendor’s cloud. Hacking.
   - Meeting metadata (participants, times, IP addresses) reside with the platform and can be subject to legal process or vendor access. Hacking.

C. Use of devices and apps during ombuds work

8. **Ombuds’ computers, phones, and tablets**
   - Keylogging malware, spyware, or compromised operating systems can capture notes, emails, and case-management data.
   - Employer or IT admin tools (remote monitoring, log collection, backups) can access files and logs unless the office is technically segregated and protected.
9. **Visitors’ devices in the room**
   - Visitors may run voice-assistants, smart-pens, or transcription apps that record sessions without fully appreciating the confidentiality implications.
   - Cloud-connected note-taking apps (Otter, Read, Notion, etc.) can upload audio and transcripts outside the ombuds’ control. Hacking.
10. **Translation apps and interpretation tools**
    - Speech-to-text translation services may send raw audio/text to external servers where it can be logged, retained, hacked, or used for model training.
    - Third-party interpreters (humans or services) become additional confidentiality and subpoena points unless tightly contracted and instructed.
11. **AI assistants, chatbots, and generative tools used by the ombuds**
    - If the ombuds pastes case details (even “anonymized”) into external AI tools, those services may store and reuse the prompts unless strict enterprise controls are in place.
    - Logs of AI prompts and outputs can be discoverable or subpoenaed as organizational records, especially if tied to identifiable patterns.

D. Note-taking, databases, and storage

12. **Handwritten notes on paper**
    - Physical notes can be seen by others if left on desks, in unlocked drawers, or carried through public spaces.
    - Paper notes can be seized under some subpoenas or search warrants unless clearly outside the office's record-keeping practices and protected by agreement/statute.
13. **Local electronic notes (Word files, spreadsheets, personal notes)**
    - Documents stored on institutional servers or synced folders (OneDrive, Google Drive) are visible to system administrators and vulnerable to breaches, and hacking.
    - Backups and shadow copies may persist even after deletion, making "cleanup" difficult if data must be minimized.
14. **Ombuds case-management databases**
    - Databases on institutional or vendor servers can be targets for hacking (credential theft, misconfiguration) or insider access.
    - Unless designed with strict data-minimization and de-identification, and masked dates, fields may make it possible to identify visitors.
15. **Analytics and reporting dashboards**
    - Aggregated dashboards may hold searchable data that could be drilled down to small cells, especially if dated, inadvertently re-identifying people.
    - Screens viewed in meetings or left open can be seen or photographed by others in the room.
16. **Email or messaging used to store "working notes"**
    - Some practitioners inadvertently treat their inbox or chats as a quasi-database, increasing exposure to IT monitoring, e-discovery, and subpoenas.

E. Communication with others about a case

17. **Consulting with other conflict-management professionals (HR, Title IX, legal, etc.)**
    - Phone, email, or chat with colleagues creates new records on multiple systems (their inboxes, logs, case files) that can be accessed, hacked, or subpoenaed.
    - Meeting in their offices may expose details to their note-taking practices, minutes, or ticketing systems.
18. **Consulting external experts (psychologists, threat-assessment, outside counsel, other ombuds)**
    - Any written description (emails, memos, secure messaging) adds another storage and subpoena point in the expert's systems which are similarly open to access.
    - Cross-border communication can bring other jurisdictions' data-access laws into play.
19. **Upward reporting of trends and systemic issues**
    - Written reports or slide decks for leadership may include small-n examples or phrasing that could be tied back to identifiable people.
    - Copies stored in leadership's email or shared drives increase surfaces for breach, search, hacking or subpoena.
20. **Good-news reports and feedback about specific actions**
    - Even positive feedback (e.g., "X manager handled Y case well") can, in a small unit, or specific time period, reveal that a particular employee raised a concern.

F. Organizational/external surveillance and interception

21. **Network monitoring by the institution**
    - Firewalls, IDS/IPS, and logging systems and hacking may capture traffic metadata and, in some setups, content (e.g., proxy logging of HTTP/S) involving the ombuds office.
    - Misconfigured logging could retain sensitive URLs, subject lines, or message bodies longer than necessary.
22. **Endpoint monitoring or mobile-device-management (MDM) tools**
    - Screen capture, keystroke logging, or file inventory tools used by IT on

organization-owned devices may inadvertently capture confidential ombuds data. Hacking.
    - "Remote wipe" or remote-access functions can be abused or misused, exposing content during troubleshooting.
23. **Spyware and state-level surveillance (Pegasus-type tools)**
    - Advanced spyware, now steadily more available, can silently turn phones into 24-hour microphones and cameras, capturing ombuds meetings and calls.
    - Such tools can exfiltrate stored notes, contacts, and messages to third parties without any local indication.

G. Legal process: subpoenas, discovery, court orders

24. **Telecom and platform records (phone, SMS, email, videoconference providers)**
    - Prosecutors or civil litigants can subpoena call logs, IP logs, and, in some cases, content from third-party providers under relatively low standards, especially in the U.S. under the third-party doctrine.
    - Even if content is encrypted end-to-end, metadata about "who contacted the ombuds when" is often available.
25. **Institutional records and IT systems**
    - Any ombuds-related data stored on central institutional systems (mail, storage, ticketing, backups) can be swept into e-discovery if not clearly excluded by charter/policy and excluded in practice.
    - Courts may order production unless strong privilege, statute, or negotiated protections apply.
26. **Vendor-held data (case-management, AI, transcription, cloud tools)**
    - Vendors can receive subpoenas or orders directly; the ombuds may not be notified in time to contest. Hacking.
    - Contract terms often govern whether vendors will resist disclosure or notify the client; weak terms increase risk.
27. **Personal devices and paper records**
    - Search warrants or discovery demands may seek devices or paper files if courts view them as organizational records, especially absent clear data-minimization policies.
    - Even where ombuds programs usually succeed in resisting such orders, the risk and burden are real and must be planned for.

III. Reviewing Core Principles in Ombuds De-identification (as reported by AI, 2026)

In ombuds practice, "de-identification" usually means stripping out or never collecting details that could reasonably let someone deduce who raised what concern, while still preserving enough information to see patterns and support systems work.

- **Collect minimal identifying data up front.** Many ombuds offices either avoid recording names/IDs altogether or keep them only in temporary, local notes that are routinely destroyed, never in the main tracking system.
- **Keep records separate and independent.** Best-practice guidance urges ombuds to maintain any working statistics or logs in systems that are technically and administratively separate

from organizational IT and are offline, and to avoid serving as a repository of HR-style personnel files.
- **Report at aggregate or "generic" levels.** When ombuds share themes, patterns, or recommendations, they do so in ways that protect identities—generalizing roles, units, and timing enough that reasonable readers cannot infer who came forward.

Data entry and case tracking

- **Strip identifiers at data entry.** One article in the *Journal of the International Ombuds Association* describes an ombuds practice of removing all personal identifiers at the point of data entry into the database, with no pseudonyms or codes that would allow straightforward re-identification.
- **Use broad categories rather than specifics.** Offices typically code cases by high-level variables—visitor role category, broad type of issue, broad organizational area—rather than specific names, job titles, or narrow units.
- **Avoid "A-number level" or similar IDs unless required.** Where identifiers are necessary, advocates push for strong rules to keep such IDs out of general reporting and to protect them as sensitive personally identifiable information.

De-identifying narrative information

- **Remove direct identifiers from narratives.** When writing notes or examples for internal use, ombuds remove names, exact titles, and direct references (e.g., "the only female neurosurgeon") that would immediately point to a person.
- **Mask quasi-identifiers through generalization.** Borrowing from broader de-identification practice, ombuds generalize or avoid details like dates, locations, roles, or demographics so that combinations of facts do not single out an individual or tiny group.
- **Use composite or "typified" examples.** For training or systemic reports, ombuds often blend elements from multiple cases into a single composite story to illustrate a pattern without exposing any one visitor—and declare the story to be de-identified.

Aggregation and thresholding for reports

- **Aggregate over time and units.** Periodic reports (e.g., annual or semi-annual) group issues across months and across units so individual events are not temporally or organizationally traceable.
- **Apply minimum cell sizes.** Some ombuds avoid reporting statistics where a category has few cases, to prevent back-tracking to a particular person or incident.
- **Focus on issues, apparent risks, and ombuds services, not individuals.** Reports emphasize types of problems (e.g., values and ethics, safety, financial risks), systemic patterns, and organizational factors rather than "who did what to whom."

Storage, access, and destruction

- **Keep no permanent confidential records on behalf of the organization.** International Ombuds Association (IOA) Standards and Best Practices say ombuds should not create or maintain records containing identifying or identifiable information "for the organization"; they maintain only what they need for their informal work.
- **Secure, limited-access storage.** Any working notes or statistics are stored in locked spaces or restricted systems accessible only to ombuds staff, with regular purging of anything that could identify visitors.
- **Consistent destruction practices.** Standards call for a "consistent practice for the timely destruction" of confidential information—e.g., shredding paper notes, wiping temporary files—wherever the data exist—so that if data were subpoenaed thereafter, they no longer exist.

De-identification when using AI and external tools

- **Avoid sending identifiers to external AI tools.** Emerging guidance warns that even

"anonymized" prompts to public AI services can be risky if they combine rare facts; ombuds are urged to either avoid such tools or use tightly controlled ones. (See the short article in this Resource Repository on choosing an AI provider.)

- **Double-check outputs for re-identification risk.** When AI or analytics tools help with theme detection, ombuds must manually review outputs to ensure small groups or unusual combinations of attributes are not exposed in reports and that no additions or deletions occur through use of AI.

IV. Not Using Dates or Masking Dates in a Database or Checklist

Consult with a cybersecurity expert if possible and ask *if it is possible not to keep dates within a year.* Or to randomize the dates within the preceding 51 weeks.

Common date-masking methods

Shift all dates by a fixed offset
Add or subtract a fixed number of days (for example, +90 days) from every date field, so relative intervals stay intact, but true calendar dates are hidden.

Apply random date variance
Add or subtract a random number of days within a chosen range (for example, −30 to +30 days) to each date independently, which makes re-identification harder but still preserves approximate timing.

Generalize or truncate dates
Store only the year, or year and month, instead of full date (for example, turning "2025-03-17" into "2025-03" or just "2025") so the data are less specific but still useful for period analysis.

Replace event date with intervals
Instead of event dates, use number of days since a specific but not obvious baseline, which removes the raw date while preserving many analyses.

Suppress or null when needed
For highly sensitive cases (or when exact timing is not needed), replace the date with null or a broad bucket such as "before 2010" or "2010–2014."

V. Understanding Confidentiality in Cloud Storage

Cloud storage can be evaluated along a set of security and governance parameters, which can be compared across providers like Microsoft 365, Sync.com, Tresorit, Proton Drive, and similar services.

Cloud Glossary: Parameter definitions

Zero-knowledge/end-to-end encryption
Whether encryption occurs on the client with keys only the user controls, so the provider cannot decrypt stored content.

Encryption in transit
Use of strong TLS/SSL for all data transfers between client and server and between data centers.

Encryption at rest

Use of strong algorithms (typically AES-256) to encrypt data on the provider's disk/servers.

Provider key access
Whether the provider holds or can access the keys needed to decrypt content (standard cloud) versus having no access (zero-knowledge).

Customer-managed keys/double-key
Options for customers to supply and control their own encryption keys, sometimes with schemes where both customer and provider keys are needed.

Jurisdiction/data centers
Primary legal jurisdiction and typical data center locations (e.g., US, EU, Switzerland, Canada) which affect privacy law and government access.

HIPAA/IRB suitability
Whether the service offers business/enterprise plans with compliance features (BAA, logging, access control) that institutions and Institutional Review Boards (IRBs) typically accept.

Default encryption coverage
Whether *all* stored content is protected by the strongest model (e.g., zero-knowledge) by default or only specific folders/features.

Collaboration features
Breadth of real-time co-editing, web apps, sharing controls, and integration with office tools.

Search and indexing
Ability to search file contents and metadata on the provider side; often reduced in zero-knowledge designs because content is opaque.

Worldwide access and data residency options
Global availability plus options to constrain storage to particular regions or countries (EU boundary, country-level residency).

VI. An AI-Generated Privacy Snapshot About Surveys for Ombuds January 30, 2026

Tool: BlockSurvey

Core privacy/security: End-to-end encrypted, "zero-knowledge" style; marketed as GDPR-aligned; no self-host, cloud only.

For ombuds use: Strong choice for highly sensitive, anonymous feedback where you can accept a privacy-focused third-party cloud and don't need on-prem hosting.

Tool: LimeSurvey
Core privacy/security: Supports encryption of stored data and some fields; EU-based and structured around GDPR; can be fully self-hosted or used as LimeSurvey Cloud.

For ombuds use: Attractive if your institution can self-host and lock it down; flexible for anonymous surveys, but you must design configs, access controls, and retention policies yourself.

Tool: Snap Surveys

Core privacy/security: TLS in transit, encryption at rest; ISO-style security posture; can run as a hosted service or be installed on your own servers.

For ombuds use: Good for organizations that want strong vendor security plus an on-premise option; suitable for a no personal information, ombuds climate and issue-spotting surveys where you still want robust controls.

Tool: Qualtrics
Core privacy/security: Enterprise-grade encryption in transit and at rest; supports GDPR compliance; cloud SaaS only with regional data-center options.

For ombuds use: Powerful for large institutions that already license it; excellent for complex surveys and dashboards, but heavier on data collection/retention than a minimalist ombuds office may prefer, so configuration discipline is critical.

Tool: SurveyMonkey
Core privacy/security: Encrypts data in transit (SSL/TLS) and at rest; has ISO-aligned security and GDPR/CCPA documentation plus a data-processing agreement.

For ombuds use: Widely available and easy to use; acceptable for many ombuds surveys if you enable anonymous responses, avoid all detailed identifiers, and carefully review collectors, metadata, and retention.

Note: This article draft is part of a Resource Repository designed to support identifying—and helping to quantify—the value of an Organizational Ombuds (OO). This Resource Repository is a work in progress. It is open to improvements, additions, deletions, critique, revision and random commentary. If any page in the repository is helpful, or needs revision, please let us know. Please contact Mary Rowe or other co-authors, if you can help to improve these pages or have another page to offer.