OPEN WAVELENGTH

Practical Tips

Robert Stewart

Director at APCO Canada

Confidentiality isn't a problem in public safety communications. It is a cornerstone of what we do. This article was written as a reflection for new and experienced communicators alike, a reminder of the everyday habits that protect those we serve. It celebrates the professionalism and quiet integrity that define our work across police, fire, and ambulance dispatch. These lessons aren't about preventing failure—they're about reinforcing the trust and excellence that already make our community strong.

Keeping Trust: The Heart of Confidentiality in Public Safety Communications

By Robert Stewart, Director of Public Safety Communications, City of Brandon

When someone dials 9-1-1, they give us more than information. They give us trust. They tell us things they wouldn't tell anyone else: where they live, what medications they take, who hurt them, or what they've just done. Police partners share details that could derail investigations if mishandled. Paramedics confide medical histories. Fire crews rely on us not to broadcast tactics over open air.

That trust is sacred. And it can vanish with a single careless comment.

Confidentiality isn't just another policy in a binder. It's the quiet promise behind every call we take—the invisible bond that keeps public safety functioning.

Information in the Communications Centre comes at us fast: Computer Aided Dispatch (CAD) entries, Canadian Police Information Centre (CPIC) hits, caller updates, radio traffic, and Emergency Medical Service (EMS) notes. It's easy to forget that every line on a screen represents a real person who trusted us with something private. We handle several kinds of protected data: personal information such as names and addresses; personal health information like medications or medical history; and highly sensitive law-enforcement data in CPIC. Each piece exists for one reason only—to help responders do their jobs safely and effectively.

The same principles apply across every discipline. Fire call-takers may receive confidential alarm codes, hazardous-material notes, or building layouts that could endanger crews or property if shared improperly. Ambulance communicators handle personal health information protected

under their province's version of the Personal Health Information Act (PHIA), sometimes while the caller is still in crisis. Whether it's a license plate, a patient condition, or a building entry code, each detail deserves equal care.

Most communicators would never dream of leaking a call to the media. Yet, many of us don't realize that oversharing *inside* the Centre can be just as risky. Peeking at a dramatic call you aren't working, passing along "juicy details" during shift change, or chatting about a case in the breakroom might feel harmless. But those habits quietly erode trust from within. Every access is logged. Every conversation leaves ripples. What starts as curiosity can end as a breach.

Imagine hearing another dispatcher handle a high-profile call and pulling it up "just to see." It feels like harmless curiosity, but unless you're directly supporting that event, it isn't need-to-know. Curiosity isn't authorization. Oversharing also takes other forms: telling the next shift colourful details about last night's call even though they don't need them, or relaying an off-the-record tidbit to a colleague "just so they know what happened." None of that serves operations—it's gossip disguised as interest.

The same principle applies when information crosses disciplines. For instance, an ambulance dispatcher might overhear details of a police file or see notes about a sensitive fire scene. Even though that information appears on your screen, it doesn't make it yours to share. The "need-to-know" rule isn't about silos—it's about purpose. If it's not directly helping someone respond or stay safe, it's not for discussion.

Confidentiality isn't about dramatic breaches; it lives in the small habits that shape our day. Locking your screen before stepping away is one. An unlocked console is an open door—anything done under your login looks like your action. Using a headset and keeping your voice low ensures that personal identifiers don't carry across the room. Practising radio discipline—transmitting only what responders need—reduces unnecessary exposure. Even the words you type in CAD matter. Keep comments relevant and professional; anything you enter could one day appear in court.

Each discipline faces its own version of this. For fire, it might mean keeping alarm codes or keyholder names secure. For ambulance, it's ensuring patient details aren't read aloud where others can overhear. For police, it's limiting identifiers over radio. The habits look different, but the principle is identical: protect the caller, protect the crew, and protect the trust.

The habit of confidentiality shouldn't stop when the headset comes off. After a tough shift, it's natural to want to debrief at home. But retelling calls to friends, neighbours, or family can expose people at their most vulnerable. What seems like an innocent story—"There was a big fire on Maple Avenue last night"—might help someone in the community identify the caller or victim. Once shared, you can't control where it goes.

Picture yourself at a barbecue when a neighbour asks, "Was that stabbing near my block?" You probably know exactly which call they mean, but confirming it would break confidentiality. A better answer is simple and professional: "I can't talk about specific calls, but it was a busy night." That keeps trust intact while still allowing you to talk about your work in general terms.

The same restraint applies when talking with colleagues from other services. For example, a police dispatcher chatting with EMS about a major crash might casually mention the driver's name or medical status. Unless that information helps coordinate care or safety, it's better left unsaid. We all share space and systems—but not every detail needs to travel between agencies.

Social media blurs the line between venting and revealing. A vague post like, "Another drunk driver tonight—some people never learn," can connect back to a real incident once friends or family start

guessing. Someone always connects the dots. Screenshots last longer than intentions. Even deleted posts linger in memory or archives. The safest rule of thumb: if a post even *might* link to a call, don't post it.

This risk extends beyond police stories. A post about "another overdose downtown" or "smoke still visible near the refinery" can point people straight to an incident. Even when names aren't mentioned, the public can piece things together faster than we expect.

CPIC access is one of the strictest privileges in Canadian public safety. Every search is audited, every transmission logged. Running a query "just to check" on a relative, old classmate, or new neighbour may feel harmless—but it's misuse, plain and simple. Think of CPIC as an evidence locker. You open it only when it's operationally required, handle what you need, and close it carefully when you're done. Anything else risks not only your own access but the integrity of the entire system as well.

For non-police communicators, the same spirit applies to any restricted system: medical databases, fire-inspection records, or provincial CAD portals. Access is a privilege earned through trust, and it carries the same responsibility.

Health details are among the most personal things a caller can share. When someone tells us about their medications, mental-health history, or conditions, they do so because they trust that we'll use that information only to help. That trust is backed by law through legislation such as PHIA in Manitoba. More importantly, it's backed by empathy. Before repeating a medical detail, even to another communicator, ask yourself: *Do they need to know this to do their job?* If not, keep it to yourself.

Imagine talking in the breakroom after a call and saying, "That overdose patient told me she was bipolar." Even if your co-worker is another dispatcher, that's still sharing personal health information unnecessarily. Confidentiality isn't suspended just because we're among our peers. For ambulance communicators, health information is the heart of every call. Diagnoses, medications, mental-health crises, and even caller tone are deeply personal data. These details should never appear in open chat channels or be repeated outside the need-to-know circle, even if shared between medical professionals.

Confidentiality is also about how we treat each other within the room. Not every dispatcher needs every detail. Shift briefings should focus on operational continuity, not storytelling. The "Did you hear what happened?" conversations after big calls might feel like bonding, but they often turn into gossip.

At handover, for instance, you might describe a domestic incident from the previous night in full detail even though the file is closed. The incoming shift doesn't need that context. What they do need is clarity about any follow-up tasks, outstanding units, or system notes. By keeping briefings focused, we respect both our colleagues and the people whose stories we hold.

Some Centres house police, fire, and ambulance dispatch under one roof. It's natural to be curious about what's happening on the other side of the room, but the same boundaries apply across agencies. Just because a call could be visible on your screen doesn't mean it's yours to explore or discuss. Each service has its own confidentiality obligations, and respecting them is a sign of professionalism.

When we limit information to those who truly need it, we create a culture of mutual respect. If we normalize discretion inside the Centre, we strengthen our ability to protect confidentiality outside it.

Everyone slips. Maybe you sent an email to the wrong address or left your screen unlocked. The most important thing you can do is report it right away. Quick reporting allows supervisors to contain the situation, notify the right people, and

demonstrate integrity. Hiding a mistake almost always causes more harm than the mistake itself.

Imagine realizing you've emailed call details to the wrong officer, or paramedic supervisor, or fire chief. It's tempting to ignore it and hope no one notices. Don't. The sooner you come forward, the sooner it can be fixed and the stronger your credibility remains.

Confidentiality isn't about fear of discipline—it's about professional pride. Every time you handle information properly, you reinforce the bond that allows people to pick up the phone and trust a stranger with their crisis. Every time you keep a detail to yourself, you reaffirm the integrity that makes public safety communications work.

Whether you're dispatching a police pursuit, coordinating a medical response, or directing fire crews into a burning structure, you're trusted with information that could change lives. Protecting that trust isn't just about compliance … it's about respect for the people we serve and the partners we work beside.

We're not guarding secrets; we're safeguarding people. Every name, address, and note is a piece of someone's life, often the hardest moment of it. How we handle those fragments defines us as professionals.

Protecting information is part of doing the job well. It sharpens focus, builds discretion, and shows pride in the craft. When you lock your screen, keep your radio transmissions concise, or resist curiosity, you're not "avoiding trouble." You are demonstrating the qualities that make a great communicator: calm, trustworthy, and dependable. You're strengthening the public's faith that their story is safe with you.

Confidentiality is confidence. Confidentiality is trust. Confidentiality is professionalism.

When we live those values every shift, we strengthen the foundation of public safety in Canada rather than "just following policy." Every voice on the line, every record on the screen, every story we keep safe is proof of one thing: we are trusted, and we intend to stay that way.