Crisis Coordination in Public Services:

Secure Collaboration for Rapid Response

Mattermost

Public services organizations, law enforcement, and first responders are the cornerstone of safe communities. The public expects these organizations to be ready to respond rapidly to emergencies and deliver essential services around the clock no matter the circumstances.

But as natural disasters, cyber threats, and operational complexities increase, the need for better coordination and faster response times does, too.

When emergencies strike, public services and first responder organizations need to act fast to protect lives and maintain public trust. To fulfill their missions, these organizations need secure, real-time collaboration tools that keep their teams connected wherever employees happen to find themselves — even when primary systems fail.

Why Public Services Need Secure Collaboration

In public services, speed and reliability of communication can make all the difference in the world.

According to a Pinkerton study, police officers have an 85% crime clearance rate when they arrest suspects within 15 minutes — compared to just 34% when the process stretches beyond that. Similarly, research shows that delays of more than 15 minutes in activating hospital rapid response teams significantly increase in-hospital mortality and prolong patient stays.

Unfortunately, without the right communication tools in place, response times suffer — and cybercriminals are making the problem worse.

Attacks on public safety systems are becoming more common, prompting warnings from the U.S. Department of Homeland Security. According to a December 2023 report, 91% of first responder agencies experienced a cyber incident — like a phishing or malware attack — within the previous 12 months.

If your agency hasn't been hit yet, it's only a matter of time.

What You'll Learn

In this guide, we'll examine how secure real-time collaboration tools can help public service organizations, law enforcement agencies, and first responders strengthen their defenses against growing cyber threats while boosting operational resilience. We'll also share best practices for establishing secure, reliable communication across your teams — along with some real-world examples of how public services organizations are using Mattermost to protect and accelerate mission-critical operations.

In healthcare, the story's the same: An attack against Ardent Health in late 2023 forced emergency rooms offline in New Mexico, Texas, and Oklahoma, highlighting the critical need for secure communication and robust incident response capabilities across the industry. With research suggesting that miscommunication is a main driver of medical malpractice claims — costing healthcare organizations $1.7 billion and nearly 1,750 patient deaths over a five-year period — secure collaboration isn't just a nice-to-have; it's a mission-critical matter of patient safety and operational viability.

To minimize risks, healthcare systems, law enforcement agencies, and other emergency services need communication tools that are resilient, adaptable, and secure. Simply put, when lives are on the line, these organizations can't afford to be offline.

Cyberattacks & Compliance:

The State of Public Service Operations

From law enforcement to emergency healthcare providers, public services agencies face unprecedented challenges. Not only do they need to keep vital services running around the clock, these organizations must enable distributed teams, navigate legacy systems, and manage digital tools that weren't designed with today's threat landscape in mind.

When communications systems go down in these environments, the impact is immediate and severe. Communication outages can delay 911 dispatches, stall police responses, and disrupt hospital coordination — putting lives at risk while eroding public trust.

At the same time, cyberattacks against first responders and public services are on the rise; the Public Safety Threat Alliance reports that an average of one public safety organization is attacked every day. Healthcare systems have also been targeted; according to Microsoft, 389 U.S. healthcare providers were hit with ransomware within the last year, forcing facilities to incur costs of up to $900,000 in downtime each day, with 99 of these organizations paying ransoms averaging $4.4 million. As regulations like HIPAA, CJIS, and the NIS2 Directive get even tighter, public agencies are under pressure to ensure both operational resilience and compliance.

In a sector responsible for protecting the citizenry and ensuring public safety, operational downtime is simply not an option. To fulfill their missions, public service organizations need to invest in secure, real-time collaboration tools and implement robust incident response strategies to maintain mission-readiness — and keep communities safe no matter what.

From Fragmented Tools to Compliance Headaches:

Key Communication Challenges for Public Services Agencies

Public services agencies, law enforcement, and emergency response teams operate in some of the highest-stakes environments imaginable. A single missed radio call or misrouted dispatch can have disastrous consequences, from delayed response times to loss of life.

By overcoming the three key collaboration challenges they face — fragmented communication tools, increasingly sophisticated cyberthreats, and stricter compliance mandates — agencies can mitigate these risks while strengthening operational resilience.

Challenge #1:

Fragmented Tools, Legacy Systems & Data Silos

Many public services organizations still rely on patchwork communication systems that include legacy radios, emails, smartphones, and ad-hoc group chats. Not only are such systems inefficient, they also create data silos — something that more than 80% of government organizations experience. In fact, just 2% of government leaders say their employees can access all of the organization's data.

Making matters worse, these siloed systems aren't built to respond urgently to emergencies. As a result, fragmented communication tools often put a damper on situational awareness and slow down response times. Agencies understand this perfectly: One report found that 89% of law enforcement departments worry about the impact legacy systems might have on the way their organizations would be able to respond during major events and cyberattacks.

By investing in a secure collaboration solution built for high-stakes environments, first responders can centralize communications, shatter silos, and make faster decisions when every second counts — serving the public better because of it.

JUST 2% OF GOVERNMENT LEADERS
say their organization's data is entirely accessible.
(Workday)

From Fragmented Tools to Compliance Headaches:

Key Communication Challenges for Public Services Agencies

Challenge #2:

Cybersecurity Risks

Hackers are increasingly targeting public safety organizations and healthcare systems, with 91% of first responders and 92% of U.S. healthcare organizations experiencing a cyberattack within the last 12 months. Not only do these attacks disable dispatch systems and compromise sensitive patient data, they shatter public trust and make communities less safe.

The financial impacts can be severe, too. In 2023, ransomware payouts reached an all-time high of $1.1B, which is even more troubling because many organizations that make these payments never see their data returned.

Add it all up, and implementing robust cyber defenses and a resilient communication layer is no longer a nice-to-have for public services and law enforcement agencies. It's mission-critical.

92% OF HEALTHCARE ORGANIZATIONS AND 91% OF FIRST RESPONDERS experienced a cyberattack within the last year. *(Ponemon Institute and Mark43)*

Challenge #3:

Compliance requirements

Public services organizations, law enforcement agencies, and first responders need to navigate an ever-growing web of cybersecurity, privacy, and operational regulations. From HIPAA and CJIS in the United States to the NIS2 Directive in the European Union, compliance requires data security, auditability, and secure handling of sensitive communications.

When organizations fail to comply with relevant regulations, it can lead to steep fines, lawsuits, and other suboptimal outcomes. To remain compliant and mission-ready, public services organizations need to adopt tools that centralize collaboration, maintain audit trails, and ensure adherence to local and national regulations.

A COLORADO HOSPITAL SYSTEM WAS FINED NEARLY $550K for HIPAA violations following a phishing attack. *(The HIPAA Journal)*

From Fragmented Tools to Compliance Headaches:

Key Communication Challenges for Public Services Agencies

Hidden Threats:

Cyber Risks & Regulatory Hurdles in Public Safety

From ransomware and phishing attacks to outdated legacy systems, public services, law enforcement, and first responder organizations face growing cybersecurity threats. As emergency communications systems become more interconnected — spanning healthcare networks, dispatch centers, and field operations — attackers have more opportunities to disrupt mission-critical services.

And the stakes keep getting higher. According to IBM's 2024 Cost of a Data Breach Report, the average data breach costs $4.9 million to resolve. For essential services, the damage goes beyond dollars, threatening lives and public safety. When the one ransomware attack took critical systems offline and forced emergency rooms to close, countless patients didn't have access to timely care because they either couldn't access facilities or sought treatment at unaffected hospitals that were much more crowded than normal.

Compliance adds even more complexity to this problem. To comply with the alphabet soup of regulations — NIST, HIPAA, and CJIS, for starters — organizations need not just secure systems but also reliable audit trails, documented workflows, and reliable cross-team coordination when the pressure is highest.

Since so many public sector organizations are still relying on siloed comms tools and legacy systems that weren't built for today's complex threat environment, teams can struggle to respond quickly to incidents — putting security, compliance, and public trust at risk.

THE AVERAGE DATA BREACH COSTS ORGANIZATIONS $4.9 MILLION

(IBM)

Secure Collaboration:

The Key to Resilient Public Services

In mission-critical sectors like emergency services and law enforcement, secure collaboration is now table stakes.

When organizations rely on fragmented tools and legacy systems, operations can run into dangerous delays and miscommunication during time-sensitive situations. By connecting all stakeholders — dispatchers, field responders, firefighters, police officers, healthcare staff, and command center personnel — across a single, secure collaboration platform, agencies can ensure that everyone stays informed and coordinated in real time, no matter where they happen to be or what the circumstances are.

By choosing a secure collaboration platform with mobile capabilities, responders in the field can access important updates, communicate seamlessly with headquarters, and otherwise stay in the loop — even in low-connectivity environments or during large-scale crises.

Beyond real-time communication, secure collaboration tools can also streamline and automate incident response. Integrations with alerting systems and monitoring platforms enable agencies to escalate incidents quickly, launch predefined response playbooks, and minimize manual coordination — all of which helps teams contain threats faster. Plus, role-based access controls (RBAC) ensure that only authorized personnel can access sensitive operational data — protecting both public safety and agency systems.

Public services organizations are under constant pressure to serve communities efficiently, maintain compliance, and respond swiftly to emergencies. With a secure collaboration platform sitting at the center of operations, agencies can increase resilience, focus, and adaptability — all while protecting lives and preserving public trust.

Secure Collaboration:

The Key to Resilient Public Services

What to Look for in a Secure Collaboration Platform

To fulfill their missions, public services organizations, law enforcement, and first responders need secure collaboration tools. But with so many options available, finding the right fit can be tricky.

Agencies looking to become more resilient and adaptable should prioritize solutions that offer the following capabilities:

- **Self-hosted or private cloud deployment.** By hosting the platform in a private cloud or on-prem environment, agencies maintain complete control over sensitive operational data. This makes it easier to comply with government security standards and regulations while helping organizations ensure continuity during critical incidents.
- **Customizability and extensibility.** A flexible platform with open APIs, granular admin controls, and strong integration capabilities allows teams to customize workflows based on the way they work — enabling them to build the perfect tool for the job and accomplish more every day.
- **Integration with existing mission-critical tools.** The ideal platform should also connect seamlessly to legacy systems — including dispatch systems, hospital records, incident reporting platforms, and security tools — to centralize communication, increase focus, and reduce operational complexity.
- **Support for interagency collaboration.** By choosing a platform that enables users from multiple agencies to collaborate seamlessly, you can ensure technical teams, leadership, and frontline responders can stay on the same page during any scenario.
- **Audit trails and compliance features.** To meet compliance mandates and data governance rules, agencies should choose platforms with built-in audit logs, role-based access controls, and real-time reporting capabilities, among other compliance features.

Best Practices:

How Secure Collaboration Makes Public Services & Law Enforcement More

Emergency services, law enforcement, and first responders do more than provide essential services. They're the first line of defense when it comes to protecting lives and keeping the public safe.

From hospitals and police departments to fire crews and disaster response units, these teams need to be able to communicate in real time, share sensitive information securely, and coordinate under pressure — often in life-or-death situations.

While every agency has unique demands, following these best practices can help organizations build a secure collaboration framework that improves outcomes and makes communities stronger and safer:

1. Establish a Unified Secure Communication Framework
2. Build Resilient and Redundant Communication Systems
3. Boost Efficiency with Integrated Collaboration Tools
4. Train Teams Continuously on Secure Communication Practices
5. Implement Proactive Threat Detection and Incident Response Protocols

1. Establish a Unified Secure Communication Framework

In public services, secure communication is more than a cybersecurity issue. It's fundamental for maintaining public trust and ensuring operational continuity. When collaboration breaks down between field responders, dispatch, and central command, the consequences can be devastating.

By establishing a unified communication framework, agencies can streamline operations, reduce delays, and ensure all teams — from hospital staff to police officers to 911 dispatchers — stay on the same page.

Execution Steps:

1. Audit current tools to determine what's fragmented and identify any gaps that might exist
2. Deploy a secure platform that brings everyone together and offers encryption at rest and in transit, multi-factor authentication, and role-based access controls
3. Ensure secure mobile access for teams in the field by choosing a solution that offers Android and iOS apps
4. Centralize messaging, document sharing, and decision-making in one platform

2. Build Resilient and Redundant Communication Systems

Resilient communication is mission-critical during crises. Whether it's a natural disaster, cyberattack, or mass casualty event, emergency responders need communication tools that can function even when traditional systems fail.

In addition to rolling out a primary communication network, public services agencies should deploy out-of-band solutions that remain operational even in degraded conditions. By doing so, they can ensure that teams can still make life-saving decisions quickly, no matter the circumstances.

Execution Steps:

1. Implement a self-hosted or private cloud collaboration platform you can access when primary networks fail
2. Deploy dedicated backup communication channels for out-of-band communication
3. Ensure mobile apps can operate in low connectivity areas
4. Design cross-agency protocols for redundancy and failover

3. Boost Efficiency with Integrated Collaboration Tools

When every second counts, the consequences of fragmented tools and siloed systems can be deadly. Whether it's patient care handoffs or cross-agency incident response, disjointed comms slows coordination down, putting people at risk.

Integrated collaboration tools that connect with hospital electronic health records (EHR), computer-aided dispatch (CAD) systems, records management systems (RMS), and internal reporting tools give teams the real-time visibility they need to act quickly — and with confidence.

By choosing an open core collaboration solution, agencies can connect to critical systems and pull data into dedicated channels, consolidating all important information and creating a single source of truth, streamlining incident response.

Execution Steps:

1. Use extensible collaboration platforms that integrate with core systems (e.g., EHR, CAD, and RMS)
2. Standardize workflows for incident escalation and resource deployment
3. Automate notifications and alerts for improved coordination
4. Centralize communication across agencies and departments to increase alignment

4. Train Teams Continuously on Secure Communication Practices

Most security breaches start with a person — not a piece of code. In fact, by one estimate, as many as 95% of all breaches begin as phishing attacks targeting unsuspecting employees. Since first responders, police officers, and healthcare workers are always under a huge amount of pressure, this makes them ideal targets.

Training your team to recognize threats, use secure communication channels, and flag suspicious activity is key to maintaining operational security.

Execution Steps:

1. Offer role-based training for different departments and roles
2. Conduct phishing simulations and real-world scenario training
3. Hold quarterly refreshers on new threats and secure tool usage
4. Reinforce secure behaviors with peer recognition and rewards

5. Implement Proactive Threat Detection and Incident Response Protocols

In emergency services, the stakes are perhaps higher than any other industry; any system downtime, however brief, can mean lives lost. That's why proactive threat detection and incident response need to be baked into the foundation of your operations.

From cyberattacks on hospital networks to compromised dispatch systems, response protocols must be tested, documented, and quickly actionable to keep the public safe.

Execution Steps:

1. Build response plans for scenarios like ransomware, outages, and data breaches
2. Automate containment workflows to minimize the spread
3. Use AI-driven monitoring tools and automation to flag unusual behavior early
4. Review incidents regularly and update protocols as needed

The Mattermost Advantage for Public Services & Emergency Response

In high-stakes public service environments — where every second matters and secure, reliable communication is non-negotiable — Mattermost serves as a central, mission-ready collaboration hub.

By delivering real-time secure communication, workflow automation, and complete collaboration control, Mattermost empowers emergency services, healthcare teams, and government agencies to respond faster, reduce friction, and stay aligned when it matters most.

What does this all look like in the real world? Here are some battle-tested use cases:

- **Multi-agency incident command.** Mattermost enables seamless coordination between EMS, fire, police, and public health departments during joint operations or disaster response. Share updates in real time, assign responsibilities, and maintain full visibility and a single source of truth throughout the incident lifecycle.
- **Field team communications.** Keep first responders, utility crews, and on-site personnel connected to dispatch and command centers with Mattermost — even in low connectivity or high-stress environments. Share location updates, incident photos, and real-time status reports in secure channels to streamline coordination and support faster action in the field.
- **Digital briefs and shift handoffs.** By centralizing collaboration, Mattermost enables public service agencies to replace whiteboards and email chains with secure digital briefings only accessible by authorized users. Share arrest logs, status updates, pending tasks, and officer safety bulletins in dedicated channels to ensure continuity between shifts.
- **Disaster preparedness drills**. As Miguel de Cervantes once wrote, being prepared is half the victory. With Mattermost, you can run simulations for natural disasters and mass violence events with built-in playbooks. By practicing turning on crisis communication channels, mobilizing teams, and logging response activities, agencies can increase preparedness and stay mission-ready.
- **Compliance logging.** Mattermost helps agencies ensure compliance by automating record-keeping to meet regulatory requirements. Every action — from message posts to task assignments — is logged with timestamps and full audit trails. Admins can easily export data for audits, FOIA requests, or internal reviews — all without disrupting operations.

The Mattermost Advantage for Public Services & Emergency Response

Public services and law enforcement agencies trust Mattermost because it helps them strengthen operational resilience with:

- **Enterprise-grade security**, including encryption, role-based access controls, and self-hosted deployment for complete data sovereignty;
- **Custom integrations**, with the ability to connect to RMS, CAD, GIS, EHR, and any legacy systems;
- **Scalable infrastructure** that supports large, distributed teams across jurisdictions, enabling tens of thousands of users to collaborate concurrently;
- **Compliance support** with audit logs, custom data retention policies, and documentation-ready workflows; and
- **Automation and AI**, which gives teams the ability to resolve incidents faster, reduce manual tasks, trigger playbooks, automate workflows, and more.

With Mattermost, first responders, law enforcement, and public services organizations stay connected, compliant, and in control — no matter what the circumstances are.

Crossover Health Accelerates Support Ticket Resolution Time 99% with Mattermost

> "Mattermost helps us ensure that we're staying HIPAA-compliant while letting our clinicians collaborate efficiently and seamlessly."
>
> **— Daniel Gover,**
> IT system administrator,
> Crossover HealthMember

Crossover Health is a digital-first national medical group that deployed Mattermost to keep its distributed team together and ensure patients receive excellent healthcare services. Using Mattermost, the group was able to accelerate support ticket resolution time by 99% while recovering as much as 15% of logistical coordination time.

As a healthcare provider, Crossover Health needs to maintain HIPAA compliance at all times — understandably a top concern for the company. Thanks to Mattermost's built-in security and compliance features, clinicians can collaborate seamlessly while keeping sensitive patient data secure. Learn more about Crossover's journey with Mattermost.

crossover

The Mattermost Advantage for Public Services & Emergency Response

Pramacom Uses Mattermost to Ensure Communications for First Responders, Police, Firefighters & Military Units Are Always Available

> If you value your data and privacy and aim for high reliability and general ease of use, then self-hosted Mattermost is by far the best option out there.
>
> **— Jan Šídlo,**
> head of IT, Pramacom

pramacom

Pramacom is a communications company based in the Czech Republic that manages a digital radio network for emergency services, law enforcement, and military personnel. Due to the high-stakes nature of the network they operate, Pramacom can't afford any downtime.

To coordinate field operations, Pramacom was looking for a secure collaboration solution that they could host on their own servers to ensure data sovereignty and maintain GDPR compliance. After considering a few solutions, the team ultimately chose Mattermost in 2018. As a result, they've sped up incident response, streamlined collaboration, and improved security — all of which add up to increasing the reliability of their network. Learn more about how Pramacom uses Mattermost to keep Czech citizens safe.

Ready to Strengthen Your Mission-Critical Operations?

For public service agencies, law enforcement, and first responders, secure collaboration isn't a luxury. It's a requirement for protecting lives, maintaining public trust, and delivering rapid coordinated responses.

If you're ready to ensure your teams can stay connected during crises and operate with confidence and precision in any situation — all while meeting strict compliance requirements — schedule a demo of Mattermost today.

Schedule a Demo of Mattermost **Schedule a Demo**

Mattermost