EVERNORTH
HEALTH SERVICES

Military OneSource Incident Response Reporting Resource Guide

Last Updated: January 2026

This guide explains the importance of promptly identifying and reporting security incidents, especially those involving Personally Identifiable Information (PII). It outlines what qualifies as a security incident, the requirement to report immediately, and the steps for submitting reports through email or the 24/7 service desk.

Why Incident Response Matters

Incident Response (IR) plays a critical role in protecting our organization, our users, and the sensitive information entrusted to us. Security incidents, particularly those involving Personally Identifiable Information (PII) can have serious operational, legal, and reputational impacts if not identified and reported promptly.

Every provider is a key part of our cybersecurity defense. Early detection and immediate reporting of suspected or confirmed incidents allow the Incident Response Team (IRT) to quickly assess, contain, and mitigate potential harm.

What is a Security Incident?

A security incident includes, but is not limited to:

- Suspected or confirmed exposure, loss, or unauthorized access to **PII**
- Phishing emails, suspicious links, or credential-harvesting attempts
- Malware, ransomware, or unusual system behavior
- Accidental misdelivery of sensitive information
- Lost or stolen devices that may contain company or customer data
- Any activity that appears inconsistent with normal system operations

If you are unsure whether an event qualifies as an incident — **report it anyway**.

EVERNORTH
HEALTH SERVICES

Immediate Reporting Requirements

All security incidents **must be reported immediately** upon discovery.

- **Do not wait** for confirmation or for an investigation to be completed
- **Do not attempt to remediate** the issue on your own before reporting
- **Do not delay,** especially for incidents involving PII

Delayed reporting can result in regulatory non-compliance and increased risk.

How to Report an Incident

Primary Reporting Method (All Incidents) during normal business hours
Email: MOS-EAP-IRT@military-onesource.com
Report incidents **immediately** once identified, even if details are still emerging.
Include, if known:

- Date and time of discovery
- Description of what occurred
- Systems, data, or individuals potentially impacted
- Any actions already taken

Incomplete information should **not** delay reporting. Please **encrypt all communications** containing **PII.**

After-Hours / Emergency Support (24/7)
Phone: Military OneSource Service Desk: 1-877-819-0739
Contact the Military OneSource Service Desk immediately for:

- Incidents occurring outside normal business hours
- Urgent or high-impact security events
- Suspected or confirmed PII exposure

Your Responsibility as a Provider

All providers are expected to:

- Remain vigilant and **immediately report** any suspected or confirmed security incidents
- Consistently follow established incident reporting procedures

Prompt reporting helps protect our mission, our systems, and the individuals whose data we are entrusted to safeguard. When in doubt – Report It. If you see something unusual, suspect a security issue, or believe sensitive data may be at risk, **report it immediately**. There is no penalty for reporting in good faith. Early reporting saves time, reduces impact, and ensures compliance