TECHMED SOLUTIONS

INCIDENT COMMUNICATION PLAN

DECEMBER 12, 2025

Table of Contents

Introduction

TechMed Solutions' Incident Response Communications plan aims to provide an overarching strategy and guiding principles to the organization when it comes to communicating with the public and internal and external stakeholders during a security incident. It is also designed as a working manual for the communications team with templates and tools to be used during an incident, for a consistent and agreed approach, and to ensure TechMed Solutions responds to incidents early, proportionately, and in terms that are accessible to the public.

Stakeholder Identification

Internal Stakeholder:

- Executives: this group includes the CEO, CIO, and CISO. This group needs to be communicated to on the financial risk, operational status, timeline, business impact of a security incident, and regulatory compliance status.
- Employees: to all staff, there must be clear and concise instructions on security actions like password resets, phishing awareness. The IT department ensures other departments stay abreast of the security posture of the organization and conducts security awareness training with approval from the CISO. The legal department must ensure the organization complies with all regulatory requirements. The HR department must ensure strict adherence to training materials.

External Stakeholder:

- Customers: they must be communicated to in case of a security incident in TechMed Solutions, with transparency on affected data, steps taken to contain the incident, and the current phase of recovery backed up with legal counsel. Customers must be abreast of any security incident with measures to take, either as changing account passwords, ignoring any email, not clicking any link, especially if sent through email.
- Regulators: this group includes HHS/OCR and PCI/SSC; they must be notified in case of a security incident in TechMed Solutions, with strict adherence to the breach notification mandate.
- Media / Public: as appropriate, the media and the general public should be notified in case of a security breach in TechMed Solutions; they must be notified with facts about the breach, how it’s been contained, and the necessary report that has been sent to regulatory bodies and affected individuals. An official press release should be circulated to the media and general public on the state of the security incident.
- Vendors / Partners: their services could be the attack vector/target through which the security incident emanated from; they must be notified.

Communication Templates

For effective communication, messages must be tailored to the audience's needs and legal obligations.

Internal Incident Notification

To: CSIRT Members, CISO

Subject: URGENT – Incident Response Activation: [Incident Number -001]

Body:

The Computer Security Incident Response Team (CSIRT) has been activated in response to a suspected security incident.

The Organization, TechMed Solutions, recently experienced a minor security breach with incident number 001. It occurred in the early hours of Wednesday, 26th November, 2025. According to the report, the severity level of the incident is medium, the incident type is unauthorized access, affected system is the development environment.

Immediate Actions Required:

- All CSIRT members should check in via the secure communication channel
- Review your assigned role and responsibilities
- Ensure you have access to all necessary tools and systems.
- Stand by for the initial incident briefing at [Time]

Secure Communication Channel: Slack / Microsoft Teams

Executive Briefing

To: CEO, COO, CFO, General Counsel

Subject: Incident Status Update – [Incident Number] – [Date/Time]

Body:

Executive Summary:

We are responding to an unauthorized access incident that was detected at the early hours on Wednesday, 26th November 2025. The incident is currently classified as Medium. Below is a summary of the current situation and our response.

Current Status:

- Systems Affected: Hybrid cloud environment (AWS primary, on-premises data center for legacy system.

- Data at Risk: protected Health Information (PHI), Payment Card Data (PCI), and Proprietary Medical Algorithm
- Business Impact: The incident exposes the organization's inability to detect, respond to, and recover from a security incident
- Estimated Recovery Time: [Provide estimate if available]
- Actions Taken: The Board of Directors mandated the establishment of a formal incident response program.
- Next Steps: the external forensics team has been contacted to detect the scope of the incident.
- Resource Requirements:
- Decision Required:

Customer Notification

To: Affected Customers

Subject: Important Security Notice – TechMed Solutions

Body:

Dear Valued Customer,

We are writing to inform you of a security incident that may have affected your personal information stored in our systems.

What Happened: On Wednesday, 26th November 2025, we discovered a minor security incident involving unauthorized access in the development environment. We immediately launched an investigation and engaged external security experts to determine the scope of the incident.

What Information Was Affected: Our investigation has determined that no customer data was exposed.

What We are Doing: We have contained the incident and taken steps to prevent further unauthorized access. We are conducting a thorough forensic investigation. We are notifying all affected individuals, we are working with law enforcement and regulatory authorities, and we are implementing additional security measures to prevent similar incidents in the future.

What You Should Do:

- Monitor your accounts for any unauthorized activity
- Consider placing a fraud alert or credit freeze with the credit bureau
- Review your account statements regularly
- Contact us if you notice any suspicious activity

Additional Resources: [link to FAQ page]

We sincerely apologize for this incident and any inconvenience it may cause. Your trust is important to us, and we are committed to protecting your information.

Sincerely,

TechMed Solutions Security Team.

Regulatory Notification

To: HIPAA

Subject: Breach Notification

Organization Name: TechMed Solutions

Date: 05-12-2025

Body:

Notification of Breach of Unsecured Protected Health Information

Pursuant to 45 CFR § 164.404, TechMed Solutions is notifying you of a breach of unsecured protected health information (PHI). The suspected breach was caused by unauthorized access to a development environment. It occurred in the early hours of Wednesday, 26th November, 2025, while the breach was discovered on Thursday, 20th November, 2025. No PHI was compromised.

Description of Breach:

Breach Notification: individual notifications were sent on 01-12-2025. Copies of individual notification letters are attached

Mitigation Measure: The affected system was isolated to prevent further escalation.

Contact Information: for questions regarding this notification, please contact: [Name, Title, Phone, Email]

Sincerely,

TechMed Solutions

Public Statement

For Immediate Release

TechMed Solutions Responds to Security Incident

Los Angeles, California – 05-12-2025 – TechMed Solutions announced today that it has discovered and is actively responding to a security incident affecting its systems.

What We Know: On 26-11-2025, we discovered evidence of unauthorized access to our systems. We immediately launched an investigation with the assistance of external security experts and have notified law enforcement.

Our Response: We have contained the incident and taken steps to prevent further unauthorized access. We are conducting a thorough investigation to determine the full scope of the incident. We are notifying all affected individuals and regulatory authorities as required by law. We are implementing additional security measures to strengthen our defenses.

Commitment to Our Customers: The security and privacy of our customers' information is our highest priority. We are committed to transparency and will provide updates as our investigation progresses.

Resources Available: customers with questions can visit [website] or call [phone number].

About TechMed Solutions: TechMed Solutions is a Healthcare Organization with 850 employees across 3 locations. The organization has over 200 customers across North America.

Media Contact: Chief Communication Officer

Law Enforcement Notification

To: [FBI Field Office / Local Law Enforcement]

Subject: Cyber Incident Notification

Organization Name: TechMed Solutions

Body:

We are notifying you of a cybersecurity incident that has affected TechMed Solutions.

Incident Summary: The incident was discovered on 26-11-2025. The incident type is a Data Breach, the system affected is the development environment, and no data was compromised.

Incident Details:

Forensic Investigation: We have engaged external forensic experts to conduct a thorough investigation. Preliminary findings are attached.

Requested Assistance: We request that law enforcement identify the threat actor.

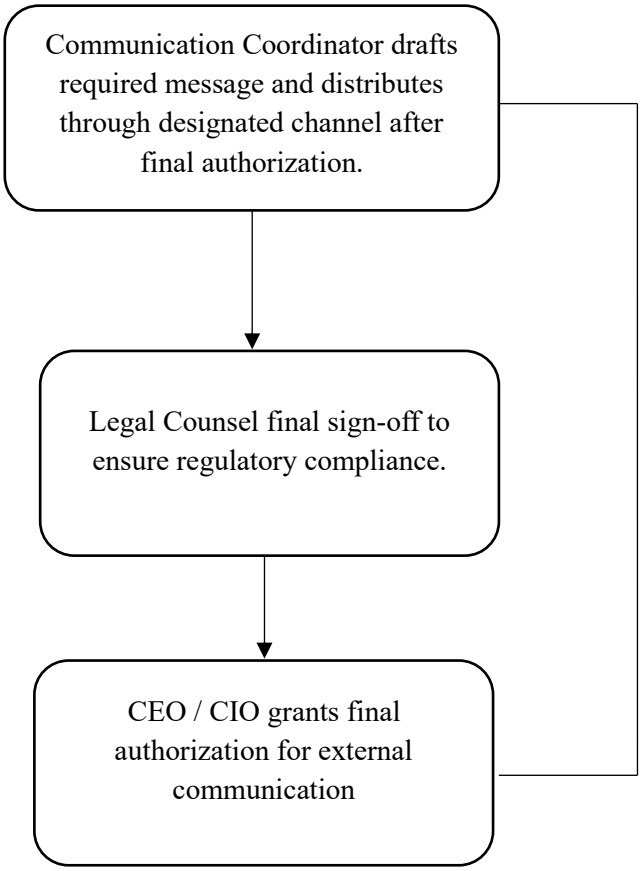
Contact Information: Incident Response Manager: [Name, Phone, Email] Legal Counsel [name, Phone, Email]

We are available to provide additional information as needed.

Communication Protocols

For secure communication across the team members, dedicated channels like Slack, Microsoft Teams should be used; use of emails, SMS should be avoided. For critical or high incidents, the executive leadership must be briefed every 4 hours at the initial stage of the discovery, after which they can be briefed on the progress twice daily, to ensure they are kept abreast. The customer and general public can be provided with updates 24 hours after containment of the security incident, with further updates on regulatory actions. The designated spokesperson will be the communication coordinator / Chief Communication Officer, liaising with the media and general public regarding the security incident.

Approval workflows for external communications flowchart:



Regulatory Notification Requirements

- According to the HIPAA Breach Notification rule, TechMed Solutions, as a Covered Entity, must notify affected individuals no later than 60 calendar days after the discovery of the security incident.
- According to PCI DSS law, TechMed Solutions must notify payment brands, acquiring banks within 24 hours of the discovery of a security incident compromising the Cardholder Data Environment (CDE).
- State breach Notification Laws, TechMed Solutions Legal Counsel should carry out reviews of the jurisdiction of affected individuals for adherence to their breach notification laws.