Quarterly Compliance Report

Security Awareness Training Documentation

January 1, 2026 - January 3, 2026

Organization:	UMC
Address:	, Lubbock, TX 79407
Report Generated:	January 3, 2026 at 11:58 PM
Generated By:	root
Report Period:	January 1, 2026 through January 3, 2026

Executive Summary

This compliance report documents UMC's security awareness training program for the period from January 1, 2026 to January 3, 2026. The organization conducted 1 phishing simulation campaign involving 1 employee.

CAMPAIGNS CONDUCTED

1

Simulation exercises

EMPLOYEES TRAINED

1

Unique participants

OVERALL CLICK RATE

100.0%

Vulnerability rate

REMEDIATION RATE

100.0%

Training completed

Campaign Details

Campaign Name	Date	Targets	Sent	Clicked	Click Rate
UMC Q1 Phishing Simulation	Jan 03, 2026	1	1	1	100.0%

Remediation Training

Employees who clicked on simulated phishing links were automatically assigned remediation training. This section documents the corrective action taken to address identified vulnerabilities.

Metric	Count	Percentage
Employees Who Clicked Links	1	100.0%
Remediation Training Assigned	1	100.0%
Remediation Training Completed	1	100.0%
Remediation Pending	0	0.0%

Compliance Attestations

HIPAA Security Rule § 164.308(a)(5) - Security Awareness and Training

UMC has implemented a security awareness and training program for all workforce members as required by 45 CFR § 164.308(a)(5).

- ☑ Training program established and documented
- ☑ All workforce members received training during this period
- ☑ Training includes protection from malicious software (phishing)
- ☑ Ongoing training provided (not one-time)
- ☑ Remediation provided for employees who demonstrated vulnerabilities

Training Frequency: Quarterly
Completion Rate: 100.0%

HITECH Act - Reasonable Safeguards

UMC has implemented reasonable safeguards to protect electronic protected health information (ePHI) through ongoing security awareness training and phishing simulation exercises as required by the HITECH Act.

- ☑ Reasonable safeguards implemented to protect ePHI
- ☑ Training program demonstrates proactive risk mitigation
- ☑ Security culture evidenced by declining click rates

This training program demonstrates our commitment to preventing unauthorized access to ePHI and reducing the risk of data breaches subject to HITECH breach notification requirements.

HITRUST CSF Control 02.g - Security Awareness Training

UMC has implemented security awareness training that meets HITRUST CSF Control 02.g requirements:

- ☑ All personnel have received appropriate security awareness training relevant to their job function
- ☑ Training is updated regularly to address new and emerging threats
- ☑ Training effectiveness is measured and monitored through quantitative metrics
- ☑ Remediation is provided to personnel who demonstrate vulnerabilities

Current Period Click Rate: 100.0%
Training Completion Rate: 100.0%

NIST Cybersecurity Framework PR.AT-1 - Awareness and Training

UMC's security awareness training program aligns with NIST Cybersecurity Framework Category PR.AT-1:

- ☑ **Identify:** Risk assessment through 1 simulated phishing exercise
- ☑ **Protect:** Training provided to 1 employee
- ☑ **Detect:** Click rate monitoring identifies vulnerable employees
- ☑ **Respond:** Remediation workflows for 1 vulnerable employee
- ☑ **Recover:** 1 employee completed remediation training

This alignment supports our cyber insurance requirements and demonstrates reasonable security controls to regulatory authorities.

State Breach Notification Laws - Reasonable Security Measures

UMC has implemented reasonable security measures as required by applicable state breach notification laws:

- ☑ **California CMIA (Civil Code §56.101):** Reasonable security procedures and practices implemented through ongoing employee training
- ☑ **New York SHIELD Act (GBL §899-bb):** Security awareness training provided as part of comprehensive data security program
- ☑ **Texas HB 300 (Health & Safety Code §181.101):** Employee training program established to protect electronic health information
- ☑ **Massachusetts 201 CMR 17.00:** Security awareness training included in written information security program (WISP)

These proactive security measures demonstrate our commitment to protecting personal information and reducing breach notification obligations under state law.

requirements. Organizations are responsible for their own compliance programs. Consult with legal and compliance professionals regarding your specific regulatory obligations.

This report documents training activities conducted during the specified period but does not constitute legal advice or certification of compliance. Regulatory compliance requires a comprehensive program that extends beyond security awareness training alone.

I certify that the information contained in this report is accurate and complete to the best of my knowledge.

_____

Authorized Signature

_____

Printed Name and Title

_____

Date