Coordinated Vulnerability Disclosure Policy

1 Purpose

This policy establishes a publicly accessible process for receiving, assessing, and addressing cybersecurity vulnerability reports in DentalMonitoring products and related systems. It defines how Dental Monitoring coordinates with external security researchers, third-party software suppliers, users, and other stakeholders to responsibly disclose and remediate vulnerabilities.

2. Scope

1.1 In-scope

This policy applies to all software components of the DentalMonitoring system, including mobile applications, web interfaces, backend services, cloud infrastructure, and APIs.

In-scope assets are grouped into the following two categories:

A. Medical Software & Clinical Platforms

Public-facing websites and applications operated under the dental-monitoring.com namespace and associated medical/clinical services.

B. Corporate / Subsidiaries / IT Infrastructure

Public-facing websites and applications operated under the dentalmonitoring.com namespace, corporate IT services, and any subsidiary-operated domains owned by the DentalMonitoring group.

For security reasons, the exhaustive list of in-scope hostnames is intentionally not published in this policy in order to reduce reconnaissance value for malicious actors. Researchers acting in good faith who are unsure whether a specific asset, subdomain, or product is in scope must request confirmation at `security@dental-monitoring.com` before any active testing.

1.2 Out of Scope

The following are excluded from this policy:

- Vulnerabilities in third-party platforms or services not controlled by Dental Monitoring (e.g., iOS, Android, web browsers, app stores)
- Physical security of user devices or facilities

- Social engineering or phishing attacks
- Denial-of-service or brute-force attacks
- Spam, User-controlled content rendering, DNS or email-related issues without demonstrated security impact

2 Reporting a Vulnerability

2.1 Reporting Channel

Security researchers, users, healthcare professionals, third-party suppliers, and any other stakeholder who discovers a potential security vulnerability in DentalMonitoring are encouraged to report it through the following channel:

Email: security@dental-monitoring.com

Security.txt: https://www.dentalmonitoring.com/.well-known/security.txt

Preferred languages: English, French

Reports may also be submitted by contacting Dental Monitoring customer support, who will escalate security-related reports to the security team.

2.2 Information to Include

To facilitate efficient triage, reporters are encouraged to include:

- Description of the vulnerability and affected components
- Steps to reproduce, including tools or configurations used
- Potential impact assessment (confidentiality, integrity, availability)
- Proof-of-concept code or screenshots (if available)
- Reporter's contact information for follow-up

2.3 Safe Harbor

Dental Monitoring will not pursue legal action against researchers who report vulnerabilities in good faith and comply with this policy.
Researchers are expected to:

- Not access, modify, or delete patient data or ePHI
- Not perform testing that degrades the service for other users
- Not disclose the vulnerability publicly before the coordinated timeline is agreed upon

- Not run automated scanners or tools that generate significant traffic against DentalMonitoring infrastructure
- Not attempt social engineering, phishing, or physical attacks against Dental Monitoring employees or facilities
- Not perform denial-of-service testing
- Comply with all applicable laws

3 Vulnerability Handling Process

3.1 Receipt and Assessment

Upon receipt, the security team acknowledges the report within 5 business days and assigns a tracking identifier. If the reported vulnerability is already known or is a duplicate of an existing report, the reporter is informed, and the report is closed.

An initial assessment is performed within 10 business days, including validation, severity scoring (CVSS v3.1), exploitability assessment (including a CISA KEV Catalog cross-reference), patient safety impact evaluation, and SBOM-based identification of affected components.

3.2 Severity Classification and Response Timelines

Severity	CVSS Score	Response Target	Remediation Target
Critical	9.0 - 10.0	Upon receipt	Hotfix process
High	7.0 - 8.9	Within 48 hours	Within 30 days
Medium	4.0 - 6.9	Within 5 business days	Within 60 days or the next release
Low	0.1 - 3.9	Within 10 business days	The security team sets the target

3.3
4.3. Remediation

Fixes are developed and validated following PRD0300 (Software Design & Development), POL1530 (Software Security Framework), and verified through PRD0302/PRD0303 (Verification/Validation Strategies).

Remediation includes software patches, configuration changes, compensating controls, or component replacement.

3.4 Communication to Reporter

- **Acknowledgment of report:** within 5 business days
- **Initial assessment result:** within 30 days
- **Status updates:** at a minimum every 30 days until resolution
- **Notification of fix availability:** before or at coordinated disclosure

4 Coordinated Disclosure

4.1 External Reports

When Dental Monitoring validates a vulnerability reported by an external reporter, a coordinated disclosure process is initiated if Dental Monitoring deems it necessary to disclose it to the public.

In which case, Dental Monitoring works with the reporter to agree on a coordinated disclosure timeline, typically 90 days from the date the vulnerability is confirmed.

Expedited disclosure may apply if the vulnerability is actively exploited, and reporters are credited (with consent) in communications to affected parties.

4.2 Internally Identified Vulnerabilities

Vulnerabilities identified through internal monitoring (PRD1525 - Threat Intelligence, vulnerability scanning, penetration testing, SBOM monitoring) follow the same assessment and remediation process. For shared open-source components, coordination with component maintainers and CISA is performed where appropriate.

5 Stakeholder Notification

5.1 Customer and User Notification

When a confirmed vulnerability requires user action or awareness, Dental Monitoring communicates through direct notification to affected healthcare professionals and practice administrators via the Dashboard or email/sms, or in-app notification to affected DM App users when appropriate.

Notifications include a description of the vulnerability, affected product version, recommended actions or compensating controls, patch availability, and contact information for further assistance.

5.2 Regulatory Notification

Dental Monitoring reports vulnerabilities directly affecting the system safety or effectiveness after the assessment to the FDA and CISA in accordance with 21 CFR Part 806 and CISA coordinated disclosure guidelines, and to national cybersecurity authorities as required by applicable law (e.g., ANSSI in France).

6 Integration with Quality Management System

The CVD process is integrated with Dental Monitoring's ISMS (ISO/IEC 27001:2022) and Quality Management System (ISO 13485:2016):

- **CAPA:** confirmed vulnerabilities revealing systemic issues trigger the CAPA process (PRD0008)
- **Security events:** reports are tracked per PRD1512, in registers REC1511 and REC1512
- **Risk management:** new threats are incorporated into the cybersecurity risk assessment (REC1549)
- **SBOM:** component vulnerabilities trigger SBOM review and update (REC1546 Section 6.5)
- **Postmarket surveillance:** vulnerability data feeds into PMS activities (REC1227)

7 Public Accessibility

This policy is maintained and publicly accessible at:

- Web: https://dentalmonitoring.com/wp-content/uploads/2026/04/POL1537-Coordinated-Vulnerability-Disclosure-Policy.pdf

8 Policy Review

This policy is reviewed at minimum annually as part of the Postmarket Cybersecurity Management Plan review, when significant changes occur in the regulatory landscape, threat environment, or product architecture, and following any incident that reveals a gap in the CVD process.