

DRAFT · NOT IN EFFECT UNTIL APPROVED

Incident Response Plan

Sample Dental Group · Plan

Document control	
Document owner	Practice Administrator
Approved by	Managing Partner Signature: _____ Date: _____
Version	0.1 (starter draft, October 16, 2026)
Review cycle	At least annually, and after a significant incident or change
Classification	Internal

Purpose

This plan describes how Sample Dental Group prepares for, responds to and recovers from cybersecurity incidents.

Scope

This document applies to all Sample Dental Group staff, contractors and service providers, including the outsourced IT provider, and to every system that stores, processes or carries patient or practice information.

Definitions and roles

1. An incident is any event that harms, or threatens, the confidentiality, integrity or availability of Sample Dental Group's systems or information.
2. The incident lead is the [Security Lead]; the backup is [name]. The incident lead may call on [IT, OT, legal counsel, insurer, outside responders].
3. Contact details for the response team, legal counsel, the cyber insurer and outside responders are kept in Appendix [X] and in a place that is reachable if systems are down.

Response steps

4. Report: anyone who suspects an incident reports it immediately to [contact].
5. Triage: the incident lead confirms whether it is an incident and rates its severity.
6. Contain: affected systems are isolated to stop the incident spreading. Evidence is preserved before systems are wiped or rebuilt.
7. Notify: legal counsel and the cyber insurer are contacted early. Decisions about notifying regulators, customers or law enforcement are made with counsel.
8. Eradicate and recover: the cause is removed, and systems are restored and verified under the recovery plan.
9. Record: actions, decisions and times are logged throughout.

After the incident

10. A review is held within [two weeks] to identify the root cause and improvements.
11. This plan is tested at least annually with a tabletop exercise and updated afterward.

Exceptions

Exceptions to this document must be requested in writing, approved by the Practice Administrator, and recorded in the exception log with a compensating control and an expiry date.

Review

The document owner reviews this document at least annually, and after a significant incident or change. Changes are approved by the Managing Partner and recorded below.

Revision history

Version	Date	Change	Approved by
0.1	October 16, 2026	Starter draft generated from the NIST CSF 2.0 assessment	

Framework mapping

Once adopted and followed, this document supports the following NIST CSF 2.0 requirements.

Subcategory	Requirement
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared
RS.MA-02	Incident reports are triaged and validated
RS.MA-03	Incidents are categorized and prioritized
RS.MA-04	Incidents are escalated or elevated as needed
RS.MA-05	The criteria for initiating incident recovery are applied
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved
RS.AN-08	An incident's magnitude is estimated and validated
RS.MI-01	Incidents are contained
RS.MI-02	Incidents are eradicated
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved

Text in [brackets] must be replaced with Sample Dental Group's own details before this document is used. This is a starting point prepared from the assessment results; it does not describe current practice until it has been tailored, approved and put into effect.