MPS — eAssist Data Security Incident Response Checklist

For Dental Practices Using eAssist Dental Solutions

Purpose:
This checklist is designed to assist dental practices in documenting and responding to reports of a potential cybersecurity incident involving eAssist. It is intended to support the practice's HIPAA Security Rule, Breach Notification Rule, incident-response, risk-analysis, and business-associate oversight obligations.

Important: A reported or alleged cybersecurity incident does not automatically mean that a HIPAA breach has occurred. Do not notify patients that their PHI was breached until the facts have been sufficiently established.

I. INITIAL INCIDENT DOCUMENTATION

Date practice became aware of potential incident: _____

How practice became aware:

☐ eAssist notification
☐ Email
☐ Telephone call
☐ News report
☐ Cybersecurity/ransomware report
☐ Employee notification
☐ IT/security provider
☐ Other: _____

Date incident reportedly occurred, if known: _____

Date eAssist reportedly discovered incident: _____

Practice contact who received information: _____

Document the initial report

☐ Save the original eAssist communication.

☐ Save relevant emails and correspondence.

☐ Save screenshots or copies of public reports.

☐ Do not alter or delete potentially relevant evidence.

☐ Open an internal HIPAA/security incident file.

☐ Assign an individual responsible for coordinating the investigation.

Incident/Case Number: _____

II. CONTACT eASSIST IN WRITING

The practice should request written information from eAssist regarding the incident.

Request confirmation of:

☐ Whether a cybersecurity incident occurred

☐ Whether unauthorized access occurred

☐ Whether ransomware was involved

☐ Whether information was exfiltrated

☐ Whether ePHI was involved

☐ Whether the practice's information was involved

☐ Whether the practice's patients were affected

☐ Date unauthorized access began

☐ Date unauthorized access ended

☐ Date eAssist discovered the incident

☐ Date eAssist contained the incident

☐ Systems affected

☐ Databases affected

☐ Categories of information potentially involved

☐ Number of individuals potentially affected

☐ Whether law enforcement was notified

☐ Whether forensic investigators were retained

☐ Whether cyber-insurance carriers were notified

☐ Whether HHS/OCR was notified

☐ Whether state regulators were notified

☐ Whether eAssist has determined that a HIPAA breach occurred

☐ Whether eAssist will provide a formal breach report

☐ Whether eAssist is providing credit/identity monitoring, if applicable

☐ What remediation has been completed

☐ What additional security controls have been implemented

III. REVIEW THE BUSINESS ASSOCIATE AGREEMENT

Obtain the current **eAssist Business Associate Agreement (BAA).**

BAA date: _____

Review the BAA for:

☐ Security requirements

☐ Breach notification requirements

☐ Security incident notification requirements

☐ Time period for notification

☐ Required information in a breach notification

☐ Cooperation with investigation

☐ Access to information necessary for the practice's risk assessment

☐ Subcontractor requirements

☐ Data return/destruction requirements

☐ Termination provisions

☐ Indemnification provisions

☐ Cybersecurity requirements

☐ Insurance requirements

☐ Other contractual requirements: _____

MPS Recommendation:
Keep a copy of the BAA and all eAssist communications in the practice's compliance documentation.

IV. DETERMINE WHAT INFORMATION eASSIST HAS

Identify the categories of information transmitted to or accessible by eAssist.

Patient Information

☐ Patient names

☐ Addresses

☐ Telephone numbers

☐ Dates of birth

☐ Insurance information

☐ Insurance identification numbers

☐ Social Security numbers

☐ Financial information

☐ Payment information

☐ Account balances

☐ Treatment information

☐ Dental procedure information

☐ Diagnosis information

☐ Claims information

☐ Other PHI: _____

Determine whether information was:

☐ Encrypted at rest

☐ Encrypted in transmission

☐ De-identified

☐ Accessible through eAssist systems

☐ Stored by eAssist

☐ Accessible by eAssist employees

☐ Accessible by eAssist subcontractors

Additional information:

V. DETERMINE WHAT ACCESS eASSIST HAS TO THE PRACTICE

Work with the practice's IT/security provider.

Systems potentially connected to or accessible by eAssist:

☐ Practice management system

☐ EHR

☐ Imaging system

☐ Patient portal

☐ Email

☐ File storage

☐ Remote desktop

☐ VPN

☐ Cloud applications

☐ Payment systems

☐ Banking information

☐ Insurance portals

☐ Other: _____

Access review

☐ Identify all eAssist accounts.

☐ Identify all eAssist user accounts.

☐ Verify current employees with access.

☐ Verify former employees no longer have access.

☐ Verify appropriate privileges.

☐ Verify MFA is enabled where available.

☐ Disable unnecessary accounts.

☐ Reset credentials where appropriate.

☐ Review privileged accounts.

☐ Review third-party/vendor connections.

VI. REVIEW SECURITY LOGS

Request assistance from the practice's IT/security provider.

Review, where available:

☐ Authentication logs

☐ Failed login attempts

☐ Successful login attempts

☐ Remote access logs

☐ VPN logs

☐ Administrative activity

☐ User activity

☐ File access

☐ Data downloads

☐ Data exports

☐ Bulk record access

☐ Unusual login locations

☐ Unusual after-hours activity

☐ Changes to user permissions

☐ Changes to banking/payment information

☐ Malware/endpoint alerts

☐ Firewall alerts

☐ Other security alerts

IT/security provider: _____

Date reviewed: _____

Findings:

_____

_____

_____

Do not destroy or overwrite relevant logs while an investigation is ongoing.

_____

VII. CONDUCT A HIPAA RISK ASSESSMENT

The practice should evaluate whether the incident creates a risk to the confidentiality, integrity, or availability of ePHI.

Questions to consider:

1. What PHI was involved?

_____

2. Whose PHI was involved?

_____

3. Was the information actually accessed or acquired?

☐ Yes
☐ No
☐ Unknown

4. Was the PHI encrypted?

☐ Yes
☐ No
☐ Unknown

5. Was the information actually exfiltrated?

☐ Yes
☐ No
☐ Unknown

6. Who potentially received/accessed the information?

---

7. Was the information actually viewed or used?

☐ Yes
☐ No
☐ Unknown

8. What mitigation has occurred?

---

9. Is there a low probability that the PHI has been compromised?

☐ Yes
☐ No
☐ Undetermined

Risk assessment conclusion:

☐ No breach determined

☐ Breach determined

☐ Additional investigation required

☐ Awaiting information from eAssist

Completed by: _____

Date: _____

VIII. MITIGATION

Document steps taken to reduce the risk.

☐ Contacted eAssist

☐ Contacted IT/security provider

☐ Reviewed system access

☐ Disabled unnecessary access

☐ Changed passwords for your practice management program and work email emails for all users

☐ Implemented/verified MFA for all remote log ins

☐ Notify your bank to monitor any suspicious activity

☐ Reviewed audit logs

☐ Preserved evidence

☐ Reviewed backups

☐ Verified backup integrity

☐ Reviewed cyber-insurance coverage

☐ Reviewed incident-response plan

☐ Updated Security Risk Analysis

☐ Reviewed BAA

☐ Evaluated alternative vendors

☐ Other: _____

IX. PATIENT NOTIFICATION — DO NOT COMPLETE UNTIL BREACH IS DETERMINED

Has the practice determined that a reportable HIPAA breach occurred?

☐ No
☐ Yes
☐ Pending investigation

If yes, document:

Date of breach determination: _____

Number of individuals affected: _____

Types of PHI involved:

Notification evaluation

☐ Individual notification required

☐ HHS/OCR notification required

☐ Media notification potentially required

☐ State notification requirements evaluated

☐ Legal counsel consulted

☐ Cyber-insurance carrier notified

☐ Notification vendor engaged, if applicable

Date notification process initiated: _____

X. VENDOR MANAGEMENT FOLLOW-UP

After the immediate incident has been addressed, the practice should reassess eAssist as a business associate.

Request updated information regarding:

☐ Incident investigation

☐ Independent forensic assessment

☐ Corrective actions

☐ Security enhancements

☐ MFA

☐ Encryption

☐ Employee security training

☐ Vulnerability management

☐ Penetration testing

☐ Backup/recovery controls

☐ Incident-response procedures

☐ Business continuity

☐ Subcontractor security

☐ Updated SOC report, if available

☐ Updated security documentation

☐ Updated BAA, if applicable

XI. SECURITY RISK ANALYSIS UPDATE

Does the incident require an update to the practice's HIPAA Security Risk Analysis?

☐ Yes

☐ No — rationale documented below

Risk identified:

Existing safeguard:

Additional safeguard needed:

Person responsible: _____

Target completion date: _____

Date completed: _____

XII. FINAL INCIDENT CLOSURE

Before closing the incident:

☐ Investigation completed

☐ eAssist response received

☐ IT/security investigation completed

☐ PHI involvement determined

☐ Breach determination completed

☐ Required notifications completed, if applicable

☐ Mitigation completed

☐ Risk Analysis updated

☐ Corrective actions completed

☐ BAA reviewed

☐ Vendor risk assessment updated

☐ Documentation retained

☐ Lessons learned documented

Final determination

☐ No HIPAA breach

☐ HIPAA breach — notifications completed

☐ HIPAA breach — notifications pending

☐ Incident remains under investigation

Final summary:

Completed by: _____

Title: _____

Date: _____

Reviewed by MPS: _____

Date: _____