

Incident Response Plan Template for Small Healthcare Practices

A Fillable Plan Sized for a Small Healthcare Practice

SIM Technology Solutions • Healthcare IT & Compliance Guide • Updated September 2026

SECURITY & RISK

Most incident response advice is written for hospital systems with a dedicated security team. This template is sized for a practice with a handful of providers and no in-house security staff. Fill it in once, print or save a copy somewhere every staff member can find during an actual incident, and revisit it at least once a year.

Practice Name:	
Plan Completed By:	
Date Last Reviewed:	
Next Review Due:	

1. Key Contacts

Role	Name / Company	Phone	Email
IT Provider / MSP			
Incident Commander (internal)			
Legal Counsel			
Cyber Insurance Carrier / Broker			
EHR / Practice Mgmt. Vendor			
Local Law Enforcement (non-emergency)			

2. Roles & Responsibilities

Who declares an incident:	
Who isolates affected systems:	
Who contacts the IT provider:	
Who contacts legal counsel and the insurance carrier:	
Who communicates with staff:	
Who communicates with patients, if needed:	

3. What Counts as a Suspected Incident

- Files renamed, encrypted, or inaccessible, or a ransom note appears
- Unexpected password reset emails or MFA prompts nobody triggered
- Unusual login times or locations flagged in email or your EHR admin console
- Staff report a phishing click or a suspicious attachment they opened
- Any unexplained data loss, missing records, or system outage

4. Response Checklist

- ☐ Isolate affected devices from the network. Do not power them off.
- ☐ Notify the IT Provider / MSP listed above immediately.
- ☐ Don't negotiate with attackers, pay a ransom, or delete anything without IT and legal involved.
- ☐ Preserve evidence. Don't reformat, reinstall, or "clean up" any system yet.
- ☐ Start a written incident timeline: what was noticed, by whom, and when.
- ☐ Determine whether PHI was involved or likely accessed.
- ☐ Contact legal counsel and the cyber insurance carrier.
- ☐ Confirm backups are intact and were not themselves affected.

5. Notification Timeline (HIPAA + Virginia)

Who	Timeline
Affected individuals	Without unreasonable delay, no later than 60 days after discovery

Who	Timeline
HHS Office for Civil Rights (500+ affected)	Within 60 days, same timeframe as individual notice
HHS Office for Civil Rights (under 500 affected)	Logged and reported annually, within 60 days of year-end
Media	Required if more than 500 residents of one state/jurisdiction are affected

6. Post-Incident Review

Root cause identified:

Changes made as a result:

Security Risk Analysis
updated (date):

Staff retrained (date):

Don't wait for an incident to write this down.

SIM Technology Solutions helps practices build, test, and keep a plan like this current, and is who you call the moment something looks wrong. Call 703-594-9226 or email info@simtsolutions.com.