CHECKLIST · HIPAA

HIPAA Breach Response Checklist: First 72 Hours

Step-by-step breach response protocol to meet the HHS notification timeline under the 2026 rules.

2 pages · PDF · Updated May 2026 · **goironfort.com**

■ *Under the 2026 HIPAA NPRM, HHS notification must occur within 72 hours of breach discovery. Use this checklist immediately upon discovering a suspected incident.*

0–4 Hours: Immediate Containment

- ■ Activate incident response team — notify IR Lead, Privacy Officer, and Legal
- ■ Isolate affected systems to prevent further unauthorized access or data loss
- ■ Preserve system state and logs — do not power off systems before forensic imaging
- ■ Document time and method of discovery, reporter identity, and initial indicators
- ■ Begin incident timeline log — every action timestamped

4–24 Hours: Investigation & Assessment

- ■ Determine scope: which systems, which ePHI, which individuals potentially affected
- ■ Assess breach vs. non-breach using the HHS four-factor risk assessment
- ■ Identify whether a Business Associate is involved — notify them within 24 hours
- ■ Engage forensic analyst if external expertise needed
- ■ Notify cyber liability insurer if applicable
- ■ Draft internal situation report for executive leadership

24–48 Hours: Notification Preparation

- ■ Complete HHS four-factor risk assessment and document conclusion
- ■ If breach confirmed: draft HHS notification using OCR breach report form

- Begin drafting affected individual notification (if applicable)
- Brief legal counsel on proposed notification content before sending
- Identify appropriate notification delivery method for affected individuals
- Prepare media statement if >500 individuals affected (prominent media required)

48–72 Hours: Notifications Sent

- Submit HHS breach notification via OCR web portal (hhs.gov/hipaa/breaches)
- Send individual notifications — by first-class mail or email if agreed
- Notify state attorney general if required by state breach law
- Notify media outlets if >500 residents in a single state affected
- Document all notifications sent with timestamps and delivery confirmation
- Update incident timeline log — preserve as compliance documentation

Post-72 Hours: Remediation & Documentation

- Implement remediation for exploited vulnerabilities
- Conduct root cause analysis and document findings
- Update policies, procedures, or technical controls to prevent recurrence
- Complete full incident report for 6-year HIPAA documentation retention
- Schedule post-incident review with IR team within 2 weeks

> ■ *Iron Fort's breach response module tracks the 72-hour clock automatically and guides your team through each phase. Get started at goironfort.com/demo*