HIPAA Breach Notification Requirements

What to do if a data breach occurs: timelines, documentation, and steps to minimize liability

What Constitutes a Breach?

A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

Not all incidents are breaches - conduct a risk assessment to determine if notification is required.

The 60-Day Rule

Covered entities must notify affected individuals within 60 days of discovering a breach.

Discovery occurs on the first day the breach is known or should have been known.

Notification Requirements

Individual Notification

- [ ] Written notice by first-class mail (or email if individual agreed)
- [ ] Include: description of breach, types of PHI involved, steps individuals should take
- [ ] Include: what entity is doing to investigate and mitigate
- [ ] Include: contact information for questions

Media Notification

Required if breach affects more than 500 residents of a state or jurisdiction

- [ ] Notify prominent media outlets
- [ ] Provide same information as individual notification

HHS Notification

Breaches affecting 500+ individuals: Notify HHS immediately

Breaches affecting <500 individuals: Notify HHS annually

Business Associate Notification

- [ ] Business associates must notify covered entity within 60 days
- [ ] Provide identification of affected individuals
- [ ] Provide details of the breach

Breach Response Checklist

- [ ] Contain the breach immediately
- [ ] Conduct risk assessment
- [ ] Document everything
- [ ] Notify affected individuals (60 days)
- [ ] Notify HHS if required
- [ ] Notify media if 500+ affected
- [ ] Provide credit monitoring if appropriate
- [ ] Review and update security measures
- [ ] Conduct post-incident analysis