HIPAA Disaster Recovery Plan Checklist

Introduction

This checklist has been compiled to help HIPAA covered entities and business associates develop an effective HIPAA disaster recovery plan as required by 45 CFR §164.308(a)(7)(ii)(B). Although other regulatory requirements are mentioned and/or referenced, the checklist is not designed to support compliance with other regulatory requirements.

Preparing for a Disaster

Before it is possible to recover from a disaster, it is essential to know what assets exist and where they are located. In the context of a HIPAA disaster recovery plan, the only asset requiring recovery is electronic Protected Health Information (ePHI).

Therefore, it is recommended that covered entities and business associates identify and document devices, systems, software, and applications that create, receive, maintain, or transmit ePHI, and map data flows of ePHI.

TIP: Further advice on asset identification and management can be found in the NIST Cybersecurity Framework ID.AM-1 to ID.AM-6 and HICP's Technical Volume 2, Practices #4.L.B. and #5.M.A to #5.L.B.

Checklist #1

- ☐ Does the IT disaster recovery team have a documented inventory of ePHI?
- ☐ How will the IT disaster recovery team be notified of changes to the inventory?
- ☐ Do document management procedures exist to amend the document as necessary?
- ☐ Does the inventory document need to be shared with other disaster recovery teams?

Developing a Disaster Recovery Plan

The next stage in developing a disaster recovery plan is to understand what threats exist that could result in a disaster. These might not only include cyberattacks, extreme weather events, and system failures, but also instrumental violence (i.e., civil unrest, active shooters, etc.), and malicious insiders.

Where possible, it is advisable to deploy a failover solution to mitigate the consequences of a disaster. Where this is not appropriate (i.e., to mitigate the consequences of a power outage), it is advisable to deploy a backup solution with remote access capabilities to restore corrupted data.

Because it is often impossible to restore everything at once, it is recommended to assess the asset inventory and prioritize the most critical assets for recovery to meet key recovery point objectives. Remaining assets should be assigned a recovery order to ensure a smooth transition to full recovery.

Checklist #2

- [ ] Have all foreseeable threats that could result in a disaster been identified?
- [ ] Have failover solutions been deployed where possible to mitigate the consequences of a disaster?
- [ ] Are procedures in place to deal with each type of disaster where failover solutions are inappropriate?
- [ ] Have suitable backup solutions with remote access capabilities been deployed?
- [ ] Has the recovery of devices, systems, software, and applications been prioritized?
- [ ] Have primary and secondary emergency communication channels been included in the plan?
- [ ] Are procedures in place to permit emergency access to facilities and devices in the event of an emergency?
- [ ] Have other healthcare industry standards been reviewed to ensure compliance with their requirements?
- [ ] Is it necessary to coordinate with other disaster recovery teams to execute the disaster recovery plan?
- [ ] Has a review of the disaster recovery plan been scheduled for within the next 12 months?

Testing a Disaster Recovery Plan

Before testing a disaster recovery plan, it will be necessary to train members of the workforce beyond the healthcare IT team on the content of the plan in order to cover the possibility of key members of the disaster recovery team are unavailable or incapacitated due to the emergency.

Thereafter, full disaster recovery testing should be conducted at least twice every year to avoid a scenario in which, five years after developing a HIPAA disaster recovery plan, only the responses to five potential disasters out of ten foreseeable disasters have been tested.

Six-monthly testing is not as disruptive as it sounds. Some tests can be conducted as tabletop exercises, while others can be scheduled to coincide with mandated Emergency Preparedness drills. The important thing is that tests are sometimes conducted remotely in case it is not possible to access buildings in which systems and devices exist.

Checklist #3

- [ ] Have members of the workforce beyond the healthcare IT team received disaster recovery training?
- [ ] Has sufficient training been conducted so that team members are familiar with their responsibilities in all disaster scenarios?
- [ ] Have tests been conducted to prioritize the recovery of critical devices, systems, software, and applications?
- [ ] Has testing been coordinated with other disaster recovery teams where appropriate?
- [ ] Has the success of the testing been evaluated to revise plans where necessary?
- [ ] Have repeat tests been conducted where necessary to ensure the revised plan is effective?
- [ ] Have failover solutions been tested to ensure disasters are mitigated wherever possible?
- [ ] Have backup solutions been tested to ensure ePHI can be recovered in full?
- [ ] Have secondary communication channels be used during testing to ensure their effectiveness?
- [ ] Have the procedures developed to comply with other healthcare industry standards been tested alongside the HIPAA disaster recovery plan?

Conclusion

Developing a HIPAA disaster recovery plan requires preparation, thought, and testing. In many cases, it also involves collaboration with other departments, training members of the workforce who may be unfamiliar with technologies, and coordination with emergency responders.

If you require any assistance developing a HIPAA disaster recovery plan, advice about how you should prioritize the recovery of assets, or help with training members of the workforce, it is recommended you seek professional compliance advice.