DISASTER RECOVERY PLAN

OntarioMD
Empowered Practices. Enhanced Care.

A disaster recovery plan consists of detailed procedures related to preparing for and executing the recovery or ontinuation of technology infrastructure after a disaster (e.g. business interruption, community emergency, etc.) has occurred. Disaster recovery planning is crucial for ensuring the continued operations of your computer systems in the event of a disruption (e.g., hardware failure, software issues, viruses, etc.).

It is recommended that the disaster recovery plan be developed in conjunction with your vendor and hardware/network provider. Back-up procedures and testing of the plan are crucial in the event of a disaster. The plan should be tested at least annually.

Guidelines & Tips

1. **Your disaster recovery plan must clearly identify all significant components and associated recovery steps. For example, if a specific workstation is critical to your operations, make sure it has its own recovery process with associated timelines and responsibility.**

2. **For each potential disaster scenario (e.g. business interruption, community emergency, etc.), corresponding business continuity and recovery procedures must be put in place.**

3. **When the business continuity plan is implemented, the recovery process must always be completed in chronological order to ensure a proper recovery.**

4. **Testing of the plan will help ensure that the recovery time matches what was negotiated in the Service Level Agreement (SLA) with the EMR vendor. Identify the maximum time required for recovery to be complete.**

5. **Clearly indicate who is responsible for performing each step in the recovery process as stated in your SLA.**

The table on the following page list examples of the systems, services and functions, identified by a practice as necessary for recovery to maintain current business operations (in order of priority). Each of these starts with the customer notifying the various vendors involved that a critical failure has occurred and the customer ensuring all required software/data back-ups are brought on-site and are available as needed.

This sample disaster recovery information is meant to be used as an example and may change or expand based on the needs of your practice.

Item	Server Components	Recovery Time	Responsibility
1	Replacement server(s) delivered		Hardware Vendor
2	Back-up/recovery software installed		Hardware Vendor
3	Anti-virus software re-installed and configured		Hardware Vendor
4	EMR server components restored		EMR Vendor
5	EMR database recovery		EMR Vendor
5a	Scheduling data		EMR Vendor
5b	EMR data		Vendor
5c	Billing data		EMR Vendor
6	Other application components and data restored (e.g., e-mail, word processing documents)		Hardware Vendor
	Fully restored and available for use (elapsed hours)		

Item	LAN Services	Recovery Time	Responsibility
1	LAN cabling replaced		Cabling Vendor
2	Replacement switches/HUB delivered		Hardware Vendor
3	Switches/HUB configured and installed		Hardware Vendor
	Fully restored and available for use (elapsed hours)		

Item	Lab Interfaces	Recovery Time	Responsibility
1	Phone lines restored		Telecommunications Vendor
2	Replacement workstation delivered		Hardware Vendor
3	Replacement modem delivered		Hardware Vendor
4	Workstation configured and installed		EMR Vendor
5	Lab services restored		EMR Vendor
	Fully restored and available for use (elapsed hours)		

Item	Network Circuit/Internet Services	Recovery Time	Responsibility
1	Replacement router delivered		Network Provider
2	Router configuration restored		Network Provider
	Fully restored and available for use (elapsed hours)		

Item	Printing Services	Recovery Time	Responsibility
1	Replacement print server delivered		Hardware Vendor
2	Replacement printer(s) delivered		Hardware Vendor
3	Print server restored		Hardware Vendor
4	Printer(s) configured and installed		Hardware Vendor
	Fully restored and available for use (elapsed hours)		

Item	Individual Workstation	Recovery Time	Responsibility
1	Replacement workstation(s) delivered		Hardware Vendor
2	Workstation(s) configured and installed		Hardware Vendor
3	EMR applications configured and installed		EMR Vendor
4	Anti-virus software re-installed and configured		Hardware Vendor
5	E-mail software re-installed and configured		Hardware Vendor
6	Browser software re-installed and configured		Hardware Vendor
	Fully restored and available for use (elapsed hours)		

EMR Vendor Contact Information: ____________________

Hardware Vendor Contact Information: ____________________

Telecommunications Contact Information: ____________________