



Indiana Professional Management Group, Inc.

Disaster Recovery Plan

Disaster and Business Contingency Plan Overview

IPMG's Disaster Recovery Plan describes the processes in place or actions staff members would take in response to a natural or human-caused disaster. The Disaster Recovery Plan is the approach IPMG would execute to recover in a timely manner in order to continue normal business operations.

Disaster Plan by Types

Environmental

- Tornado
- Fire
- Flood
- Drought
- Snowstorm
- Freezing Conditions
- Earthquake
- Electrical Storm
- Contamination and Environmental Hazards
- Epidemic or pandemic

Equipment Failure and Other Emergencies

- Internal Power Failure
- Heat, Ventilation, Air Conditioning Failure
- Health and Safety Regulation

Plan

In the event of an environmental, equipment failure, and other emergency disasters, employees have the ability to work remotely and access the ePHI from any computer that has a working internet connection using an individualized username and password to continue regular job duties. IPMG uses web-based systems controlled by the State of Indiana to store all electronic protected health information (ePHI) for individuals served. Employees are provided the necessary equipment with required safeguards that are in compliance with HIPAA to ensure the privacy and security of ePHI when working offsite. When an environmental event occurs, IPMG will contact the insurance company and information technology (IT) vendor for guidance and recovery efforts to continue normal business operations.

Network

- Cyber crime
- Loss of records or data
- IT system failure

My company... Your company... Our company! **100% Employee-Owned!**

Plan

In the event of a network failure or other network disaster, all electronic records are stored in a secure cloud-based storage that can be recovered from any point in a 30-day period. The network equipment and backup management of the cloud storage is managed by IPMG's information technology (IT) vendor. The IT vendor is local to the IPMG home office and can repair or replace equipment timely to resume normal business operations. For any network or equipment downtime, a user can connect a device to another network and access systems and information to continue regular job duties.

In the event IPMG experiences a cyber-attack, the IT vendor will be contacted for repair and recovery efforts. IPMG has cyber security insurance coverage and would be contacted for their guidance. The proper federal, state and local authorities, such as the Federal Bureau of Investigations (FBI) and local United States Secret Service Electronic Crimes Task Force, would be contacted to report the incident.

Organized and/or Deliberate Disruption

- Act of terrorism
- Act of sabotage
- Act of war
- Theft
- Arson

Plan

If IPMG experiences an organized or deliberate disruption, the proper federal, state, and local law enforcement agencies will be contacted. IPMG employees are provided the necessary equipment with required safeguards that are in compliance with HIPAA to ensure the privacy and security of ePHI when working offsite. If an organized or deliberate disruption occurs, IPMG will also contact the insurance company and information technology (IT) vendor for guidance and recovery efforts to continue normal business operations.