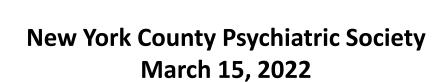
CONTINGENCY PLANNING



Charles D. Cash, JD, LLM

Associate Director of Risk Management Professional Risk Management Services (PRMS)

CME DISCLOSURE

I have no financial relationships with any ineligible companies.

DISCLAIMER

Nothing I say today is legal advice!

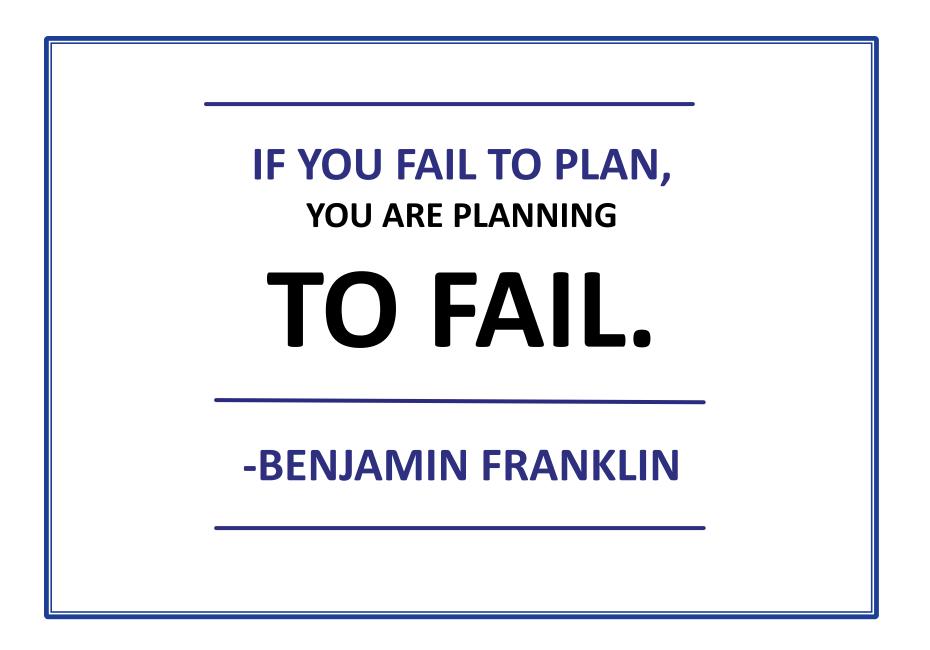
OBJECTIVES

At the conclusion of this program, attendees will be able to:

- Explain the importance of having contingency plans for an office-based practice.
- Describe the elements of a contingency plan.

GOALS OF A DISASTER PLAN

- Minimize the probability of injury or loss related to your patients, visitors, and or employees in an emergency;
- 2. Minimize, or prevent altogether, the risk of property loss (including equipment, patient and business records, etc.)
- *3. Minimize* down time and expedite your recovery from the disaster.



DEVELOPING THE PLAN GETTING STARTED

GETTING STARTED: MAKE A LIST

- Tornado
- Hurricane
- Flood
- Earthquake
- Blizzard
- Fire
- Burst pipe
- Power outage
- Hazmat spill
- Bomb threat
- Nuclear disaster

- Pandemic
- Tsunami
- Terror attack
- Medical emergency
- Psychiatric emergency
- Violent patient
- Ransomware attack
- Psychiatrist's health crisis
- Civil unrest
- Avalanche
- Etc.

Early warning

- Community alerts
- NOAA Radios

List of contacts

- Staff
 - > All methods of contact
 - > Chain of command
- Utility companies
- Plumber
- Electrician
- Internet service provider
- Cell phone service provider
- EHR tech support

List of contacts

- Building manager
- Building security
- Insurance agent
- Cleanup/restoration company
- Health department
- FEMA
- PRMS or your own carrier

Patient communication plan

- Outgoing voicemail message
- Website
- Patient portal
- Other social media
- Can landline number be forwarded to a cell
- Instructions for answering service

Securing medical records *before* a disaster

- Electronic health records
 - > HIPAA Security Rule
 - > Backup
 - Backup tape secure location
 - Remote storage separate locations

Securing medical records *before* a disaster

- In office
 - Locked
 - > Fire-proof cabinet
 - > Away from water
- Off-site

Securing medical records after a disaster

- Act quickly!
- Secure what remains of records
- Take photos of damaged area
- Keep copies of insurance claims
- Newspaper clippings
- Ascertain whose records were affected

Securing medical records after a disaster

- Reconstruct
 - > Start with most active files
 - Clearly document reconstruction
 - > Be candid with patients
 - > Gather copies from other providers
 - > Pharmacy records
 - > PMP
 - > Duty to retain damaged records

Insurance coverage

- Sufficient funds to get you back into operation?
- Current or replacement value?
- Photos or video of assets
- Floods and earthquakes?
- Business interruption insurance?
- Keep copies off-site

Remote operation/Business continuity

- Equipment
 - Computer
 - > Fax
 - Scanner
- Records access
- Billing system
- Cash reserve/line of credit

Loss of internet

- Record access
- Prescription pads
- Encounter forms
- Paper progress notes
- Receipt book
- Message slips

Emergency supplies/equipment

- First aid kit
- Flashlight
- Fire extinguisher
- Defibrillator
- Basic tool kit
- Battery operated radio
- Supplies to shelter in place

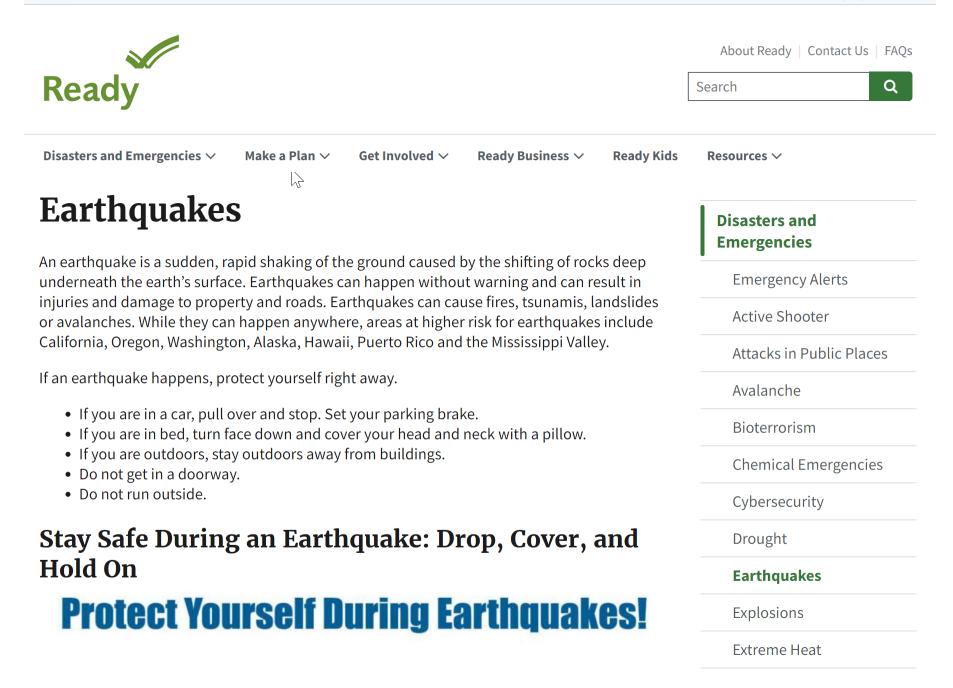
Contingency plan

- Contacts
- Chain of command
- Access records, voicemail, calendar, etc.
- Psychiatrist to cover
- Prescription refills
- Instructions re release of records
- What to tell patients
- Others to call for advice

DEVELOPING THE PLAN SPECIFIC NEEDS

HELPFUL HINT

Every state and most large cities have an emergency management office tasked with providing guidance and information in case of disaster. Most, if not all, of these offices have websites with useful information that will aid you in your emergency planning.



<u>Fire</u>

- What's already in place?
- Building evacuation plan
 - > Route unobstructed
 - > Fire doors unlocked
 - > Make copies of maps
- Smoke detectors
- Sprinkler system
- Fire and other alarms
- Fire extinguishers regularly checked
- If no plan, discuss

Fire safety tips

- Don't overload circuits
- Replace frayed cords
- Turn off/unplug unused appliances
- Keep fire doors closed
- Don't block exits
- Remove paper and trash
- Don't allow candles
- Fire extinguisher
- Smoke alarms

Fire – other considerations

- Designated location
- Ensure file cabinets closed
- Patients with mobility issues

Flooding

- Consider office location
 - > Flood plain
 - > First floor
- Storage within office
 - > Active and inactive
- Off-site storage
 - > Home
 - > Storage facility
 - > Other

Tornado/severe storms

- Advance warning
- Basement
- Designated storm shelter
 - > Not cluttered with storage
- Other area in building
- Map
- Plan for directing patients

Cyber/Ransomware Attack

- Malicious software encrypts files
- Payment is demanded for encryption key
- Phishing emails or "drive-by" downloading
- Healthcare providers often targeted
 - > Value of healthcare records
 - > Industry transition to EHRs
 - > Lack of security technology in small practices

How to prevent

- Recognize the risk
- Train staff
 - > Preventing ransomware
 - Email attachment
 - Emails
 - Downloading software
 - What info is okay to access and what is not
- Backup important data and store offline

How to prevent

- Encrypt sensitive practice data
- Implement technical safeguards
 - > Up-to-date antivirus software
 - Enable automated patches for operating system and web browsers
 - > Use complex passwords
 - > Enable pop-up blockers
- Don't get complacent
- OCR Security ListServ

Psychiatric/medical emergencies

- Involuntary commitment procedure
- If using medical supplies/equipment:
 - Secure storage
 - Access
 - Expiration
 - Credentials
 - > PPE

Violent patient/visitor

- Training for front-line staff
 - Identify problem
 - Under influence of alcohol/drugs
 - Agitation
 - Anger
 - Profanity
 - > Activate emergency system
 - > Retain distance
 - > Call 911
- Panic button
- Back exit
- Avoid after-hours appointments

FINALIZING THE PLAN

FINALIZING THE PLAN

- Keep it simple
 - > Easy to understand = easy to implement
- Keep it accessible
- Keep in practice
 - Regular training
 - > Testing
 - Is staff familiar with plan?
 - Do they know protocols for each type of disaster?
 - Do they know and understand their respective duties in each situation?
- Keep it updated

RESOURCES

- Federal Emergency Management Agency *www.fema.gov*
- FEMA links to your local state Emergency Management Agency www.fema.gov/emergency-management-agencies
- American Red Cross www.redcross.org/services/disaster/beprepared/busi_industry.html
- U.S. Department of Homeland Security *www.ready.gov*