Disaster Preparedness:
The roles of people and technologies to ensure safety
Introductions

Cheri Silveira, Director of Risk Management, Xpio Health

Adam Bullian, JD Xpio Health

Nancy Del Real, Behavioral Health Manager, Information Systems, Imperial County Behavioral Health Services

Cinthia Madrigal, Administrative Analyst, Information Systems, Imperial County Behavioral Health Services
The IT component of Contingency Planning is the process of ensuring that essential information processing functions (such as access to EHR or patient information) can be maintained throughout a variety of incidents and emergencies.

Minimum IT Security requirements:

- **Identify** the functional areas essential to business operations.
- **Determine** how each situation, such as fire or flood, would affect these key areas, what actions would be taken and the resources needed for each.
- **Set goals** for the return to essential operations and return to full normal operations.
- **Identify each required process** and document each step in the process, what needs to be done, along with the staff and other resources needed to complete the work. Develop plans for each functional area and the organization as a whole.
- **Implement a communications and education plan** to keep employees informed of changes and remind them of their roles and responsibilities.
Business Impact Analysis

An agency first must identify and prioritize essential functions and what is required to support those functions. Include communication channels and how best to reach staff and clients.

Consider business, clinical and financial processes; who provides services, who receives services, recovery time and other processes that are dependent. Remember to keep IT a priority.

Example:

**Business unit** = Crisis Service Program
**Process** = Provides walk in and phone crisis services at the Main St. location
**Priority** = High
**Services Provided** = Crisis staff on site and phone management staff located at same location
**Recovery Time Objective** = Need to be back up within 1 hour
**Process Depends on** = Rented facility management, hard-lined phone systems, EHR system, staff on-site
**Required by** = Community members in crisis (consider higher volume during an emergency)
**Systems used** = Electronic Health Record, State Eligibility System, Phone Company (both hard line and wireless)
Threats and Risks

Identify possible threats and risks so you can describe how you will mitigate.

Examples:
1. Damage to building/facility that prevents access
2. Destruction of essential equipment, i.e. servers, networks
3. Loss of communication; email, phones
4. Loss of access to EHR/client records
5. Staff/Management unable to report to work
6. Loss of contractor/vendor support
7. Damage to business/client documents
8. Loss of data integrity, i.e. phishing that results in data encryption, physical damage to database
IT Disaster Recovery

IT Disaster Recovery is a subset of the Business Continuity Plan. This is where you address procedures to maintain or restore the essential IT services/functions.

Emergency Mode Operations will address now to notify staff to carry out their responsibilities and document alternate personnel as needed during the course of an emergency.

Communication is the key.
Continuity Plan

Operational Phases

1. Readiness and Preparedness
   • Planning, training, testing

2. Activation and Relocation
   • Guides the response, with a focus on alert, notification, communication and relocation

3. Continuity Operations
   • Process of restoring essential functions, delegation of authority, and interim processes

4. Business Resumption
   • The process of restoring all functions at the original level, location
Maintenance of Plan

A plan is not developed and then put in a drawer. The overall review should include:

• **Schedule** an annual review of the documentation and update as needed.

• Confirm all **policies and procedures** are updated.

• **Test** your plan; quarterly table top testing with representatives from the organization is recommended with an annual full restore from back up test.

• **Train, train, train** so staff feel comfortable with the process.
Imperial County – Who We Are

Clients Served FY16-17: 7,683
Staff: 515 and growing
System Users: 442

Databases:
- Electronic Health Record
- Shared Files
- Document Imaging
- Accounting

Applications:
- ICBHS Network
- MyAvatar
- MS Office
- Outlook
- Cisco Registered Envelope Service
- FoxPro
- Kef
Imperial County – Who We Are

1. Structure – County MHP
   - Department Information System
   - Supported by Systems Technology

2. Information Systems
   - Supports applications and data
   - Ensures HIPAA Compliance

3. Systems Technology
   - Supports hardware – configuration and installation
   - Supports network configuration / firewalls
Imperial County - Process of putting plan together

- Put together a **Team**
- Assign **responsibilities**
- **Coordinate** meetings with Team
- Identify and prioritize key risks
- Obtain a **template** and modify according to your organization’s needs
- Attachments i.e. Policies & Procedures, Tables
- Present plan to Management for **approval**
Imperial County -
Team Members and Responsibilities

- Information Systems/Systems Technology Manager/Supervisor
  - Provided guidance and leadership for sign off
- Administrative Analysts
  - P&P
  - Coordination of Emergency contact, Information/Documentation
- Systems Support Analyst
  - Servers Layout/Technical Procedures
- Contract Xpio Health
  - Guidance and coordination
Imperial County - Communication Strategies

- Disaster/Crisis Line of Succession for clinical staff
- Information Systems Team for activation of plan
- Management/Supervisors need staff personal phone numbers
- Method of communication
  - Phone
  - Text
  - Email
  - Other
Imperial County - Testing, Training and Maintenance

- Coordinate and conduct **tabletop testing**
  - Scenario
  - Tested with one Program, will eventually test by division
  - Quarterly Tabletop & Annual backup recovery

- **Training** Provided
  - Education to all staff members
    - Management
    - Team Leaders
    - All Staff

- Ensure plan **maintenance**
  - Living Document
Imperial County - Lessons Learned

- Multiple priorities made it difficult to prioritize the plan development
- Coordination and flexibility of resources, staff, timing, and supplies in relation to the County Emergency Operations Plan
  - Cross training
- Understand your situation
  - Budgetary, resources, organizational processes
- Time commitment and preparation
- Complete P&P’s before starting Plan
  - Access Control policy & Contingency Plan Policy
Imperial County-Desktop Testing Recommendations

- Select a Crisis/Access unit as the testing program
- Select your most likely scenario
- Keep the testing team small (6-8 people) with different roles
  - Manager
  - Supervisor
  - Clinician
  - Clerical
  - Systems Support Analyst
  - Administrative Analyst
  - Facilitator
  - Scribe
- Use your past experiences and test results as a way to guide updates to the plan.
QUESTIONS ANSWERED HERE EVEN THE SILLY ONES