Community Clinic Association of Los Angeles County

Business Continuity and Electronic Health Record Resource Toolkit

July 2013
Acknowledgements

Community Clinic Association of Los Angeles County
Members and Staff

Jason Hua, Chief Information Officer, Venice Family Clinic
Ofer Ho, Chief Information Officer, Eisner Pediatric & Family Medical
Stephen Gutierrez, Director of Information Technology, Northeast Valley Health Corp
Michael Gorecki, IT Systems Administration, Family Health Care Centers of Greater Los Angeles
Martin Perez, Manager of Health Information Technology, The Saban Free Clinic
Paul Ramos, Chief Financial Officer, PPS, South Central Family Health Center
Trevor Rhodes, MPA, Disaster Preparedness Coordinator, CCALAC

Prepared by:
Connect Consulting Services
Nora O’Brien, MPA, CEM
1104 Corporate Way, Sacramento, CA 95831
916 806-7361 NoraOBrien@me.com
Ellie Anderson, Anderson Healthcare Readiness, hcreadiness@gmail.com
Eileen Tremaine, Tremaine Consulting Group, eileentremaine@me.com
OUTLINE THE LOGISTICS OF RECOVERING CRITICAL BUSINESS FUNCTIONS.

SPECIFY THE CRITICAL BUSINESS ACTIVITIES THAT NEED TO CONTINUE AFTER AN INCIDENT.

IDENTIFY THE TEAMS THAT WILL COMPLETE THE SPECIFIC ACTIVITIES NECESSARY TO CONTINUE CRITICAL BUSINESS AFTER A CALAMITY.

IDENTIFY KEY INDIVIDUALS WHO WILL MANAGE THE PROCESS OF RECOVERING AND RESTORING THE BUSINESS.

PROVIDE A PLAN OF ACTION TO FACILITATE AN ORDERLY RECOVERY OF CRITICAL BUSINESS FUNCTIONS.

MINIMIZE ECONOMIC LOSSES RESULTING FROM DISRUPTIONS TO BUSINESS FUNCTIONS.

Table of Contents

PROJECT OBJECTIVE FOR BUSINESS CONTINUITY ............................................................................................................. 6

MINIMIZE ECONOMIC LOSSES RESULTING FROM DISRUPTIONS TO BUSINESS FUNCTIONS ................................................. 6

PROVIDE A PLAN OF ACTION TO FACILITATE AN ORDERLY RECOVERY OF CRITICAL BUSINESS FUNCTIONS ..................... 6

IDENTIFY KEY INDIVIDUALS WHO WILL MANAGE THE PROCESS OF RECOVERING AND RESTORING THE BUSINESS AFTER A CALAMITY ............................................................................................................. 6

IDENTIFY THE TEAMS THAT WILL COMPLETE THE SPECIFIC ACTIVITIES NECESSARY TO CONTINUE CRITICAL BUSINESS FUNCTIONS ............................................................................................................... 6

SPECIFY THE CRITICAL BUSINESS ACTIVITIES THAT NEED TO CONTINUE AFTER AN INCIDENT .......................................................................................................................................................... 6

OUTLINE THE LOGISTICS OF RECOVERING CRITICAL BUSINESS FUNCTIONS ............................................................................................................................................................................. 6

Electronic Health Record Step 1: Assess Your Practice Readiness ............................................................................................................. 6

Electronic Health Record Step 2: Plan Your Approach ................................................................................................................................. 8

Electronic Health Record Step 3: Select or Upgrade to a Certified EHR ............................................................................................................. 11

Electronic Health Record Step 4: Conduct Training & Implement an EHR System ............................................................................................................. 12

Electronic Health Record Step 5: Achieve Meaningful Use ................................................................................................................................. 14

Electronic Health Record Step 6: Continue Quality Improvement ............................................................................................................. 16

Appendix A: BCP-Hazard Vulnerability Assessment Tool- see attached ............................................................................................................. 28

Appendix B: Clinic Disaster Preparedness and Business Continuity Worksheet ............................................................................................................. 29

Appendix C: Clinic Business Continuity Plan: Electronic Health Record Planning Tool ............................................................................................................. 38

Business Continuity Plan ............................................................................................................................................................................. 41

Plan Objectives ............................................................................................................................................................................. 41

Assumptions ............................................................................................................................................................................. 41

Disaster and Adverse Event/Incident Definition ............................................................................................................................................................................. 42

Key Roles and Responsibilities ............................................................................................................................................................................. 43

Disaster Declaration ............................................................................................................................................................................. 46

Notification ............................................................................................................................................................................. 46

Adverse Events Response ............................................................................................................................................................................. 46

BCP Contact List ............................................................................................................................................................................. 49

Appendix D- How to Conduct a Business Impact Analysis Step Process ............................................................................................................. 51

Appendix E- EHR Vendor Selection Planning Checklist ............................................................................................................................................................................. 59

Appendix F- Electronic Medical Record - Patient Centered Medical Home Implementation Planning Crosswalk ............................................................................................................................................................................. 61

Appendix G: Disaster/Disruption Mitigation Strategies ............................................................................................................................................................................. 62

Appendix H: HIPAA Compliance Guidance Regarding Disaster Recovery Planning ............................................................................................................................................................................. 64

Appendix I: Vital Records Worksheet ............................................................................................................................................................................. 66

Appendix J- Community Clinic Exercise Planning Checklist ............................................................................................................................................................................. 68
About The Resource Toolkit

The Community Clinic Association of Los Angeles County (CCALAC) has developed this resource toolkit in order to provide templates, information, and tools for members to enhance your CC business continuity planning (BCP) as you implement and maintain your electronic health records (EHR) systems. Business Continuity plans are one of the requirements in Health Resources and Services Administration Program Information Notice HRSA EP Expectations PIN 2007-15 that encourages community clinics (CC) to have emergency plans in place in times of disaster or emergencies. While the majority of CCs have some back up plans in place to access vital records after disaster, comprehensive business continuity plans also need to address alternate staffing plans and alternate facilities that will allow you to continue to serve your communities and patients despite business interruptions.

It is recommended that you review the entire toolkit regardless of which stage of EHR implementation your clinic organization is in to determine if there are tools and resources that can increase your organization’s disaster resiliency after disaster. In addition, much of the Patient Centered Medical Home (PCMH) work that your CC is undertaking can also be integrated to your emergency operations and business continuity planning.

The BCP- EHR Resource Toolkit is organized in the following sections:

- **Business Continuity Planning Considerations for each EHR step**
- **Community clinic planning tools, templates, and resources** to support your business continuity and electronic health records planning work
- **Public Domain reference and resources** documents
Business Continuity Introduction to Keys Terms and Concepts

Business continuity is the activity performed by an organization to ensure that critical business functions will be available to patients, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as patient care, project management, system backups, and clinic operations. Business continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

For example, if the Internet and power is knocked out due to an earthquake, or the clinic building is damaged, or your core staff is evacuated, injured or unavailable, your clinic organization would activate your business continuity plan that gives you alternate operational procedures to serve your patients. Those alternate operational procedures could include strategies that such as reverting to paper patient records, using your mobile medical van to serve patients at another site, or obtain staff from another of your clinic sites or from a fellow community clinic. The more robust your business continuity plan is that incorporates the three core planning considerations, the more likely your clinic organization can quickly recover after a disaster.

Business continuity planning identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization. The foundations of business continuity are the standards, program development, and supporting policies; guidelines, and procedures needed to ensure a firm to continue without stoppage due to planned or unplanned events, irrespective of the adverse circumstances or events.

The term Business Continuity describes a mentality or methodology of conducting day-to-day business, whereas business continuity planning is an activity of determining what that methodology should be.
**Business Continuity Plan** is a roadmap for continuing operations under adverse conditions and may be thought of as the incarnation of a methodology that is followed by everyone in an organization on a daily basis to ensure normal operations.

Business Impact Analysis (BIA): A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resources loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

**Project Objective for Business Continuity**
- Minimize economic losses resulting from disruptions to business functions.
- Provide a plan of action to facilitate an orderly recovery of critical business functions.
- Identify key individuals who will manage the process of recovering and restoring the business after a calamity.
- Identify the teams that will complete the specific activities necessary to continue critical business functions.
- Specify the critical business activities that need to continue after an incident.
- Outline the logistics of recovering critical business functions.

**What is disaster recovery? DRP is different than BCP. EHR is part of both.**

Disaster recovery is the technical aspect of business continuity. The collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption of IT services.
Electronic Health Record Step 1: Assess Your Practice Readiness

Key Business Continuity Planning Considerations

**Data and Communication Infrastructure:**
- Educate the staff on business continuity principles by developing business continuity plan that takes into account not just data protection but also staffing and facility availability.
- Conduct a Hazard Vulnerability Assessment (HVA) to determine which man-made and natural disasters that your organization is at greatest risk of interrupting your business and your organization’s EHR.
- Create/maintain an existing business continuity plan in place regarding data protection.
- Ensure that the security and risk assessment process assesses the data protection, facility risks, and the loss of staff risks.
- Identify alternate connectivity needs that could provide you EHR access after disaster.
- Determine whether you have the capacity to self-host your EHR environment or if you should contract hosting.

**Facility:**
- Create/maintain a business continuity plan in place regarding how to access patient data without your facilities.
  - Can you relocate at another CC site of yours and/or your neighboring CC?
  - Can you use another location such as a church or school?
  - Do you have the use of a mobile medical van to treat patients at an alternate location?
  - What medical and non-medical supplies as well as equipment do you need to temporarily relocate your CC facility?
- Include your facilities and operations staff in the workflow assessment process to identify staff and facility processes along with IT that could support business continuity activities.
- Include your facilities staff in the workflow redesign process to ensure that data, facility, and staff planning considerations are taken into account.
- Understand that vital records include not only patient data, but also electronic and hard copy documents, references and records needed to support essential business functions. This includes documents such as your Emergency Operations Plan, Business Continuity Plan, personnel, social security, payroll, insurance, and contract records, as well as Mutual Aid Agreements.
Staffing:
- Identify which CC staff and external vendors perform key business functions
- Create/update an alternate staffing plan in place regarding how to access vital records without your key staff in times of disaster
- Include your facilities and operations staff in the EHR Planning Team, workflow assessment team and workflow redesign teams so that more than just the IT perspectives are represented

Community Clinic Business Continuity - EHR Tools

- Appendix A: Business Continuity Electronic Health Records Hazard Vulnerability Assessment Tool – This tool allows CCs to pinpoint your EHR and clinic operations disaster risks as it relates to your EHR stage

- Appendix B: Clinic Disaster Prep and Business Continuity Worksheet- This introductory assessment is meant to provide a venue for clinics to keep important contact information updated, identify areas of excellence in planning, and assist clinics in considering areas where in-services, individual or small group training, or information gathering is beneficial for the clinic’s Business Continuity plan.

Public Domain Business Continuity – EHR Reference and Resource Documents
1. Kaiser HVA Tool- This HVA tool was created by Kaiser Permanente for medical health centers
Electronic Health Record Step 2: Plan Your Approach
According to Health IT.gov and the National Learning IT Consortium, below are 7 steps to planning for an EHR. Each of the EHR planning steps have elements that are linked to emergency management and business continuity.

1. Analyze and map out the practice’s current workflow and processes of how the practice currently gets work done (the current state).
   a. **Business Continuity Planning Consideration**: When you identify your current workflow, identify the information technology activities but also the operational and staff responsibilities for each of the steps.

2. Map out how EHRs will enable desired workflows and processes, creating new workflow patterns to improve inefficiency or duplicative processes (the future state).
   a. **Business Continuity Planning Consideration**: Conduct a Business Impact Analysis to determine each of the business functions, a criticality score based upon need ranging from critical business functions to delayed (email vs. conducting a health fair), and ID internal and external staff dependencies.

3. Create a contingency plan – or back-up plan – to combat issues that may arise throughout the implementation process.
   a. **Business Continuity Planning Consideration**: Have the back-up plan include duties for IT, facilities, and a redundant staffing plan
   b. **Business Continuity Planning Consideration**: Have your organization listed as a vital priority resource for voice communication [Government Emergency Telecommunications Service (GETS)] and [Wireless Priority Service] for wireless communication

4. Create a project plan for transitioning from paper to EHRs, and appoint someone to manage the project plan.
   a. **Business Continuity Planning Consideration**: Create a EHR to paper EHR modified process.
   b. **Business Continuity Planning Consideration**: Create the EHR- paper-tracking tool to be used in time of disaster.
5. Establish a chart abstraction plan, a means to convert or transform, information from paper charts to electronic charts. Identify specific data elements that will need to be entered into the new EHR and if there are items that will be scanned.

6. **Business Continuity Planning Consideration**: When developing the chart abstraction plan, create chart abstraction procedures, identify and cross train several IT staff to conduct process.

7. Understand what data elements may be migrated from your old system to your new one, such as patient demographics or provider schedule information. Sometimes, being selective with which data or how much data you want to migrate can influence the ease of transition.
   
a. **Business Continuity Planning Consideration**: Determine which modified data fields are needed for a paper patient tool that takes into account medical billing, patient medical history, and staff involvement—i.e., medical assistant vs. provider usage.

8. Identify concerns and obstacles regarding privacy and security and create a plan to address them. It is essential to emphasize the importance of privacy and security when transitioning to EHRs. Get started using the Health Information Privacy and Security: 10 Step Plan.
   
a. **Business Continuity Planning Consideration**: Security risk assessment and management encompasses IT and communications infrastructure, facilities, and staffing risks.

**Community Clinic Business Continuity—EHR Tools**
- Appendix C: Clinic Business Continuity Plan (BCP) – Electronic Health Record Planning Tool This Business Continuity Plan (BCP) – Electronic Health Record (EHR) planning tool will assist in planning for immediate and long-term response to adverse events and disasters by outlining the actions necessary to ensure continuance of patient care and business operations.

- Appendix D: How to Conduct a Business Impact Analysis Step Process- This tool provides a step-by-step process for conducting a clinic business impact analysis.

**Public Domain Business Continuity—EHR Reference and Resource Documents**
- [National Association of Community Health Centers Business Continuity Planning Tool](#) - It is intended to provide community clinics an easy to use tool to create and improve their business continuity plan and program.
- **California Hospital Association Continuity Planning Documents** - These continuity planning tools are designed to educate hospitals on establishing and maintaining a continuity program that will allow the continuation of essential clinical, research, business and administrative operations in the event of natural, technological, man-made or public health emergencies.

- **NHS North East London Business Continuity and Electronic Health Record Sample Plan** - This business continuity plan describes the process for ensuring business continuity in the event of inability to access the EHR. It provides guidance to staff to ensure essential clinical information is available to staff while EHR is unavailable and essential clinical and reporting data is recorded on EHR in a timely manner following the resumption of electronic health service.
Electronic Health Record Step 3: Select or Upgrade to a Certified EHR

Besides factors such as price and software support in considering which EHR vendor would best suit your organization should be a consideration for those EHR vendors that have developed strong alternate business procedures so that they can continue their business after disaster. Below are some business continuity questions to ask when evaluating EHR vendors:

**General emergency management and business continuity questions**

- Has the EHR vendor conducted a Hazard Vulnerability Assessment to determine their man-made and natural disaster risks and vulnerabilities?
- Does the EHR vendor have a comprehensive business continuity plan in place that addresses data, facility and staffing impacts?
- How often and how (tabletop exercise and/or functional exercise) is the EHR vendor’s business continuity plan exercised and updated?
- Has the EHR vendor had business interruptions in the past and what were the action steps to get their business operations reconstituted?

**Data and Communication Infrastructure**

- What are the patient record data protection processes does the EHR vendor has in place?
- How does those data protection process meet the HIPAA privacy standards in time of disaster?
- Has there been a previous data breach and what were the policies that were put in place to minimize future data breaches?
- What is the EHR vendor’s technical assistance process to help you move from EHR to paper patient tracking and other viral records back to EHR after disaster?
- Is your EHR vendor listed as a vital priority resource for voice communication Government Emergency Telecommunications Service (GETS) and Wireless Priority Service for wireless communication?
- Does the EHR vendor have:
  - Alternate Internet access procedures and equipment?
  - A generator or alternate power supply?
  - Recommendations for data back-up processes?
  - Redundant communication systems and/or equipment such as satellite phones, ham radios, push-to-talk radios, etc. to reach out to vendors, other businesses, partners, and customers?
Facility
- Does the EHR vendor have an alternate facility plan if the main building(s) are unavailable after disaster?
- Does the EHR vendor have a plan that addresses policies and procedures to temporarily relocate to an alternate location?
- Does the EHR vendor have policies in place to prioritize customers' needs based upon their needs after disaster?

Staffing
- How many of the EHR vendor’s staff are cross-trained on the organization’s alternate back-up procedures?
- Has the EHR vendor determined their critical business functions and which internal and external staff dependencies complete those business functions?
- Does the vendor have an alternate staffing plan in place to address interruptions in service?

Community Clinic Business Continuity - EHR Tools
- Appendix E - EHR Vendor Selection Business Continuity Planning Checklist - Complete checklist that provides business continuity themed questions to ask of your potential EHR vendors

Public Domain Business Continuity – EHR Reference and Resource Documents
HealthIT.gov EHR Selection Tools - These tools provide you with resources to identify the most appropriate EHR vendor for your organization

HITEC-LA EHR Selection Tool - The downloadable Word document, written in RFI format, enables providers to gather detailed information from EHR vendors about their product which is based on the HRSA document, Electronic Health Records: Selection Guidelines for Health Centers HRSA EHR Selection Tool
Electronic Health Record Step 4: Conduct Training and Implement an EHR System

According to Health IT.gov and the National Learning IT Consortium, EHR implementation involves the installation of the EHR system and associated activities:

- Chart abstraction plan and other data migration plans in conjunction with your EHR vendor
  - Business Continuity Planning Consideration: Develop clear abstraction plan procedures to ensure more than a few staff people are trained on the process
- Execution of an EHR implementation training plan that includes practice specific goals and needs, as well as compliance with Meaningful Use objectives
  - Business Continuity Planning Consideration: Develop EHR training plan that provides a role for both IT and operations staff to ensure that many perspectives are included in the training plan and implementation
  - Business Continuity Planning Consideration: Develop a EHR non-access scenarios based upon different types of disasters (flood, earthquake, fire, etc.) to test your business continuity plan after you go live with the EHR system
- Privacy and security risk management mitigation plan
  - Business Continuity Planning Consideration: The privacy and security risk management plan must take into account not only the security risks that will impact data protection but also the internal and external man-made and natural disaster risks faced by the organization that could impact the staffing and facility risks
  - Business Continuity Planning Consideration: Identify gaps in planning and training for existing business continuity plan.
  - Business Continuity Planning Consideration: Develop disaster mitigation strategies to address the potential for the unavailability of your EHR due to disaster.
  - Business Continuity Planning Consideration: Ensure that your disaster recovery plan is compliant with Health Insurance and Privacy and Portability Act (HIPAA) regulations.

Community Clinic Business Continuity- EHR Tools

- Appendix F- EHR -PCHM — Business Continuity Planning Crosswalk- This tool is intended to be used to determine the emergency management and business continuity planning gaps and overlap of both PCMH and BCP standards and planning elements.
Appendix G- Disaster Mitigation Strategies – This information provides guidance on developing disaster mitigation strategies.

Appendix H- HIPAA Guidance on Disaster Recovery Regulations- Contingency planning is a HIPAA Security standard that establishes and implements, as needed, policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI

Public Domain Business Continuity – EHR Reference and Resource Documents

- **Health IT.gov Security Risk Assessment** - This tool was created by HealthIT.gov to assist healthcare providers in assessing their risks related to data breaches

- **Disaster Resource Guide- BCP in a Healthcare Environment Article** - this article summarizes the healthcare business continuity challenges and implementation strategies

- **ABA Guide to Developing and Conducting Business Continuity Exercises** - This guide developed by the American Bar Association Guide provides suggestions, and examples to assist members in planning and conducting business continuity exercises.

- **FEMA Business Continuity Plan Scenarios** - Several scenarios for testing business continuity plan

- **Hunting the Black Swans in Your Continuity Program Article** - “Black Swans” in your Continuity Program are those events that remain outside the range of your normal expectations, and may well produce a significant negative impact when they occur. This series discusses some of the most common of these “black swans” in business continuity programs, those that are really staring us in the face and screaming for attention.
Electronic Health Record Step 5: Achieve Meaningful Use

The five domains of achieving Stage 1 Meaningful Use, which is the use of certified EHR technology to achieve health and efficiency goals, are determined by the Centers for Medicare and Medicaid. For each of the domains, listed below are the business continuity planning considerations.

- **Improve Quality, Safety, Efficiency**
  
  - **Business Continuity Planning Consideration:** Ensure that your EHR plan includes an alternate IT, facilities, staffing plan for your organization
  
  - **Business Continuity Planning Consideration:** Develop an Incident Command System (ICS) as part of your emergency preparedness and business continuity plan to ensure that you can provide efficient patient care after disaster.

- **Engage Patients & Families**

  - **Business Continuity Planning Consideration:** Promote disaster preparedness to clinic staff, Board members, and patients because when all are engaged in disaster preparedness, they are more likely to be clear on their roles in disaster

- **Improve Care Coordination**

  - **Business Continuity Planning Consideration:** Determine if other healthcare partners (hospitals, pharmacies, and long term care agencies) have business continuity plans in place to support sharing patient records and to provide continuity of care despite the potential lack of EHR access

- **Improve Public and Population Health**

  - **Business Continuity Planning Consideration:** Consider creating an emergency supply cache of medical (crash cart, bandages, suture supplies, PPE) and non-medical supplies (water, food, blankets, duct tape, flashlights) so that you can respond to your patients’ needs after disaster

- **Ensure Privacy and Security for Personal Health Information**

  - **Business Continuity Planning Consideration:** Consider not only the personal health information data risk mitigation but also those risks due to man made or natural disasters that could impact your facility and staff
Business Continuity Planning Consideration: Consider how your organization can safely access the patient records despite lack of building access or available trained staff

Community Clinic Business Continuity - EHR Tools
- Appendix I- Clinic Vital Records Worksheet- This worksheet was designed to help community clinics identify the vital records and design systems to keep those records safe and appropriately saved and/or accessible (depending on the type of record) during an incident

Public Domain Business Continuity – EHR Reference and Resource Documents
- KSPCA Clinic Incident Command Roles and Responsibilities- This appendix offers a general explanation of ICS and its use, and it identifies staff positions that will assume responsibility of the ICS functions during an incident
- HIPAA Regulations and Resources
  - Final Rule, GPO
  - HIPAA Survival Guide
  - HITECH Act
  - CDC Disaster Preparedness and Business Continuity Worksheet
Electronic Health Record Step 6: Continue Quality Improvement
This final phase refers to reassessing what you have learned from training and everyday use of the system. It emphasizes continuous evaluation of your clinic’s goals and needs post EHR implementation to continue improving workflows that achieve the individual practice’s goals and needs while leveraging the functionality of electronic health records (EHRs).

With the EHR system in place, it is recommended that your organization have a business continuity implementation plan that includes the following elements:

- Test the business continuity plan with drills and exercises on an bi-annual basis
  - Plan on alternating between tabletop (discussion-based) exercises and functional (operational-based) exercises every 6 months
- Write an after action report (AAR) and improvement plan (IP) that captures the lessons learned from the drills that seek to improve plan
- Implement the improvement plan recommendations (drill and/or actual disaster lessons learned) into the plan update
- Update your business continuity plan on an annual basis or when you make a significant business process changes like adding practice sites

Community Clinic Business Continuity- EHR Tools
- Appendix J: Exercise Planning Checklist- This tool provide guidance to clinics on how to plan for a tabletop exercise.

Public Domain Business Continuity – EHR Reference and Resource Documents
- Hospital Continuity Program Checklist- This checklist is intended to provide hospitals with guidance on Hospital Continuity Program components.
- Business Continuity Planning Tabletop Exercise White Paper
- Guide to Developing and Conducting Business Continuity Exercises
- BCP Test – Situation Manual scenarios in it for testing plan
- NJPCA – Cyber Attack - New Jersey PCA – Cyber Attack After Action Report
- After Action Report/Improvement Plan for Real Incidents Template
Patient Centered Medical Home and Business Continuity Crosswalk

The patient centered medical home is a care delivery model designed to improve quality of care through enhanced access, planning, management, and monitoring of care. The HRSA Patient Centered Medical Home Initiative (PCMH) encourages health centers to undertake and document the practice changes that will enable them to gain recognition from National Committee for Quality Assurance (NCQA) through their Patient-Centered Medical Home (PCMH) program. To promote quality improvement, the PCMH Initiative provides access to survey-related education, training, and technical assistance resources that highlight the benefits of seeking recognition and common barriers to success.

Each of the NCQA PCMH standards also has elements of emergency management and business continuity planning considerations.

PCMH Standard #1- To enhance access and continuity:

- **BCP Planning Consideration**: When developing after hours policies for this step, develop an incident command system to manage the patients needs outside of normal business hours

- **BCP Planning Consideration**: One of the Must Pass Standards is “Access During Office Hours” – when CHC develop a business continuity plan to continue to treat patients in an alternate way despite a business interruption of disaster, it can help you accomplish this

PCMH Standard #2- Identify and Manage Patient Populations: Collect and use data for population management

- **BCP Planning Consideration**: Develop an alternate business process to revert to paper patient record tracking in case your electronic health record systems (EHRs) are not accessible after internal or external disaster
  - Alternate business process also should include a process to move from paper tracking back to your EHR system

- **BCP Planning Consideration**: Determine the core data fields needed to be collected so that you can complete billing for reimbursement after disaster
  - After Hurricane Katrina in 2004, millions of care provided by went uncompensated for years because of the lack of patient data needed to bill-
    CMS Hurricane Katrina Provider Reimbursement Article
PCMH Standard #3- Plan and Manage Care: Use evidence-based guidelines for preventive, acute and chronic care management, including medication management

- **BCP Planning Consideration**: Consider creating an emergency supply cache of medical (crash cart, bandages, suture supplies, PPE) and non-medical supplies (water, food, blankets, duct tape, flashlights) so that you can respond to your patients’ needs after disaster

- **BCP Planning Consideration**: If applicable, consider developing a pharmaceutical cache so that medications are available to your patients—especially those with chronic conditions. After a major disaster, supply chains slow down making Rx access difficult

- **BCP Planning Consideration**: Partner with humanitarian organizations like Direct Relief and AmeriCares to access Rx after disaster

PCMH Standard #4- Provide Self-Care Support and Community Resources: Assist patients and their families in self-care management with information, tools and resources

- **BCP Planning Consideration**: Develop a preparedness plan that encourages your staff and patients to prepare for disaster by developing a go-kit, a family communication plan, etc.

- **BCP Planning Consideration**: Ensure that disaster mental health resources are available your staff and patients

PCMH Standard #5- Track and Coordinate Care: Track and coordinate tests, referrals and transitions of care

- **BCP Planning Consideration**: Any medical surge capacity planning can be coordinated with meeting this consideration. Develop policies such as a referral process to alternate levels of care (hospitals, long term care if needed), coordination with emergency medical services (EMS), and determine if additional patients can be served in the health center exam rooms after disaster

- **BCP Planning Consideration**: Determine a CHC alternate business process to share patient information with healthcare partners even if the Electronic Health Record may not be available after disaster
PCMH Standard #6: Measure and Improve Performance: Use performance and patient experience data for continuous quality improvement

- **BCP Planning Consideration:** Conduct drills and exercises to test emergency operations plans and business continuity plans
  
  - Write an after action report (AAR) and improvement plan (IP) to incorporate the lessons learned after the exercise into the updated plan emergency operations plans and business continuity plans
  
  - Write an AAR and IP after the CHC experiences an internal or external disaster

**Community Clinic Business Continuity- Patient Centered Medical Home- EHR Tool**

Appendix F- EHR -PCHM – Business Continuity Planning Crosswalk- This tool is intended to be used to determine the emergency management and business continuity planning gaps and overlap of both PCMH and BCP standards and planning elements.

**Public Domain Business Continuity – PCMH Reference and Resource Documents**

- [HRSA Patient Centered Medical Home Initiative](#)
- [CPCA Patient Centered Health Home Resources](#)
Alternate Care Site (ACS): A location where patient care can resume in the event of an interruption or disaster. In California there are “Government Authorized ACS’s” as defined in Volume II: Government- Authorized Alternate Care Sites of the CDPH’s Healthcare Surge Standards and Guidelines (2006). Though the manual was developed primarily for hospitals, other healthcare providers (such as CHC’s and Long Term Care Facilities) were increasingly recognized as being integral to any successful surge response, and encouraged to use the Standards and Guidelines. A Government- Authorized ACS provides guidance as well as legal waivers that could be signed by the Governor in the event of a surge incident. It includes specific guidance and general planning considerations for coordinating site locations, developing staffing models, defining standards of care & developing administrative protocols and also provides guidance on obtaining reimbursement at these sites from the state and federal governments.

Building (or Facility) denial: Any damage, failure or other condition, which causes denial of access to the building or the working area within the building, e.g. fire, flood, contamination, loss of services, air conditioning failure, forensics.

Business Continuity Plan: Please see the Toolkit document entitled Business Continuity Planning Overview and Key Concepts

Business impact analysis (BIA): A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resources loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

Business Impact Assessment (BIA): Ask the following questions: How bad can things get? What are the most important resources, systems, outputs, and dependencies by business function? What impact does unavailability have?

Business Recovery Coordinator: Activates Business Continuity Plan, Disaster Recovery Plans and/or Emergency Preparedness Plans and works with administration, advisory committees, and Recovery Teams to allocate resources and coordinate implementation of the Recovery Plans. Serves as the primary contact and coordinates the recovery effort. Insures that status of the recovery effort is communicated to the appropriate levels of the organization. Insures that an After Action Report (AAR) is conducted and that and Improvement Plan are incorporated into the Business Continuity Plan.
Clinic Site: This term refers to individual clinics in their geographical location, specifically the actual clinic facility. A clinic may belong to a group (in this sense, not referring to the clinic association), an umbrella company or parent company with the same name, but each location with a facility or mobile van is called a clinic site. *Example:* Family Health Care Centers of Greater Los Angeles operates multiple clinic sites. One of their clinic sites is called Bell Gardens Family Medical Center, and another clinic sites belonging to FHCCGLLA is the Downey Family Medical Center.

Cold Site: One of three types of back-up sites (hot, warm, and cold) for Business Continuity function during an event, it is a back-up site is considered to be one of the main pillars of Business Continuity Planning—the pillars being (1) vital data access, (2) staffing, and (3) the facility itself. This addresses the issue of “un-usability” of the community health center and is not necessarily co-located with the Alternate Care Site. Any of the three back-up sites can be another location operated by the clinic organization, or contracted by a company specializing in disaster recovery services. It is possible for multiple organizations to agree to operate a joint back-up site. Specifically, a cold site is the least expensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster. The availability and access to hardware and software during an event (anticipated to be low), as well as the time and possibly additional personnel needed to set it up, may make this a low-value option for community health centers.

Critical (or Essential) Business Functions: Those functions considered essential to the ongoing operation of the organization or business unit. Critical functions also include anything that might adversely impact service delivery or significantly impair the administrative or financial integrity of the organization.

Disaster Recovery Planning (DRP): Typically, the technology aspects of a business continuity plan, to recover information system resources to full or partial production processing levels in the event of an extended power disruption or data line damage. Normally, information system resources will be restored according to a priority indicated by what is “mission critical” to the organization.

Disclosure of sensitive information: This is a serious information security incident, which can result in severe embarrassment, financial loss, and even litigation where damage has been caused to someone’s (generally an employee or patient—someone the community health center has data files on) reputation or financial standing. This includes HIPPA/protected health information violations. Further types of serious
disclosure involve secret patent information, plans and strategic directions, research, information disclosed to legal representatives etc. Deliberate unauthorized disclosure of sensitive information is also referred to as sabotage (external source)/espionage (internal source). As intimated above, this could occur accidentally, as a result of a natural or manmade incident, or it could occur as the result of a deliberate attack on patient data files. Whether the CHC employs Electronic Medical Records or uses paper records, at a minimum the HIPPA information must be protected through multiple security redundancies. (Illustrative scenario—an individual decides to break the law and hack into or physically break into patient records in an attempt to steal identities. Protected health information is compromised through this hack or physical break-in. Your job is to recognize this and other potential scenarios, and take steps to mitigate the risk, and prepare for it, writing your response plan, exercising it. This is a very serious direct threat to your CHC’s business reputation and finances.)

Equipment Failure (excluding IT hardware): Community Health Centers may rely on a whole range of different types of equipment in order to run their essential business processes. It may be possible to move to alternate processes to enable clinic functions to continue, but it will require considerable planning and preparation, starting with the identification of all pieces of equipment necessary for essential business functions.

**Hazard and Vulnerability Analysis (HVA):** An analysis of your CHC’s vulnerability to particular hazards provides the foundation for many activities, including Business Continuity Planning. The HVA identifies the hazards and/or vulnerabilities that need special attention, the actions that might be taken to reduce the impact of those hazards, and what resources are likely to be needed. Your CHC most likely completed an HVA prior to the development of its Emergency Operations Plan, which you can review, update and use to help guide all-hazards Business Continuity Planning.

**Hot Site:** See earlier general explanation of a back-up site under “Cold Site;” however, a hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organization’s requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organizations
that operate real time processes such as financial institutions, government agencies and eCommerce providers.

Impact: Impact is the cost to the enterprise, which may or may not be measured in purely financial terms.

Information Security: The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.

Internal arrangement: Other rooms within the organization could be equipped to support business functions (i.e., training rooms, cafeterias, conference rooms, etc).

Internal power failure: A type of incident (like a fire, flood or earthquake) singled out here only because it relates to another Business Continuity worksheet on Vital Records.* An internal power failure is an interruption to the electrical power services caused through internal equipment or cabling failure. This type of fault will need to be repaired by a qualified electrician and delays will inevitably impact the business process. Where particularly serious faults have occurred, such as damage to main cables, the repairs could take some time and could have a severe effect on the business.

IT system failure: As CHCs migrate more and more data onto IT systems (including EMRs), a failure to these systems can be particularly devastating. The types of threats to computer systems are many and varied, including hardware failure, damage to cables, water leaks and fires, air conditioning system failures, network failures, application system failures, telecommunications equipment failures etc. Reliable vendors of EMR systems should always have a plan in place and operational at your CHC for data back-up and recovery (usually either to a cloud or one or more sites well outside any potential disaster zone for your clinic). Other vendors that you may contract to for payroll or billing must also be questioned about their data back-up systems as part of your Business Continuity Plan.

Off-site location: A storage facility at a safe distance from the primary facility, which is used for housing recovery, supplies, equipment, vital records etc.

Operational Impact: An impact, which is not quantifiable in financial terms but its effects, may be among the most severe in determining the survival of an organization following a disaster.
Parent Clinic Network/Parent Clinic Organization: Many “Clinic Sites” (as defined above) may belong to a Parent organization or umbrella organization, and this should be taken into account when undertaking Business Continuity Planning. A CHC may be very small and operate all of its clinic and business office functions out of only one clinic site, but for all other CHCs, consider how your normal business operations are interconnected throughout your network (do you have/plan to get one EMR system for your Clinic Network? Do you have one or more pharmacy/dispensary sites at your clinics that other clinics in your network rely on? Is there a “business office site” either at one of the clinic sites or at its own address that handles data such as payroll, facility and provider insurance, vendor agreements and any other vital records for the Clinic Network?) Once you can map out how critical business functions are handled throughout your Clinic Network, you can strengthen and provided backup critical business functions. If your CHC belongs to a Parent Clinic Network, it may also help you more easily with staff-sharing, facility-sharing, equipment-sharing and other activities that your CHC may decided to engage in during an event to keep vital business operations going.

Reciprocal arrangement (CHCs may use MOUs, or Memoranda of Understanding, to accomplish the same thing): An agreement in which two parties agree to allow the other to use their personnel, resources or facilities during a disaster, to the degree possible.

**Recovery Point Objective (RPO):** It is the acceptable level of data loss expressed in time, usually since the last backup. This is defined by the data content owner of an IT application.

**Recovery Time Objective (RTO):** It is the time from disaster declaration to the restoration of the application. This is defined by the data content owner for an IT application.

Resumption (of care): The process of resuming critical business operations (i.e. treating patients) quickly following an interruption or disaster.

Site access denial: Any disturbance or activity within the area surrounding the clinic site which renders the site unavailable, e.g. fire, flood, riot, strike, loss of services, forensics. The site itself may be undamaged.

System Recovery: The procedures for rebuilding a computer system to the condition where it is ready to accept data and applications. System recovery depends on having access to suitable hardware.
*Vital Records: One of the most critical concepts to understand and act upon. Vital Records are all data and information required to support essential business functions, including patient medical records—paper or EMR. Vital Records include historical, regulatory requirements including, but not limited to, policy and procedures manuals, input documents or data, manuals for software and other applications, payroll, facility and provider insurance, vendor agreements. For CHCs belonging to a Parent Clinic Network (i.e. having more than one “Clinic Site”), some vital records may be maintained at a “business office site” for the clinic group—what records must be maintained (such as timesheets, etc.) by each clinic site during an incident v.s. what vital records will be maintained and communicated by the central business office, if applicable? Additionally, these records should be maintained off-site (and out of the likely geographical area for likely incidences as defined in your HVA) at a third party vendor, or through use of cloud data storage, with hard copies of as many vital records as possible at the Parent Clinic Network command center/Clinic Site command center. *See Worksheet: Vital Records for CHCs

Warm Site: See earlier general explanation of a back-up site under “Cold Site.” A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

Developed by Healthcare Readiness at Anderson Consultation through industry knowledge of California CHCs.
Additional Sources: University of Texas Medical Branch at Galveston. Emergency Operations: BCP; CDPH Standards and Guidelines
List of Appendices

Appendix A- BCP Hazard Vulnerability Assessment Tool
Appendix B- Clinic Disaster Prep and Business Continuity Worksheet
Appendix C- Clinic BCP Planning Tool
Appendix D- How to Conduct a Business Impact Analysis Step Process
Appendix E- EHR Vendor Selection Business Continuity Planning Checklist
Appendix F- EHR -PCHM -Business Continuity Planning Crosswalk
Appendix G- Disaster Mitigation Strategies
Appendix H- HIPPA Guidance on Disaster Recovery Planning
Appendix I- Clinic Vital Records Worksheet
Appendix J- Exercise Planning Checklist
Appendix A: BCP-Hazard Vulnerability Assessment Tool- see attached

This document is a sample Hazard Vulnerability Analysis tool. It is not a substitute for a comprehensive emergency preparedness program. Individuals or organizations using this tool are solely responsible for any hazard assessment and compliance with applicable laws and regulations.

INSTRUCTIONS:
Evaluate potential for event and response among the following categories using the hazard specific scale. Assume each event incident occurs at the worst possible time (e.g., during peak patient loads).

Please note specific score criteria on each worksheet to ensure accurate recording.

**Issues to consider for probability** include, but are not limited to:
1. Known risk
2. Historical data
3. Manufacturer/vendor statistics

**Issues to consider for response** include, but are not limited to:
1. Time to marshal an on-scene response
2. Scope of response capability
3. Historical evaluation of response success

**Issues to consider for human impact** include, but are not limited to:
1. Potential for staff death or injury
2. Potential for patient death or injury

**Issues to consider for property impact** include, but are not limited to:
1. Cost to replace
2. Cost to set up temporary replacement
3. Cost to repair
4. Time to recover

**Issues to consider for business impact** include, but are not limited to:
1. Business interruption
2. Employees unable to report to work
3. Customers unable to reach facility
4. Company in violation of contractual agreements
5. Imposition of fines and penalties or legal costs
6. Interruption of critical supplies
7. Interruption of product distribution
8. Reputation and public image
9. Financial impact/burden

Issues to consider for **preparedness** include, but are not limited to:
1. Status of current plans
2. Frequency of drills
3. Training status
4. Insurance
5. Availability of alternate sources for critical supplies/services

Issues to consider for **internal resources** include, but are not limited to:
1. Types of supplies on hand/will they meet need?
2. Volume of supplies on hand/will they meet need?
3. Staff availability
4. Coordination with MOB’s
5. Availability of back-up systems
6. Internal resources ability to withstand disasters/survivability

Issues to consider for **external resources** include, but are not limited to:
1. Types of agreements with community agencies/drills?
2. Coordination with local and state agencies
3. Coordination with proximal health care facilities
4. Coordination with treatment specific facilities
5. Community resources

Complete all worksheets including Natural, Technological, Human and Hazmat. The summary section will automatically provide your specific and overall relative threat.
Appendix B- Clinic Disaster Preparedness and Business Continuity Worksheet

Disaster Preparedness and Business Continuity Worksheet


(Further adapted from University of Texas Health Science Center at Houston by Healthcare Readiness at Anderson Consultation in California)

---

Introductory Business Continuity Overview Assessment to be Completed and Updated (Monthly Updates are Recommended Depending on Staff Turnover, and Updates are Unlikely to Take Long)

IMPORTANT: UNDERSTANDING THE PURPOSE—This introductory assessment Is meant to provide a venue for clinics to keep important contact information updated, identify areas of excellence in planning, and assist clinics in considering areas where in-services, individual or small group training, or information gathering is beneficial for the clinic’s Business Continuity plan.

Instructions: It is recommended to have the Nurse Manager READ through this brief survey (about 10 minutes).

Then he or she may designate (if desired) the individual(s) best suited to initially complete the survey. Recommendation: an individual with a good overall knowledge of clinic operations should shorten the length of time taken to complete the assessment, or select individuals could complete designated portions of the assessment. Where “No” answers are indicated when “Yes” is the optimal answer, names of those answering “No” should be noted solely for the purpose of training and education.

The task of updating the assessment at a regular interval—depending on clinic turnover—may then be turned over to clerical staff or whomever the Nurse Manager considers best suited to the task. Unless staff turnover is high and/or contact information changes frequently, this should not take much time. Again, where “No” answers are indicated when “Yes” is the optimal answer, names of those answering “No” should be noted solely for the purpose of training and education.
CLINIC DESCRIPTION

Name of Clinic: ____________________________
Name of Clinic Organization (if Applicable): ______________________________
Address: _________________________  _________________________, CA
Name of the Medical Director and Nurse Manager for clinic addressed in this plan:

______________________________                    _______________________________________

Name of person completing this worksheet : ______________________________   Phone number:

________________
Date completed: ______________

BASIC COMMUNICATIONS

Provide the various ways that subordinates can use to contact the Medical Director

<table>
<thead>
<tr>
<th>Name</th>
<th>Office Number</th>
<th>Home Number</th>
<th>Cell Phone</th>
<th>Pager</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Provide the various ways that subordinates can use to contact the Nurse Manager

<table>
<thead>
<tr>
<th>Name</th>
<th>Office Number</th>
<th>Home Number</th>
<th>Cell Phone</th>
<th>Pager</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Provide the various means that can be used to contact clinical and administrative personnel

<table>
<thead>
<tr>
<th>Name</th>
<th>Office Number</th>
<th>Home Number</th>
<th>Cell Phone</th>
<th>Pager</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Has all staff been made aware of the process by which information about this clinic site’s status in an emergent situation will be communicated?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Has all staff been made aware of the importance of being prepared at home with an “all hazards” home preparedness kit? (Access www.ready.gov for suggest kit contents)

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Does a written call-back procedure plan exist?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Have ALL staff been made aware of the call-back procedure, not only in written form, but through an in-service?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>
### BASIC RISK AWARENESS

Are the appropriate management staff aware of key details regarding the property insurance of clinic building(s), equipment, etc. including the deductible and any key exclusions to coverage that may apply?  

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Are the appropriate management staff aware that supplemental insurance can be purchased for specific pieces of equipment that may be critical to operations?  

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Are the appropriate management staff aware that supplemental insurance can sometimes be purchased for specific events not covered in the basic policy (such as flooding)?  

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Are all staff aware that personal property is not covered by clinic property insurance?  

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Are any clinic activities carried out in leased space?  

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

If yes, verify emergency support measures provided by landlord and attach to this document.

---

**Names and Initials of Management Staff Signing off that they have Basic Risk Awareness as outlined above:**

____________________________________  _____________  

____________________________________  _____________  

____________________________________  _____________  

____________________________________  ______________  

---

**PROTECTION OF EQUIPMENT AND CRITICAL MATERIALS**
<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are critical pieces of equipment protected from risks such as theft, water leaks, and/or electrical surges/outages?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is temperature or time sensitive equipment equipped with failure alarms?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there an after hours and on weekends alarm monitoring process?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If yes, who monitors and how?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the basic security measures employed are not sufficient to halt malicious acts (e.g. forced entry into office or lab and theft of laptop or equipment) has consideration been given to how information or data might be recovered if lost, such as daily data uploads and back ups?

Name the individual(s) that have overseen the basic security measures and deemed them insufficient and have them initial by their name. (Suggest a workgroup including. Attach a sheet to this Worksheet Entitled “List of Concern About Insufficient Security Measures & Suggested Improvements and Revisions”

______________________________

______________________________

______________________________

______________________________

PROTECTION OF DATA AND SPECIMENS
<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does this clinic use Electronic Health Records exclusively?</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Does clinic use Electronic Health Records partially (moving over to EHR system; adopting a limited EHR/Health Information Technology system, etc)?</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Is clinic part of a larger clinic network (i.e. all local Planned Parenthood)?</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Is clinic data saved on a cloud or off-site servers so that it is protected by emergency back ups?</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>If the clinic belongs to a network, is the data stored in a tertiary location (cloud or server off-site from all local network clinics)?</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Is any information (data or documents) stored on laptops routinely saved to network drives? Circle one if “yes”:</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Secondary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tertiary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For any information retained locally, does any mechanism exist for its protection or recovery?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Are any critical specimens that require freezer storage on emergency power supplies?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Are all critical freezers equipped with an audible alarm if the unit loses power or compressor malfunctions? Yes  No  N/A

Have any subsets of samples been stored in a separate location to afford recovery if power is lost or a freezer malfunctions? Yes  No  N/A

If so where are they located?

## PROCUREMENT OF KEY SUPPLIES

Enter the name and contact information of the primary and two back up individuals who are able and authorized to make purchases for necessary supplies in the event of an emergency.

<table>
<thead>
<tr>
<th>Name</th>
<th>Office number</th>
<th>Home number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enter the names and contact numbers for suppliers of key resources, such as dry ice, medications (if clinic has a pharmacy/dispensary). Include existing contracts for emergency provisions. Also include information on a back up supplies.
If access to your clinic were restricted or prohibited for some period of time due to an emergency, indicate which options might be possible to continue operations:

- ( ) remote access of computer data files and work from home or off-site
- ( ) access to patient information for the purposes for informing patients and rescheduling appointments
- ( ) work in like-facility/community clinic until recovery is achieved
- ( ) other – briefly describe:

### AVAILABILITY OF PEER-TO-PEER SUPPORT IN EVENT OF LOSS

Provide the name, location and contact information of a local like-facility that might be willing and able to assist in clinic continuity if an emergency occurs. Also include the contact information for a like-facility outside the Los Angeles area.

<table>
<thead>
<tr>
<th>Local like-facility/community clinic contact person(s) name(s)</th>
<th>Name of like-facility</th>
<th>Contact number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ASSET DOCUMENTATION AND INSURANCE RECOVERY

Indicate the type of documentation that exists that could be used to facilitate any possible insurance claims in the event of a loss:

- [ ] receipts
- [ ] inventories
- [ ] means for tracking loss of business income
- [ ] dated photographs or videotapes

Indicate the location of any documents checked: ____________________________________________

### OTHER SPECIAL CONSIDERATIONS

Please include in the space below any other information that may be useful to facilitate continuity of activities in the event of an emergency. Attach additional sheets if necessary.

<table>
<thead>
<tr>
<th>Out of affected region like-facility contact people’s names</th>
<th>Name/location of like-facility</th>
<th>Contact number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix C: Clinic Business Continuity Plan: Electronic Health Record Planning Tool

Table of Contents

Business Continuity Plan (BCP) – Electronic Health Record (EHR) 45
Plan Objectives 45
Assumptions 45
Disaster and Adverse Events 46
Key Roles and Responsibilities 47
Disaster Declaration 49
Notification 49
Adverse Event Response 50
  Unplanned Loss of Access to EHR 50
  Short-Term Loss of Access to EHR 50
  Long-Term Loss of Access to EHR 51
  Loss of Facilities 51
BCP Contact List 52
# Emergency Notification Contacts – Primary

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Address</th>
<th>Home Phone</th>
<th>Mobile/Cell Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan (BCP) Coordinator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(EHR Vendor Name)</em> Business Continuity Plan (BCP) Coordinator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinic <em>(EHR Vendor Name)</em> Liaison</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinic Communications Coordinator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinic Administrative Staff:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Nursing Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Operations Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

# Emergency Notification Contacts – Backups (in case primary is unavailable)

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Address</th>
<th>Home Phone</th>
<th>Mobile/Cell Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan (BCP) Coordinator - Alternate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(EHR Vendor Name) Business Continuity Plan (BCP) Coordinator - Alternate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinic (EHR Vendor Name) Liaison - Alternate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinic Communications Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinic Administrative Staff:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Executive Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Business Continuity Plan

This Business Continuity Plan (BCP) – Electronic Health Record (EHR) will assist (clinic name) in planning for immediate and long-term response to adverse events and disasters by outlining the actions necessary to ensure continuance of patient care and business operations.

Immediate response to adverse events and disasters may prevent loss of life and minimize injury to people and damage to property. Long-term response takes over after there is no threat to life or property.

This BCP-EHR will work to assure the long-term survival of the organization and will develop an organized responses to:

- Loss of the use of facilities such as an office or building.
- Inaccessibility of information and data (for clinics this relates specifically to medical records, schedules and billing).
- Unavailability of staff.
- Loss of medical equipment.
- Loss of technical resources such as hardware, software, Internet services and communication services. Anything else that may prevent normal operations or interfere with patient care and safety.

This plan is limited to major interruptions of service as outlined above where the ability to deal with and treat patients is curtailed for more than a one or two-hour timeframe.

Plan Objectives

The BCP:

- Serves as a guide for recovery.
- Identifies temporary business activities required during interruptions.
- Identifies procedures and resources needed to assist in recovery.
- Identifies vendors, patients and other parties that must be notified in the event of a disaster.
- Assists in avoiding confusion that can be experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval vital records.

Assumptions

The BCP is based upon the following assumptions:

- Key people will be available following a disaster.
- Broad scale disasters such as widespread flooding are beyond the scope of this plan.
This plan relates only to disasters affecting the clinic and its immediate environs. This document and all vital records are stored in a secure off-site location and are not impacted by the disaster. This plan will be accessible immediately in the event of a disaster. Each support organization, including the electronic medical record (EMR) vendor, will have its own plan consisting of appropriate recovery procedures and critical resource information.

Disaster and Adverse Event/Incident Definition

Disasters and adverse events are defined as any loss of utility service (power, water), connectivity (system sites) or catastrophic event (weather, natural disaster, vandalism, EMR service outage) that causes an interruption to the service provided by the clinic. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

Adverse Event Examples

BCPs address specific adverse events that pose a threat to a clinic and should consider and address possible threats whether man-made or natural, and the probability of those threats occurring. Threats and overall plans should be reviewed and evaluated annually.

Threats include situations such as:

- Fire
- Flood
- Internal contamination (clinic or full building)
- Nearby contamination affecting access (train derailment, gas station leak, tanker truck accident) Infectious disease
- Theft
- Vandalism (internal and external)
- Extreme weather Loss of power Loss of telecommunications (Internet and/or phone)
- Temporary or permanent loss of key staff member(s)
- Denial of service (DNS) attack, malware infestation in clinic or data center
- Loss of data center (and access to the clinic data), destruction of data at data center
- Widespread data corruption
- EMR vendor or other vendor failure (goes out of business suddenly)

This list is not definitive. If other threats are a risk, they should be addressed by the BCP.

Outcomes of these threats may include:

- Loss of access to the clinic or building (temporarily or permanently).
- Loss of computer and or medical equipment.
- Loss of paper records or access to paper records.
- Loss of availability to electronic medical records including scheduling, billing, patient charts.
- Loss of specific knowledge regarding patients and or processes not documented by unavailable staff members.
- Temporary or complete loss of business.
- Loss to third parties of patient data (privacy breach).

**Key Roles and Responsibilities**

When developing a BCP, specific roles and responsibilities need to be assigned.

The Clinic BCP Coordinator, the *(EHR Vendor Name)* BCP Coordinator, the Clinic *(EHR Vendor Name)* Liaison and the Clinic Communications Coordinator should have an identified alternate in case of non-availability.

**Clinic BCP Coordinator**
The clinic BCP coordinator is a role undertaken by a designated lead physician or clinic manager, with a clearly identified backup in case the lead is unavailable or indisposed.

The clinic BCP coordinator must:
- Determine how threats can be eliminated or mitigated.
- Develop plans to recover from damage caused by specific threats.
- Initiate and conduct periodic tests of the plan (once per year at a minimum).
- Hold the master copy of the plan and coordinate all updates.
- Retain an offsite copy of the BCP.
- Review and update the BCP on an annual basis.
- Initiate the execution of the BCP and coordinate its implementation when an adverse event occurs.
- Train staff so they can fulfil their role(s) in the plan when it is implemented.
- Collect vital contact information for staff, EHR vendor, suppliers, and insurance and restoration companies.
- Approve expenses such as new purchases, payroll and ongoing expenses.
- Accept overall responsibility for re-establishing normal operations.

It is the Clinic BCP Coordinator’s responsibility to plan and execute recovery from the specific threats based on how quickly management decides the clinic needs to recover and what they are willing to spend on recovery planning and processes.

The Clinic BCP Coordinator should consider the following:
1. The impact on business operations
   - Patient care
   - Patient safety
• How quickly the clinic needs to recover before complete loss of business
• How much loss can be tolerated
• How long the clinic can survive if a critical person is unavailable or only partially available
• Banking, payroll, other business functions

2. The resources that have been compromised
• Staff required (at a minimum) to operate the clinic
• Required computer and medical equipment
• If new identification badges (fobs) are necessary
• Required communication systems
• Alternate banking services
• Alternative billing processes

3. Damage mitigation actions to consider
• Reducing hours of operation
• Using temporary employees or staff from other clinics
• Referring patients elsewhere
• Determining alternative methods for notifying staff and patients of disruption or closure
• Deciding who will enter or re-enter data once systems are available
• Determining the budget to develop the recovery strategy, what will be available following a significant event and how the funding will be accessed during recovery
• Securing back-up facilities that might be used; can arrangements be made with another clinic or specialist?

Infectious disease requirements differ slightly from other scenarios but should be included in BCPs. Adequately addressing infectious disease requirements includes:
• Educating and training of staff.
• Developing a triage system for diagnosis and treatment.
• Coordinating with health authorities.
• Planning for recovery of practice.

(EHR Vendor Name) BCP Coordinator
The (EHR Vendor Name) BCP Coordinator works with the clinic to re-establish access to the EHR and patient data, both in the short-term during immediate recovery and long-term should the physical clinic environment need to be re-established.

The (EHR Vendor Name) BCP Coordinator:
• Obtains new equipment for the clinic.
• Facilitates reconnection to the Internet and the vendor data center.
• Facilitates data recovery if required.
• Assists with establishment of temporary facilities if required.
Facilitates EMR setup in the clinic including re-establishing roles and permissions, configuration and resetting preferences.

Tests the environment before implementation.

In the event that the (EHR Vendor Name) BCP Coordinator cannot be reached or is unable to respond to a failure or outage, the Clinic BCP Coordinator should contact their Alternate (EHR Vendor Name) BCP Coordinator or other identified entity (IT Management Company/Vendor). Working with the Clinic, the Alternate (EHR Vendor Name) BCP Coordinator will attempt to establish appropriate lines of communication with the EMR vendor, inform them of the situation and request their immediate assistance.

If the outage is the result of the failure of the (EHR Vendor Name)’s business, the (EHR Vendor Name) BCP Coordinator will work with the clinic to:

- Immediately gain access to the clinic’s data from the (EHR vendor)’s data center.
- Obtain a current copy of the backup system to allow the clinic to continue (limited) operations.
- If this is not possible, obtain a copy of the (EHR Vendor Name)’s software from the data center or from escrow to be used in the interim by the clinic.
- Pursue all contractual and legal avenues to restart services and determine how these services can be supported in the short term.
- Work with the clinic on a transition plan to move to an alternative service provider.

All processes and activities required to address this scenario should be documented as addendums to the BCP.

**Clinic EHR Liaison**

It is beneficial to appoint a clinic representative who can act as the primary liaison with the (EHR Vendor Name) in support of the Clinic BCP Coordinator. Operationally, the Clinic EHR Liaison:

- Retains an offsite copy of the BCP.
- Provides access to facilities for the EMR provider.
- Works with the vendor during EMR setup.
- Identifies training requirements for replacement personnel.
- Assists with pre-implementation testing.
- Assures verification of data recovery.

**Clinic Communications Coordinator**

The Clinic Communications Coordinator is the primary communications conduit for the clinic in support of the Clinic BCP Coordinator. The Clinic Communications Coordinator:

- Retains an offsite copy of the BCP.
- Maintains contact with staff.
- Initiates contact with the EMR vendor.
- Maintains contact with local, regional and state health authorities as required.
• Contacts the Office of Information and Privacy Commissioner (OIPC) if required.
• Contacts the media when necessary.
• Contacts patients.
• Contacts other vendors and suppliers.

**Disaster Declaration**
Senior clinic management and the Clinic BCP Coordinator are responsible for declaring a disaster to the various recovery personnel as outlined in the plan.

**Notification**
Regardless of the disaster circumstances or the identity of the person(s) first made aware of the disaster, the BCP must be activated immediately in the following cases:
- The EHR is or will be unavailable for *(list number)* or more hours.
- One or more complete facilities are or will be unavailable for *(list number)* or more hours.
- If any problem at any system and network facility occurs or exists that would cause either of the above conditions to be present.
- There is certain indication that either of the conditions are about to occur.

**Adverse Events Response**

**Unplanned Loss of Access to EHR**
Unplanned loss of access to EHR can be caused by local issues including power failure, and local network issues or issues with the EHR network.

1. In the event of loss of access or slow-running of EHR, clinicians are to inform *(the EHR Help Desk, the Clinic Manager, or Nursing Director)*.
2. On notification of loss of access to EHR, *(the EHR Help Desk, the Clinic Manager, or Nursing Director)* will contact *(EHR Vendor Name)* to determine how long service will be interrupted. Loss may be related to the data center, the connectivity to the data center or problems within the clinic.
3. *(the EHR Help Desk, the Clinic Manager, or Nursing Director)* will contact the Clinic BCP Coordinator of Loss of Access to EHR and status.
4. Agree on a communication plan with *(EHR Vendor Name)* to monitor progress to resolution.
5. If a limited local copy of the system is available, access and print patient schedules and chart summaries for the next three days.
6. If the outage will extend beyond *(number)* days, work with *(EHR Vendor Name)* to access data for the extended period of the outage.
7. Prepare or access temporary paper charts for use in patient consultations during the system outage.
8. Initiate the communications plan for notifying patients that:
   a. Scheduling services are limited.
   b. Appointments may be cancelled at short notice.
c. Any visits than can be delayed, for example annual physicals are being deferred.
d. Prescription renewal processes will change during the service interruption.
9. Initiate the communications plan for notifying EHR related partner health facilities, area health providers and others identified.
10. Mobilize staff to enter patient visit information that was gathered when the EHR system was unavailable into the electronic charts once the system is restored. This includes scanning the paper charts, attaching the scans to the electronic record and then destroying the paper charts.

Short-Term Planned Loss of Access to EHR
Short-Term Planned Loss of Access to EHR will be caused by planned maintenance or testing on EHR system. When planned, (the EHR Vendor) will contact the Clinic to coordinate Clinic operations to assure minimal loss in productivity.

1. Prepare or access temporary paper charts for use in patient consultations during the system outage.
2. Initiate the communications plan for notifying patients that:
   a. Scheduling services are limited.
   b. Appointments may be cancelled at short notice.
   c. Any visits than can be delayed, for example annual physicals are being deferred.
   d. Prescription renewal processes will change during the service interruption.
3. Initiate the communications plan for notifying EHR related partner health facilities, area health providers and others identified.
4. Mobilize staff to enter patient visit information that was gathered when the EHR system was unavailable into the electronic charts once the system is restored. This includes scanning the paper charts, attaching the scans to the electronic record and then destroying the paper charts.

Long-Term Planned Loss of Access to EHR
Long-term planned loss of access to EHR can be caused by major upgrades to the system.

1. Prepare or access temporary paper charts for use in patient consultations during the system outage.
2. Initiate the communications plan for notifying patients that:
   a. Scheduling services are limited.
   b. Appointments may be cancelled at short notice.
   c. Any visits than can be delayed, for example annual physicals are being deferred.
   d. Prescription renewal processes will change during the service interruption.
3. Initiate the communications plan for notifying EHR related partner health facilities, area health providers and others identified.
4. Mobilize staff to enter patient visit information that was gathered when the EHR system was unavailable into the electronic charts once the system is restored. This includes scanning the paper charts, attaching the scans to the electronic record and then destroying the paper charts.

Loss of Facilities

1. Contact *(EHR Vendor Name)* to access and print patient schedules and contact information for the expected duration of the facility loss.
2. Initiate the communications plan for notifying patients that:
   a. Non-urgent appointments are cancelled.
   b. Alternative arrangements are taking place (for example, home visits) if required.
   c. Prescription renewal processes are changed during the service interruption.
3. Initiate the communications plan for notifying EHR related partner health facilities, area health providers and others identified.
4. Prepare or access temporary paper patient charts for use in consultations during the system outage.
5. Initiate physical facility recovery plan. This may include:
   a. Sharing facilities with other clinics.
   b. Renting temporary or permanent replacement facilities.
   c. Bringing in portable facilities if feasible.
   d. Arranging for minimum equipment for the temporary facilities.
6. Work with the EMR vendor to commission the EMR in the new facility.
7. Mobilize staff to enter patient visit information that was gathered when the EMR solution was unavailable into the electronic charts once the system is restored. This includes scanning the paper charts, attaching the scans to the electronic record and then destroying the paper charts.
<table>
<thead>
<tr>
<th>Name/Contact</th>
<th>Business Phone</th>
<th>Home Phone</th>
<th>Cell Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>EHR Vendor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Service Provider (ISP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telecommunications Service Providers – Land, Cellular</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partner Health Care Organizations – Local, Regional, State, National (CPCA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(HRSA – Project Officer)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Contacts—Local, Regional (Newspapers, Radio, List Serve, Internet)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix D- How to Conduct a Business Impact Analysis Step Process

Business Continuity Planning (BCP) is a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption. A Business Impact Analysis (BIA) is the foundation for building successful BCP.

The Business Impact Analysis (BIA) is a detailed study of all the business processes within the organization, department by department. Each department’s processes are then analyzed to give the team a complete picture of health center critical (and non-critical) operations. There will be overlap, on occasion, from one process to another and this should be noted in the analysis.

It is both necessary and helpful to create directions on how to perform the different processes especially if they require specific steps. It is also important to understand any regulatory and legal requirements that apply to your specific health center such as processes that have to be maintained in a disaster or specific requirements to operate your health center at an alternate location.

A **Process** is a systematic series of activities that produce a specific outcome. Processes should be divided into two separate areas: Critical and Non-Critical:

1) **Critical Processes** are essential functions that are important to the mission of the organization and must be maintained during an emergency event (*Is it essential today to keep the business open?*). An example of a critical process is patient registration.

2) **Non-Critical Processes** play an important function to the organization but not essential during an emergency event to keep the business open. An example of a non-critical process is scheduling routine patient visits.

There are two things to consider when reviewing your Processes: **Time and Data:**

1) **Time** is analyzed to determine what the acceptable amount of downtime is before this function must be operational.
   
   a. **Recovery Time Objective** is the maximum time and minimum service level allowed to restore a process following a disruption. RTOs represent the maximum amount of time that a business function can continue to operate without vital resources. If a business were to exceed this time objective it might well sustain financial, regulatory, client service, public image or other irreparable damage.

2) **Data** analysis gives you what amount and type of data must be available so that you can still be open for business without severely impacting the business operations.
   
   a. **Recovery Point Objective** is the maximum period of time that data may be lost from an IT service due to a disruption

A plan should be create for each critical process to be maintained, within the limits of time and data identified.
Business Impact Analysis Template

**HEALTH CENTER NAME**

**Business Impact Analysis Form**

Department: __________________________________________________________

Business Process: ______________________________________________________

Type:  □ Critical Process  □ Non Critical Process

Priority:  □ High  □ Medium  □ Low

Description: __________________________________________________________

Number of Patients and/or Staff Affected: ________________________________

________________

Employee(s) in charge: ________________________________________________

________________

**Process Information**

Recovery Point Objective: Time: □ ___ Hours □ ___ Day(s) □ ___ Week(s) □ ___ Month(s)

Recovery Time Objective: Time: □ ___ Hours □ ___ Day(s) □ ___ Week(s) □ ___ Month(s)

Service level: _________________________________________________________

________________

Is this function a grant deliverable?    □ No □ Yes – Which grant(s)?

Is this function required by law/regulation? □ No □ Yes – Which governmental agency? _________

**Resources Required for Resumption and Recovery**

□ Personnel: __________________________________________________________

□ Vendor(s)/Outside Provider(s): _________________________________________

□ Key Contact(s): _____________________________________________________

□ IT hardware and software: ____________________________________________

□ Records (electronic or paper): _________________________________________

□ Medical equipment: _________________________________________________
Facility/office space: ____________________________

Plan for short-term (< 3 days) disruption:

Plan for long-term (> 3 days) disruption:
Business Impact Analysis Report Summary

Your organization should write a report, based on the findings of the Business Impact Analysis you have done within each department, which summarizes the key findings. It is advisable to share the report with the different departments to ensure accuracy.

The report will describe the critical processes within your organization and the equipment, tools and staff required to ensure these processes become live as soon after a disruption as possible to keep your business moving forward.

It is helpful to have a Business Impact Analysis Report Summary that will direct you on the critical information, staff, equipment and tools needed in a disruption. If an emergency occurs, this will be easier to utilize than reading through the report. The BIA Report Summary will list important criteria by groups, such as BC Team, Senior Leadership and Vendors contacts along with resources needed to operate the business. The summary can include:

- Business disruption events and measure probabilities
- Critical Business Processes and their priority level (e.g. low, medium, high)
- Critical computer resources that support key business functions
- Disruption impacts and allowable outage times
- Recovery priorities
- List the names and contact information of the Business Continuity Team
- List the names and contact information of the Senior Management Contacts
- Create a summary of Resources identified in the BIA process that are needed to continue doing business within the critical processes. This can include quantity, information on back-ups, location, ID#, etc.
- Create a list of contact information for Key Contacts, Vendors and Suppliers as well as back ups

<table>
<thead>
<tr>
<th>Business Impact Analysis Report Summary</th>
<th>Primary Workspace</th>
<th>Primary Systems &amp; Electronic Data</th>
<th>Key Personnel</th>
<th>Key Vendors and Services</th>
<th>Vital Records (Paper Files &amp; Mail)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible Scenarios</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electric Internal</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Con Ed failure</td>
<td>Y</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Back-up Generators failure</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Gas Leaks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Telecommunications Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure (Lan/Wan)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Loss of Vendor Service</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Voice Service</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Cellular Service</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Data Transmissions</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Router / Hub Failure / Firewall</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Overloaded : Performance failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Center Failure</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>Infrastructure damaged</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Mainframe failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Server failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Router failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>Hubs failure</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>Y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Water / Plumbing / Sprinkler Malfunction</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken Pipes</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td>Loss of Water Supply</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Flooding</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td>Drain Blockage</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Heating, Ventilation &amp; Air Conditioning Failure</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Cooling</td>
<td>Y</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Loss of Heating</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fire</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Arson</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td>Explosion</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>R</td>
</tr>
</tbody>
</table>

56
<table>
<thead>
<tr>
<th>Event</th>
<th>R</th>
<th>R</th>
<th>R</th>
<th>G</th>
<th>G</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightening</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smoke Damage</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Building Collapse</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td>Some (not all) floors damaged</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td>Access to building</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Physical Security compromised</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weather</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cold Weather</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Heat / Hot Weather</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Snow or Winter Storms</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>High Temperature / High Humidity</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Floods or Rain Storm Damage</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>High Winds</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Hurricanes</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Thunderstorm / Lightning</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Earthquake</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Hail Storm</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Tornado</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyberhacking (Internal and External)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Embezzlement</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>Sabotage</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td>Internal Hackers (Cybercrime)</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Firewall Compromised</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Capacity or Denial of service Attacks</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Data Theft or Destruction</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Unauthorized Activity</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>R</td>
<td></td>
</tr>
</tbody>
</table>

57
<table>
<thead>
<tr>
<th></th>
<th>G</th>
<th>R</th>
<th>G</th>
<th>R</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer Viruses</strong></td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td><strong>Trojan Horses</strong></td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td><strong>Application/ Systems Damage</strong></td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Terrorism</strong></th>
<th>G</th>
<th>R</th>
<th>G</th>
<th>R</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bombing</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>/ Bomb Threat</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>Bio-terrorism (ex. Anthrax)</strong></td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>Nuclear Attack</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>Hostage Situation</strong></td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td><strong>Cyberhacking</strong></td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td><strong>Espionage</strong></td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td><strong>Epidemic</strong></td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td><strong>Release of Toxins in Mail/Water/Air</strong></td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>Machine Explosion</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>Physical Plant Explosion</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td><strong>Injury/Illness/Death of key mgmt/personnel</strong></td>
<td>R</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Compromise of Physical Security</strong></th>
<th>G</th>
<th>R</th>
<th>G</th>
<th>G</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Break-ins</strong></td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td><strong>Theft / Vandalism</strong></td>
<td>R</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
</tr>
<tr>
<td><strong>Kidnapping</strong></td>
<td>G</td>
<td>G</td>
<td>R</td>
<td>G</td>
<td>G</td>
</tr>
</tbody>
</table>

| **Errors / Omissions**             | G | R | G | G | R |
| **Labor Strike / Dispute**         | G | R | G | G | R |

<p>| <strong>Taxi Strike</strong>                    | G | G | R | R | G |
| <strong>Police Action</strong>                  | R | G | R | R | G |
| <strong>Protestors/Riots/Civil</strong>         | R | G | R | R | G |</p>
<table>
<thead>
<tr>
<th>Disorder</th>
<th>R</th>
<th>G</th>
<th>R</th>
<th>R</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>War / Political Unrest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Vendor Loss**

<table>
<thead>
<tr>
<th>Temporary disruption of Service</th>
<th>G</th>
<th>G</th>
<th>G</th>
<th>R</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long term loss of vendor</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Vendor Bankruptcy</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>R</td>
<td>G</td>
</tr>
</tbody>
</table>

**Accident**

| Airplane Crash                  | R | R | R | R | R |
| Nuclear Disaster (ex. Indian Point) | R | R | R | R | R |
| Explosions                      | R | R | R | R | R |
| Hazardous Materials             | R | G | R | R | R |
| Toxic Contamination             | R | G | R | R | R |

**Transportation**

| Airport Closure                 | G | G | R | G | G |
| Bridge & Tunnel Closure         | G | G | R | G | G |
| NYC Lockdown                    | G | G | R | G | G |
| Subway System Shutdown          | G | G | R | G | G |
| Bus (Transit Strike)            | G | G | R | G | G |

| Floor Collapse                  | R | R | R | G | R |
| Roof/Ceiling Collapse           | R | R | R | G | R |

**KEY**

- **G**: Low Risk or N/A
- **Y**: Risk with Mitigation Control
- **R**: High Risk
Appendix E-EHR Vendor Selection Planning Checklist

This checklist is intended to be used during the Electronic Health Records vendor selection process to ask questions of the EHR vendor to ensure that they have a comprehensive business continuity plan in place that addresses data and communications infrastructure, an alternate facility plan, and an alternate staffing plan. The questions listed below highlight concepts that are standard emergency management and business continuity planning best practices.

General emergency management and business continuity questions

☐ Has the EHR vendor conducted a Hazard Vulnerability Assessment to determine their man-made and natural disaster risks and vulnerabilities?

☐ Does the EHR vendor have a comprehensive business continuity plan in place that addresses data, facility and staffing impacts?

☐ How often and how (tabletop exercise and/or functional exercise) is the EHR vendor’s business continuity plan exercised and updated?

☐ Has the EHR vendor had business interruptions in the past and what were the action steps to get their business operations reconstituted?

☐ Does the EHR vendor’s business continuity plan have Memorandums of Understanding (MOUs) with like organizations to support significant downtime of business operations?

☐ Does the EHR vendor have business interruption insurance?

☐ Does the EHR vendor have an incident command system (ICS) organization developed with staff identified with response roles?

Data and Communication Infrastructure

☐ What are the patient record data protection processes does the EHR vendor has in place?

☐ How does those process meet the HIPAA privacy standards in time of disaster?

☐ Has there been a previous data breach and what were the policies that were put in place to minimize future data breaches?

☐ Where and how does the EHR vendor have data back ups, i.e., alternate servers outside of immediate area, Cloud, etc.

☐ What is the EHR vendor’s technical assistance process to help you move from EHR to paper patient tracking and other viral records back to EHR after disaster?

☐ Is your EHR vendor listed as a vital priority resource for voice communication Government Emergency Telecommunications Service (GETS) and Wireless Priority Service for wireless communication?

☐ Does the EHR vendor have:

☐ Alternate Internet access procedures and equipment?

☐ Data backup processes?

☐ A generator or alternate power supply?
Redundant communication systems and/or equipment such as satellite phones, ham radios, push-to-talk radios, etc. to reach out to vendors, other businesses, partners, and customers?

**Facility**
- Does the EHR vendor have an alternate facility plan if the main building(s) are unavailable after disaster?
- Does the EHR vendor have a cache of emergency supplies and equipment to address the response and recovery operations?
- Does the EHR vendor have a plan that addresses policies and procedures to temporarily relocate to an alternate location?
- Does the EHR vendor have a plan and processes to relocate back to their building and reconstitute their business once recovery tasks are complete?
- Does the EHR vendor have policies in place to prioritize customers’ based upon their needs after disaster?

**Staffing**
- How many of the EHR vendor’s staff are cross-trained on the organization’s alternate back-up procedures?
- Does the EHR vendor have an Employee Assistance Program that addresses disaster mental health resources and support?
- Has the EHR vendor determined their critical business functions and which internal and external staff dependencies complete those business functions?
- Does the vendor have an alternate staffing plan in place to address interruptions in service?
- Is the staff trained on their emergency roles during response and recovery operations?
Appendix F- Electronic Medical Record - Patient Centered Medical Home Implementation Planning Crosswalk

<table>
<thead>
<tr>
<th>Electronic Health Record Step</th>
<th>PCMH Standard</th>
<th>Emergency Management and Business Continuity Planning Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Assess Your Practice Readiness</td>
<td>Standard #1- Enhance Access and Continuity</td>
<td>Hazard Vulnerability Assess</td>
</tr>
<tr>
<td>Step 2: Plan Your Approach</td>
<td>Standard #2- Identify and Manage Patient Populations</td>
<td></td>
</tr>
<tr>
<td>Step 3: Select and Certified EHR</td>
<td>Standard #3- Plan and Manage Care</td>
<td></td>
</tr>
<tr>
<td>Step 4: Conduct Training and Implement an EHR System</td>
<td>Standard #4- Provide Self-Care Support and Community Resources</td>
<td></td>
</tr>
<tr>
<td>Step 5: Achieve Meaningful Use</td>
<td>Standard #5- Track and Coordinate Care</td>
<td></td>
</tr>
<tr>
<td>Step 6: Continue Quality Improvement</td>
<td>Standard #6- Measure and Improve Performance</td>
<td></td>
</tr>
</tbody>
</table>

62
Appendix G: Disaster/Disruption Mitigation Strategies

The BCP Team should look at creating mitigation strategies and procedures, protection and backups for the Health Center, such as:

- Review EHR Vendor’s BCP and other documentation related to disaster planning;
- Develop redundant tele-connectivity to include DSL and satellite;
- Internal and external structure reinforced at the physical site
- Ensure fire detection and suppression systems are current and operable
- Develop back-up systems and procedures for computers and software

Develop mitigation strategies and procedures that support business processes of the Health Center:

- Procedures to incorporate appropriate inventory of critical equipment
- Maintain adequate supplies of water, non-perishable food items, batteries, medical supplies
- Develop offsite backup systems for data, critical software, and facilities
- Develop disruption alternatives for:
  - Power
  - Communications
  - Data and records, and recovery of information
  - Facility
  - Staffing
Appendix H: HIPAA Compliance Guidance Regarding Disaster Recovery Planning

Contingency planning is a HIPAA Security standard that establishes and implements, as needed, policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.

A HIPAA Disaster Recovery Plan is a document that specifies the resources, actions, personnel and data that are required to protect and reinstate healthcare information in the event of a fire, vandalism, natural disaster or system failure. The Disaster Recovery Plan is a required implementation, as defined within the HIPAA Contingency Plan standard in the Administrative Safeguards section of the HIPAA Security Rule that addresses how natural disasters could damage systems that contain electronic health information and develop policies and procedures for responding to such situations.

A HIPAA-compliant Disaster Recovery Plan must state:
- How operations will be conducted in an emergency and which workforce members are responsible for carrying out those operations;
- How data will be moved without violating HIPAA standards for privacy and security;
- How confidential data and safeguards for that data will be restored.

Although HIPAA doesn't specify exactly how to do accomplish the disaster recovery, it does note that failure to adequately recover from a disaster could lead to noncompliance which exposes officers of the organization to repercussions, such as fines or jail time.

The Security Rule applies to protected patient health information in electronic formats. This is protected patient information either transmitted by electronic media or maintained on electronic media. Covered entities that maintain or transmit protected health information are required by the Security Rule (see 45 C.F.R. §164.306) to:
- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- Ensure compliance with this subpart by its workforce.

According to the HIPAA regulations, Covered Entities are allowed to use a flexible approach when implementing the above requirements. Specifically, Covered Entities may use any security measures that allow the Covered Entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
With this information in mind, organizations must adhere to the Security Rule's standards and specifications for backing up and safekeeping electronic data. Covered Entities also need to institute a contingency plan to be prepared for an emergency, such as a natural disaster or computer virus attack that results in a major data loss. The Contingency Plan must include the following:

- Establish and implement, as needed, policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (Administrative Safeguards - §164.308(a)(7)(i)).
- Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
- Disaster recovery plan (Required). Establish and implement procedures to restore any loss of data.
- Emergency mode operation plan (Required). Establish and implement procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. Covered Entities must also have certain physical safeguards, such as facility access controls. They must:
  - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed (Physical Safeguards - §164.310(a)(1)).
  - The contingency operations should establish and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency (§164.310(a)(2)(i)).
Appendix I: Vital Records Worksheet

Vital Records are all data and information required to support essential business functions. This Worksheet was designed to help Community Health Centers identify their vital records and design systems to keep those records safe and appropriately saved and/or accessible (depending on the type of record) during an incident. Below is a graphic showing the different types of vital records that CHCs may have. Only you will be able to provide a comprehensive list of all such records, but this Worksheet provides a guide to the process of identifying and securing CHC vital records.

(1) Come up with a complete list of Vital Records. To facilitate thinking about each type of record that could be considered by your organization to be a Vital Record, use the graphic above. The list may be quite daunting, so use the described ranking system (or come up with your own ranking system) to categorize the list of vital records to make managing it much easier.

Decide which are the most important and time-sensitive records for which you must figure out a back-up access plan so they can be used and accessed before, during and after an incident (category red). An example of category red vital records may include things like facility insurance policies, and provider licensing records. For vital records that would normally fall into category red, but which require additional time/resources for 'planning use and access before, during and after an incident', use category orange. An example of category orange vital records may include records/systems for processing patient insurance/co-payments during an incident. Payroll records may belong to either category red or category orange, depending on how complex the payroll system is. Vital records which are important to the overall success of your CHC business, but which you can back-up to a remote server/cloud and do not need to access during an incident, should be placed in category yellow. A possible category yellow record example would be tax records.

If applicable, there may need to be a division of labor between a clinic site (and which vital records it is responsible for securing) and the parent clinic organization (and the records it must secure for its business office). Different clinic organizations may choose to tackle the challenge in different ways, but for category red and orange records, redundancy is usually the best policy.
(2) Periodically (or if you have notice of an incident such as a power outage resulting from a rolling blackout, or the predicted landfall of a large weather system), back-up and print out those category red/orange records as applicable.

(3) Medical Records: Electronic Medical Records (EMR) and Paper Medical Records. If you currently are using an EMR system, you should find out how the EMR is backed up and how protected data stays protected (not only during incidents such as disasters, but also during cyber-attacks). Medical Records are the most challenging aspect of your vital records to maintain, whether you use EMRs or paper records.

**Paper Patient Medical Records**: If you use paper records, located in one or possibly two locations, it is easy for them to be destroyed by incidents such as fire, flood, structure failure and exposure to the elements, smoke, etc. If your structure remains intact though, paper records will likely allow you to access recent patient history, treatment and prescription data for much of your CHC population. In other words, the primary emergency management downside to paper records is that they are very difficult to adequately back up, but the emergency management upside is that, barring structure failure, they can be the only way to have access to patient data in an incident (since most significant incidents include a loss of power). There are also issues regarding the security of paper medical records, particularly during an incident—this is another emergency management consideration to be taken into account if you have not yet switched to EMRs. Patient data are probably the vital records of greatest importance to the long-term recovery of CHCs, and the loss of records due to facility damage/destruction could potentially cause the failure of the business, at least at that clinic site.

**Electronic Medical Records (EMRs)**: There is a similar up- and downside from an emergency management point of view to Electronic Medical Records (EMRs). All good EMR systems should include data back up (to the cloud, or one or more off-site and out-of-area servers) and HIPAA-compliant security measures. This should ensure that patient data from before an incident will not be lost (assuming the data entry is up-to-date). Such measures, however, do nothing to insure access to patient data *during and immediately after an incident*, as power is frequently disrupted during many incidents and/or EMR access can also go down (i.e. with disruption to data/internet lines). To ensure that patient data collected during any time when the EMR system is down can be saved—for legal purposes both beyond and including HIPAA, as well as billing and critical data points that must be collected for FQHC status, HRSA, etc.—CHCs using EMRs
at this point need to keep all the reference paperwork and paper medical record forms at hand for those times when the EMR is not accessible.

Appendix J- Community Clinic Exercise Planning Checklist

3 - 6 months in advance of the exercise

- Determine with your internal CHC Emergency Preparedness Committee the scenario that you use you will use that reflects the hazards faced by your CHC and/or region.
- Determine which part of your emergency operations plan that you want to test using a
- Develop TTX objectives with your internal CHC Emergency Preparedness Committee.
- Determine the scope of how the emergency will affect your TTX, i.e., all CHC practice sites and CHC staff, or just partial staff and/or sites affected, etc.
- Set the date for the TTX to make sure that the appropriate CHC staff (senior leadership, including at least one representative from each department, i.e., clinical, operations, administration, etc.) has it on their calendars. Set aside at least two hours for the TTX to allow full staff participation and debriefing.
- Check with your public health, hospital, and/or office of emergency services to review their existing tabletop and/or functional exercise scenarios.

2 months in advance

- Review with the your internal CHC Emergency Preparedness Committee your existing emergency preparedness plan.
- Identify the facilitator, observers, and reporters/recorder roles for each of your internal CHC Emergency Preparedness Committee members. Review their roles with each committee members so they are clear on their duties.

1 month in advance

- Develop the injects- details that are specific to your CHC that creates “problems” that your CHC has to solve throughout the TTX. Don’t share the complete scenario with all staff in advance so that they will be able to “think on their feet”.
- Have the CHC Emergency Preparedness Committee develop an agenda for the TTX.

1 week in advance

- Order the food; confirm the room, the AV equipment and all the participants.
- Make copies of the CHC internal emergency preparedness plan for reference.
- Print the TTX ground rules to remind participants about the process.
Day of the exercise

- Cover TTX ground rules and objectives, ID the facilitator, observer, and recorders with participants.
- Conduct TTX with the players.
- Have copies of CHC EP plan available for reference.
- Conduct TTX “hotwash” immediately after and record participant’s experiences.

1 -2 weeks after

- Develop your After Action Report (AAR) that evaluates the TTX based upon the predetermined objectives.
- Review AAR with your CHC EP Committee for changes to EP plan for that will be reflected in your improvement plan.

TTX Scenario Development Tips

- Make it a plausible, known threat either for a man-made or natural disaster event your community could face.
- Modularize your TTX to include several timeframes of emergency response and recovery, i.e., at the time of the event, 6 hours later, the next day, the next week, etc.
- Once comfortable with conducting internal TTXs, invite local stakeholders to join you the next time- CHC Board members, public health, hospital, office of emergency services, community organizations, etc.

Some of the content in this document was adapted from the United States Department of Commerce, National Institute of Standards and Technology, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006. To access complete guide, please visit: NIST Guide.