DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING FOR EMR SYSTEM IN HEALTH FACILITIES IN KENYA

Julius Ogony[1], Ali Karisa[1], Mysha Sissine[2], Benard Ajwang[1], Joshua Oiro[3], Donna Medeiros[2], Bobby Jefferson[2]
[1]Futures Group, Kenya; [2]Futures Group, USA
[1]Morningside Office Park, Ngong Road, Nairobi, Kenya, [2]One Thomas Circle, NW Suite 200, Washington, DC 20005 USA
jogony@futuresgroup.com

ABSTRACT
Futures Group has been mandated by Ministry of Health (MoH) to rollout IQCare Electronic Medical Record (EMR) Patient Management and Monitoring System in health facilities in Kenya. Ideally the EMR should be available for use at the facilities with no or minimal disruption in terms of system failure, unavailability or data loss. This can only be achieved by having a disaster management and business continuity plan in every facility where EMR has been deployed.

KEY WORDS
Disaster Recovery; Business Continuity Planning; Electronic Medical Records; Patient Management and Monitoring.

1. Introduction

A disaster in EMR implementation can be termed as a predictable or unpredictable natural, accidental or manmade event which will result in widespread partial or total disruption of patient management and monitoring through loss of human lives, equipment or data at health facility. It is usually an event that cannot be contained using own resources, hence external help, resources and support will be sought.

Disaster comprises of four (4) components namely:

i. Preparedness
ii. Prevention/Mitigation
iii. Response
iv. Recovery

i. Preparedness
Preparedness involves measures put in place to ensure that the health facilities are able to detect disasters before they happen and be capable of coping with the effect of disasters if they do occur.

ii. Prevention/Mitigation
Prevention/mitigation involves measures to eliminate or reduce the probabilities of disasters happening in a facility.

iii. Response
Response involves measures taken in anticipation of, during and immediately after a disaster to ensure that the effects are minimized.

iv. Recovery
Recovery involves measures which support restoration/resumption of EMR services in affected service areas and reconstruction of data and physical infrastructure and/or equipment to acceptable operational levels in a facility.

Business continuity is the activity performed by a facility to ensure that critical healthcare functions will be available to patients, healthcare providers, facility non-medical workers, stakeholders, and other entities that must have access to those functions. These activities include routine operations such as patient care, monitoring, health records backups, and clinical operations. Business continuity is not something implemented at the time of a disaster; but refers to those activities performed daily to maintain service, consistency, recoverability and continuity.

Therefore the foundations of business continuity are:

- ✓ Standards
- ✓ Plans
- ✓ Program development
- ✓ Policies
- ✓ Guidelines
- ✓ Procedures

A facility needs to ensure there is continuity without stoppage due to planned or unplanned incidents, irrespective of the adverse circumstances or events.

Disaster recovery is the technical aspect of business continuity. This is the collection of both human and non-human resources and activities required to re-establish EMR systems (e.g. computers, servers, personnel, and other infrastructure such as networking, telecommunications, systems, etc.) at the facility or an alternate site following a disruption of EMR systems.

DOI: 10.2316/J.2014.216.815-0015

2. Objectives of Disaster Recovery and Business Continuity in EMR

The primary objectives of Disaster Recovery and Business Continuity planning in EMR are:

- ✓ Minimize threats, impacts and downtime
- ✓ Mitigate any losses in terms of data and information
- ✓ To ensure facility continues to operate and to do it in a cost-effective way
- ✓ Provide a plan of action to facilitate an orderly recovery of critical EMR functions
- ✓ Identify key individuals who will be involved to manage the process of recovering and restoring the EMR systems to normalcy after a disaster
- ✓ Identify the teams that will complete the specific activities necessary to continue critical medical record functions
- ✓ Specify the critical medical record activities that need to continue after an incident
- ✓ Outline the logistics of recovering critical facility medical records functions

3. Developing a Recovery and Business Continuity Plan

Developing a business continuity plan requires an assessment of facility service areas, applications, equipment and devices that are critical to the EMR operations at the facility, and also when these areas are significantly impacted by the system outages (e.g. after an outage of a minute, an hour, a day, etc.). Contingency plans for outages of varying duration and for various types of service areas need to be planned, developed, and integrated in the plan.

The following steps will be applied as part of the whole process:

Step 1 – Forming a Disaster Management and Recovery Team

A facility will have to form a Disaster Management and Recovery Team. This team will be responsible for reviewing possible disaster risks that a facility faces. At minimum, there should be one person from each department impacted by the EMR, and as many as can be spared from the Information Technology (IT) department.

The team needs to be large enough to be able to accomplish the tasks anticipated, but not so large that it becomes ineffective.

Step 2 – Technical Risk Analysis

The team will list all potential hazards and vulnerabilities and a proposed solution for each. A thorough understanding of the various components of facility network, including performance issues and usage throughput are considered. Also a list of internal vulnerabilities, such as viruses, patches or configurations are considered.

Technical analysis will look into issues of security components such as firewalls, intrusion detection systems (IDS), anti-virus etc. A complete network schema diagram will also be availed.

Step 3 – Non Technical Risk Analysis

The facility team will analyze risks that the facility faces outside of the technical arena. This comprises of the following non-exhaustive list of what some of these threats may include:

- ✓ Power outages
- ✓ Flood
- ✓ Civil unrest
- ✓ Sabotage
- ✓ Labor disputes
- ✓ Fire
- ✓ Physical security breaches
- ✓ Storms
- ✓ Terrorism
- ✓ Patient confidence

In this step list all the areas of the facility most likely to be impacted by threat. Determine what inspections can be made to identify specific risk factors and list the steps to mitigate potential loss.

Step 4 – Business Impact Analysis

Business impact analysis is done at the facility departmental level. While technology certainly is involved, the bottom line is the cost associated with an interruption of EMR system and the impact it has on the facility as a whole. Rather than focusing on specific resources, such as servers or networks, this analysis must focus on individual service areas within the facility.

In this step you list critical resources that each service area relies on plus resources that are critical and rate the criticality each resource as high, medium or low. Determine which factors are associated with an interruption of service in that particular service area. These cost factors could include financial, non-financial and costs due to loss of "goodwill" such as loss of patients, service delivery delays, and damage to patient confidence.

The time frames in which time sensitive operations, processes and functions must resume will be considered. This will lead to an estimate of the resources necessary for successful resumption, recovery, and restoration.

Step 5 – Development of Disaster Recovery and Business Continuity Plan
List all service areas and their location. Also make a list of critical resources that should be considered in the plan. Rate the impact of losing this resource (high, medium, low) and make a determination as to whether it should be included in the plan. Think about any constraints that may be encountered in implementing the plan and how these constraints might be dealt with.

Step 6 – Patient, Employee and Vendor Backup
Back up your patient, employee and vendor data off site and at a reasonable distance. Redundancy will keep facility data and information safe and available should EMR system go down. Also, it is important to maintain a reasonable distance, preferably 5 kilometers away from facility.

Step 7 – Establishment of Incident Command System (ICS)
Develop an Incident Command System (ICS) as part of your disaster preparedness and business continuity plan to ensure that facility can provide efficient patient care after disaster. In the ICS there should be minimal but adequate equipment and resources to offer services to patients in various service areas of the facility. The operating hours of ICS should also be stated to the team.

Step 8 – Prioritizing Recovery in Facility Service Areas
The core applications and EMR-dependent service areas need to be prioritized. Ranking and prioritizing facility service areas can be a complex undertaking, as areas will have varying levels of importance to the facility. For example, the EMR system will be highly critical to the facility registration area but not critical to pharmacy – even though both are ultimately critical to the functioning of the facility. There are additional complications, an example of which is the loss of the EMR that might have a major impact on one service area after a few minutes whereas another unit could go for 24 hours before a significant impact.

Some of the patient care service areas to be prioritized which are dependent on EMR system are:

- ✓ Accessing and editing the electronic medical record
- ✓ Ordering laboratory tests and reviewing results
- ✓ Ordering imagery examinations and reviewing results
- ✓ Providing medications and viewing patient medication profiles
- ✓ Registering and tracking the status and location of patients
- ✓ Scheduling patients and resources such as clinical and operating rooms
- ✓ Processing fee payments and issuing of receipts
- ✓ Managing of inventory through Supply Chain Management (SCM)

Step 9 – Key Personnel in Escalation Process
Knowing who to contact at a critical moment is absolutely vital to the success of recovery plan. Develop a template to create a list of critical personnel, their contacts, organized by service area of concern, and who should be called in case of emergency. The list should also have names and contacts of their next-of-kin who can be reached during emergency in case individual facility staff cannot be reached.

Step 10 – Vendor List
In the event of an emergency, vendors may need to be contacted quickly. Create a directory of all vendor account numbers, contact information and agreements. If a Service Level Agreement (SLA) is in place, make a copy of it and store it with the printed version of the Disaster Recovery and Business Continuity Plan, immediately after the list has been updated.

Step 11 – Documentation of Hardware and Software
Create a software inventory, which includes:

- ✓ Date of purchase
- ✓ License information
- ✓ Software packages
- ✓ Version numbers
- ✓ Vendor information
- ✓ Vendor contact
- ✓ Training required
- ✓ Service Level Agreements (SLAs)

A complete hardware inventory is also required. Create an inventory of hardware in facility such as server, switch, router, firewall, desktop, laptop, tablet, printer, etc. This inventory should include serial number of each item.

Specific tasks which are regularly performed also need to be documented. It cannot be assumed that all personnel will inherently know how to do all these unique tasks. Identify specific tasks or procedures that you have already documented, that are required as part of the EMR operation of the facility.

Documentation will also be done for information on remote site addresses, contact information, equipment and directions. This will help in resumption of EMR system services as soon as possible.

Step 12 – Regular Meetings and Recovery Plan Tests
Building a disaster recovery plan is not a one-and-done strategy. Since threats and hazards keeping changing, it is a continually changing and evolving process. Regular testing and meetings will help facility determine how

much it can handle disasters should they happen. The meetings should be held after ever incident to assess the performance and suitability of the plan.

Some facilities may prefer to test the plan annually, other's quarterly. Preferably testing should be done at least once a year. Some facilities will test everything at once; others will test in phases, such as doing the data backup system one day and emergency services relocation on another. Based on the size of the facility, medical specialties, location and the location of emergency service providers, among other things, the team must decide what model will work best for individual facility.

4. Challenges

EMR implementation can pose data security challenges with small disruptions (e.g. power failure) and larger events (e.g. flooding, hardware malfunction/virus) (Dynes et. Al 2006). In the current world, Disaster Recovery and Business Continuity Plans are imperative to ensuring the sustainability of a business. Without a thorough plan in place, there is a high risk that a facility would not survive a major disaster, hence EMR system interruption. With such a great need for the plan, there still exists major road blocks to implementation and sustainability of a Disaster Recovery and Business Continuity plan.

One recurring challenge is the continued lack of involvement of senior management and the board of directors of facilities. This issue is commonly a result of a delegation, by senior management, of the general overseeing of the disaster management issues to middle management. Once delegated, it is frequently the plan for senior management not to remain actively involved; however, involvement of senior management and the board of directors should remain a priority, to confirm the plan is effectively implemented, tested, and managed. In order to ensure this occurs, a facility should develop a steering committee which is comprised of key members of management and stakeholders. The committee should meet frequently to ensure a successful and sustainable plan is implemented and maintained.

In addition to the lack of involvement from senior management, facilities also struggle with some of the following challenges:

- ✓ **Managing growing data** - An outdated or under-performing backup/recovery solution may not be able to efficiently manage a growing volume of business data. Valuable IT resources that are needed for other business-critical tasks must spend hours managing data protection, thus contributing to an increase in operational costs and making other areas of IT vulnerable to failure.

- ✓ **Automated backups** - Using stand-alone devices rather than network-based solutions requires dedicated human resources to make sure that backups are started and completed. This leads to an increase in human error as the need for intervention grows.

- ✓ **Recovering data from offsite storage media** - Many facilities choose to send backup CDs, DVDs, and tapes offsite for enhanced disaster protection and safety. Subsequently, data recovery from an offsite backup may take extra time in terms of hours or possibly days to be accessed.

- ✓ **Managing data protection at remote/satellite branches** - Remote sites usually operate with few or no IT resources. If the data protection solution at the remote site is outdated, underperforming, or unreliable the local IT resources may be unable to resolve the problem for several days or weeks, therefore the data at the remote site becomes vulnerable to threats.

- ✓ **Meeting regulatory requirements** - Non-compliance with international or industry-defined data protection regulations could result in fines, legal fees, and damage the facility's reputation.

- ✓ **Lack of budget and IT expertise** - Data protection is a complex and expensive effort, and a facility may choose only basic data protection solutions to address its current needs. Such solutions may fit tight budgets, but they may not deliver all the features a facility need - especially when the next 12 to 24 months of data growth and performance requirements are considered. The use of under-performing solutions leads to a host of backup/recovery management issues and could even disrupt business activities. Additionally, many remote sites seem unaware of the abundance of affordable, simple, and efficient solutions on the market. Unlike centralized IT departments, many of these sites simply do not have the time and resources to research and test new solutions before making a purchase decision.

5. Lessons Learned

Although catastrophic disasters are unlikely, it is important to prepare for these events when planning and implementing EMR systems. The plan should enable disaster management process during EMR deployment on sites.

Lack of effective continuity planning or inefficient recovery efforts can be extremely costly, resulting in unknown or unacceptable losses. Inefficient planning can also be costly, while not ensuring the facility can recover after an incident. Waiting for an incident to happen to see how a facility reacts is a recipe for disaster. Facilities always learn from actual crises, but learning should be against plans that were put in place as opposed to the deployment of the EMR system. A facility that takes measured proactive steps, and tests its plan will have a much more efficient and effective recovery effort.

Adequately trained facility recovery staff with a comprehensive plan can take much of the worry and load off of management so they can continue focusing on the day-to-day running of facility.

Facilities have tendencies of justifying reasons for not having a Disaster Recovery and Business Continuity Plan in place quoting some of the following "Dangerous Excuses":

- ✓ It costs too much money to prepare
- ✓ There is no or not enough budget for it
- ✓ There is no enough time and/or resources
- ✓ It will never happen to our facility
- ✓ Why bother? We have good backups and fallback
- ✓ We "plan" on implementing one next year
- ✓ We have lived like so for many years

6. Next Steps

As EMR use is expanding in Kenya, there is a need to develop a disaster recovery and business continuity plan for EMR deployment to help facilities operate with minimal disruptions in disaster events.

Facilities should deploy a holistic approach management process to prepare for possible disruptions to business processes and manage risks to business operations. Facilities can automate their approach to disaster recovery and business continuity, and enable rapid, effective crisis management by deploying a coordinated and integrated approach.

7. Conclusion

Disasters happen every day. They range from every day events, such as server failure, to catastrophic natural events such storms, hurricanes, earthquakes and floods. Because the healthcare delivery system plays such a critical role in a society, a healthcare facility needs to be prepared for any eventuality.

Facilities have complex recovery requirements; a facility's recovery plan must be robust and thorough. A facility should establish outside relationships – with other healthcare delivery systems and with disaster management agencies that offer flexible and adaptable recovery options. A facility disaster recovery plan should be comprehensive, covering restoration of data, staff, equipment, operations, power, connectivity and technology.

While revenue loss is obviously a critical issue for facilities which are often operating on razor thin margins, ensuring continuity of patient care is the most important priority for any facility concerned with disaster recovery. For a healthcare delivery system, recovery and business continuity is a matter of life and death.

References

[1] Geoffrey H. Wold (1997), *Disaster Recovery Planning Process. Systems Support, Inc.* pp. 214-232.

[2] Austin, C., Trimm, J., Sobczak, M. (1995) *Information Systems and Strategic Management. Health Care Management Review*, Vol. 20 No. 3, pp. 26-33.

[3] Campbell EM. Sittig DF. Guappone KP. Dykstra RH. Ash JS. (2007) *Overdependence on Technology: an unintended adverse consequence of computerized provider order entry.* Annual Symposium Proceedings/AMIA Symposium.

[4] Johnson, M.E. and Goetz, E. (2007) *Embedding Information Security into the Organization, IEEE Security and Privacy*, vol. 5, no. 3, pp. 16-24.

[5] Dynes, S. (2006) *Information Security and Health Care – A Field Study of a Hospital After A Worm Event* http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecHealthCare.pdf

Accessed 17-Jun-2014