Data Management Best Practices in Radiation Oncology

1. Data & Network Security
2. Data Redundancy
3. Disaster Recovery Planning

Collin Brack, M.B.A., CPHIMS
Manager, Software Systems Programming
Department of Radiation Oncology

UTMB®
The University of Texas Medical Branch

- According to a recent NFIB National Small Business Poll, man-made disasters affect 10% of small businesses, whereas natural disasters have impacted more than 30% of all small businesses in the USA. Hurricanes are by far the most destructive force causing power failure, flooding, customer loss, and the closure of many businesses.

Shameless Wikipedia Quotes

"Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure."

"A Business Continuity Plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity."

source: http://en.wikipedia.org/wiki/Disaster_recovery

Disaster Recovery Planning

- An in-house, departmental, team based effort
- PHYSICIST RESPONSIBLE FOR CLINICAL DATA MANAGEMENT ELEMENTS
- Goal is to identify central Information System weaknesses
- Part of the Business Continuity Plan (BCP)
- Executive-level approval and sign-off

rise of BCP/DR

"…regulatory and global business focus on BCP arguably waned after the problem free Y2K rollover…this lax attitude ended September 11th 2001."

Best-practices buzzword

- What do we mean by best practices?
- “Best” according to who?

DR Plan Prerequisites

1. Data & Network Security
2. Data Redundancy
3. Disaster Recovery Planning

0. Define Data!
1. Data & Network Security
2. Data Redundancy
3. Disaster Recovery Planning

Data: Source vs Legal

- Can vary by state, specialty, and practice setting
- Helpful to divide data into 4 categories:
  - Legal Health Record
  - Patient-Identifiable Source Data
  - Administrative Data
  - Derived Data

Data: Legal Health Record

- “The legal business record generated at or for a healthcare organization. This record would be released upon request.”

- Radiation Oncology examples?

source: Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." Journal of AHIMA

Elements of Legal Health Record

* advance directives
* anesthesia records
* care plan
* consent for treatment forms
* consultation reports
* discharge instructions
* discharge summary
* e-mail containing patient-provider or provider-provider communication
* emergency department record
* functional status assessment
* graphic records
* immunization record
* intake/output records
* medication orders
* medication profile
* minimum data sets (MDS, OASIS, etc.)
* multidisciplinary progress notes/documentation
* nursing assessment
* operative and procedure reports
* orders for diagnostic tests and diagnostic study results (e.g., laboratory, radiology, etc.)
* patient-submitted documentation
* pathology reports
* practice guidelines or protocols/clinical pathways that imbed patient data
* problem list
* records of history and physical examination
* respiratory therapy, physical therapy, speech therapy, and occupational therapy records
* selected waveforms for special documentation purposes
* telephone consultations
* telephone orders

Source Data Definition:

- “An adjunct component of the legal business record as defined by the organization. Often maintained in a separate location or database, these records are provided the same level of confidentiality as the legal business record. The information is usually retrievable upon request. In the absence of documentation (e.g., interpretations, summarization, etc.), the source data should be considered part of the LHR.”

- Cone beam CT Example?

source: Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." Journal of AHIMA

Administrative & Derived Data:

- Administrative data (payment purposes)
- Derived data are anonymous, aggregated or summarized data (reports)

A subpoena for a patient's LEGAL health record in Radiation Oncology would most likely include a request for the following data EXCEPT

20% a) Diagnostic Films

20% b) Consultation reports

20% c) Special Procedure report

20% d) Incident or patient safety reports

20% e) Treatment Completion Report

2. A subpoena for a patient's LEGAL health record in Radiation Oncology would most likely include a request for the following data EXCEPT
    (a) Diagnostic Films
    (b) Consultation reports
    (c) Special Procedure report
    (d) Incident or patient safety reports
    (e) Treatment Completion Report

    Answer: d –Incident or patient safety reports are considered administrative data

    Ref 1: Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." Journal of AHIMA 72, no.9 (2001): 88A-H.
    Ref 2: AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes." Journal of AHIMA 76, no.8 (September 2005): 64A-G.

Data & Network Security

- Next Prerequisite because why backup corrupt data?

- **3 Key Security Elements**

  ANTI-VIRUS

  PHYSICAL NETWORK SECURITY

  VIRTUAL NETWORK SECURITY

Data Security

- Anti-virus Issues:
  - Choose institutional virus scanning first
  - Address shortcomings with IS Leadership / CIO if current solution does not fit RadOnc needs
  - Vendors NOT RESPONSIBLE for anti-virus and often discourage installation (real-time scanning)
  - Virus definitions must be automated
  - Example of virus that corrupted RadOnc EMR data

Network Security

- Can’t manage data if it has been compromised
- Dept. Homeland Security recommendation for “compromised” computer:
  - Identify the backdoor or trojan and remediate?
  - No, low-level format hard drive and restore non-compromised data

Physical network security

- Isolated network for sensitive systems
- Radiation Oncology examples include:
  - LINAC console
  - Dedicated R&V server/client network

Physical network vs. VLAN

- VLAN (Virtual LAN): isolate a set of computers connected to a network and are created in software on routers/switches
- Same network switch, isolated virtually not physically
- Examples in Radiation Oncology:
  - Multi-site clinics where physical network isolation not practical
  - Large networks which do not employ sub-netting
  - Don’t trust your network or those on the network! Security breaches occur *within* organizations

…from VLANs to Firewalls

- Firewalls traditionally protect systems from WAN or external network threats
- Employed at edge routers and public-facing servers
- Firewalls installed on computers can cause connectivity issues, better to use network segmenting
- Client or workstation firewalls should be used if connected directly to router (i.e. home internet)

Information Security “best practices” for a Radiation Oncology department WITHIN a hospital would include all of the following EXCEPT

20% a) Virtual or physical network segmenting

20% b) Real-time Virus Scanning

20% c) Operating System Patch Deployment

20% d) Workstation Firewalls

20% e) The creation of user accounts for vendor maintenance

3. Information Security "best practices" for a Radiation Oncology department WITHIN a hospital would include all of the following EXCEPT
   (a) Virtual or physical LAN (network) segmenting
   (b) Real-time Virus Scanning
   (c) Operating System Patch Deployment
   (d) Workstation Firewalls
   (e) The creation of user accounts for vendor maintenance

   Answer: d– Workstation firewalls are more applicable to home use, not the enterprise

Ref 1: H. F. Tipton et al. Information Security Management Handbook, Vol 2., 2007.
Ref 2: Siochi et al. Information technology resource management in radiation oncology. JACMP 10(4), 2009.

- We've identified the target Data
- Protected the Data from virus & network vulnerabilities
- Focus shifts to Data Redundancy

Data Redundancy / Backups

- Simply ask the following question:

"Where, physically, does my data[base] live?"

- Client/Server models are creating confusion:
  - Data can live off-site with a vendor (ASP model)
  - Data can live in Departmental server (internal custodianship)
  - Data can live in Data Center (centralized IS custodian)
  - Data can live on the client (dangerous)

Data Redundancy 101

- Centralized (Enterprise) IS Department are experts at data management within the Data Center. Their jobs depend on it. (Institutional EHR, PACS)
- Must make strong case to not locate Radiation Oncology data within this environment.
- Hybrids: physical server redundancy with one server in data center and a mirrored server in Radiation Oncology

We can do it in-house

- Opting out of centralized IS data center resources and what this entails
- Prepare to become IT server/hardware expert:
  - RAID (hard drive mirroring and redundancy)
  - Software-based RAID vs hardware based RAID
  - Physical backup management (tape rotations & architecture)
  - Backup scheduling and reporting (what & when)
  - Annual disaster recovery simulations
  - Bare-metal backups vs file-level backups
  - Hard-drive encryption for systems vulnerable to theft (laptops)
  - Sustain this expertise in-house while providing adequate cross-coverage

Data Management Opus: DR Plan

- Identified the source and legal Data
- Ensured that a base level of security is in place
- Implemented Data Redundancy
- Document everything in a formal DR Plan (Part of the BCP Process)

3.2 Risk Analysis

The BCP Project Team has examined each potential environmental disaster or emergency situation including, but not limited to, organized disruption (i.e. human cause); loss of utilities and services disruption; equipment or system failure; and serious information security incident.

Each of the above potential threats has been examined in detail and an analysis developed to evaluate the consequences of each. Each scenario has also been assessed for the possible of occurrence (probability rating) and possible impact (impact rating.)

Below is a roll-up of the most significant items as indicated by the Radiation Oncology team.

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	IMPACT RATING (SEE TABLE BELOW)	RISK RATING PROBABILITY x IMPACT =	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Flood	5	5	25	Treatment machines are on the first floor and are subject to rising water damage. Loss of machines will result in patient relocation and staffing issues.
Cyber Crime	4	4	16	Disclosure of patient data and/or deletion of patient data. Delays associated with restoring records.
Hurricane	5	4	20	General disruption of all services and staffing issues. Property damage, patient and staff safety.
Electrical Storms	5	3	15	Possible power and equipment failure.

what's wrong with this slide?

Disaster Facts

Common IT disasters:

Power outages	28%
Storm damage	12%
Floods	10%
Hardware error	8%
Bombing	7%
Hurricanes	6%
Fires	6%
Software errors	5%
Power surge/spike	5%
Earthquake	5%

DR Plan must defin

Recovery Time Objective (RTO):

How long will it take to "recover" the data? Shorter the RTO, more expensive, i.e. tape backup located 20 miles away = RTO of 2 hours.

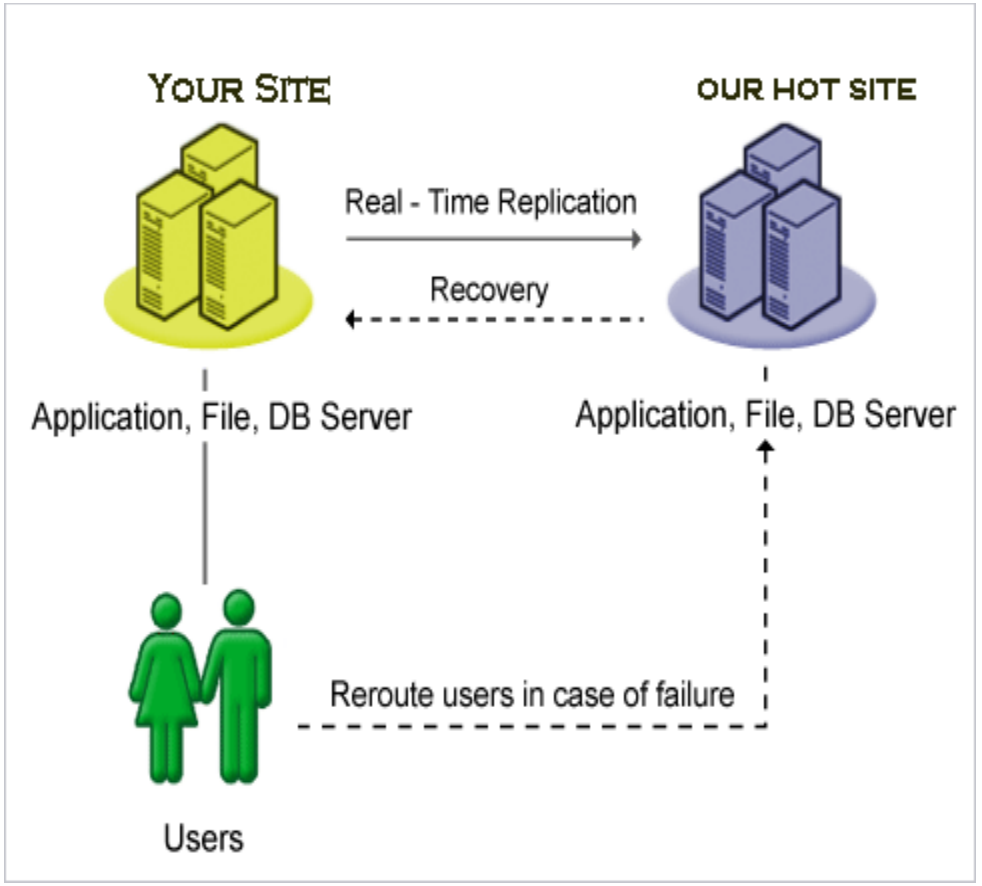
Recovery Point Objective (RPO):

How long "back" do I have a recovery point? 1 day snapshot vs incremental backups...

DR Plan must describe in detail:

Hot Site:

Cloned hardware, resident data, sync metric is RPO, reduced capacity (licenses) and capabilities (bandwidth), staffing issues, $$$$



Cold site:

Inexpensive, no hardware, BYO data, longer RTO.

"Go buy a some servers and start restoring tapes when they arrive."

Warm Site:

Minimal hardware, networking, backups via sneaker-net.

"Wait to license servers with vendor and FedEx the tapes over…"

A Radiation Oncology department's Disaster Recovery plan is a sub-set of the broader, hospital-wide contingency documentation know as the

20% a) Business Continuity Plan

20% b) HIPAA Contingency Document

20% c) HIPAA Continuity Plan

20% d) JCAHO Emergency Preparedness Plan

20% e) Sentinel Event Plan

4. A Radiation Oncology department's Disaster Recovery plan is a sub-set of the broader hospital-wide contingency documentation know as the
   (a) Business Continuity Plan
   (b) HIPAA Contingency Document
   (c) HIPAA Continuity Plan
   (d) JCAHO Emergency Preparedness Plan
   (e) Sentinel Event Plan

   Answer: a – Business Continuity Plan

   Ref: Carrison K. S. Tong, Eric T. T. Wong. Governance of Picture Archiving and Communications Systems: Data Security, 2007.

DR Plan Justification: HIPAA

HIPAA Security Rule 164.308(a)(7)(i)

7.

i. *Standard: Contingency plan*. 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.

ii. *Implementation specifications*:

A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

ii. Implementation specifications:

A. Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

ii. Implementation specifications:

B. Disaster recovery plan (Required).
Establish (and implement as needed) procedures to restore any loss of data.

ii. Implementation specifications:

C. Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

- i.e. Business Continuity Plan

ii. Implementation specifications:

D. Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

E. Applications and data criticality analysis (Addressable).

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Hospitals in the US are required by law to implement specific Disaster Recovery planning measures in relation to HIPAA. Which of the following contingencies measures is NOT REQUIRED but instead considered OPTIONAL?

25%	a)	Establishment of an emergency mode operation plan
25%	b)	Creation AND execution of an annual simulated data restoration
25%	c)	The creation AND execution of a data backup plan
25%	d)	The creation of a disaster recovery plan

10

1. Hospitals in the US are required by law to implement specific Disaster Recovery planning measures in relation to HIPAA. Which of the following contingencies measures is NOT REQUIRED but instead considered OPTIONAL?
    (a) The establishment of an emergency mode operation plan
    (b) The creation AND execution of an annual simulated data restoration
    (c) The creation AND execution of a data backup plan
    (d) The creation of a disaster recovery plan

    Answer: b – The creation AND execution of an annual simulated data restoration

    Ref : HIPAA Security Rule 164.308(a)(7)(i)