Data Flow and Management in Radiation Therapy

- Issues in Data Flow and Data Management in Radiation Oncology – C. Bloch
- DICOM- an Overview with an Emphasis on Therapy - R. Siochi
- Issues in Data Flow Management in Radiation Oncology: Disaster Recovery - C. Brack

Issues in Data Flow and Data Management in Radiation Oncology

The Medical Physics Perspective

C. Bloch, Ph.D. DABMP

July 21, 2010

Learning Objectives:

1. Review the variety of types of patient data common in Radiation Oncology.
2. Understand the basics of HIPAA as it pertains to pertaining that data and business continuity.
3. Understand the various causes of electronic data loss, including viruses, worms, computer system failures and theft.
4. Review how network topology can be used to enhance efficiency as well as provide additional layers of protection for patient data.

Am I in the right room?

- Do you ever have computer problems?
- Do you want SAM credit?

Pre-requisites:

- Your computer is plugged in
- You've tried rebooting
- You still have problems.

Overview

Radiation Therapy has evolved to the point that all clinical information and processes are computerized. However, this evolution had occurred in relative isolation from other departments which we now want to be integrated with. Patient records are in the hospital EMR, the RO EMR, DI PACS…

Everything is networked – the network is the key.

Evolution

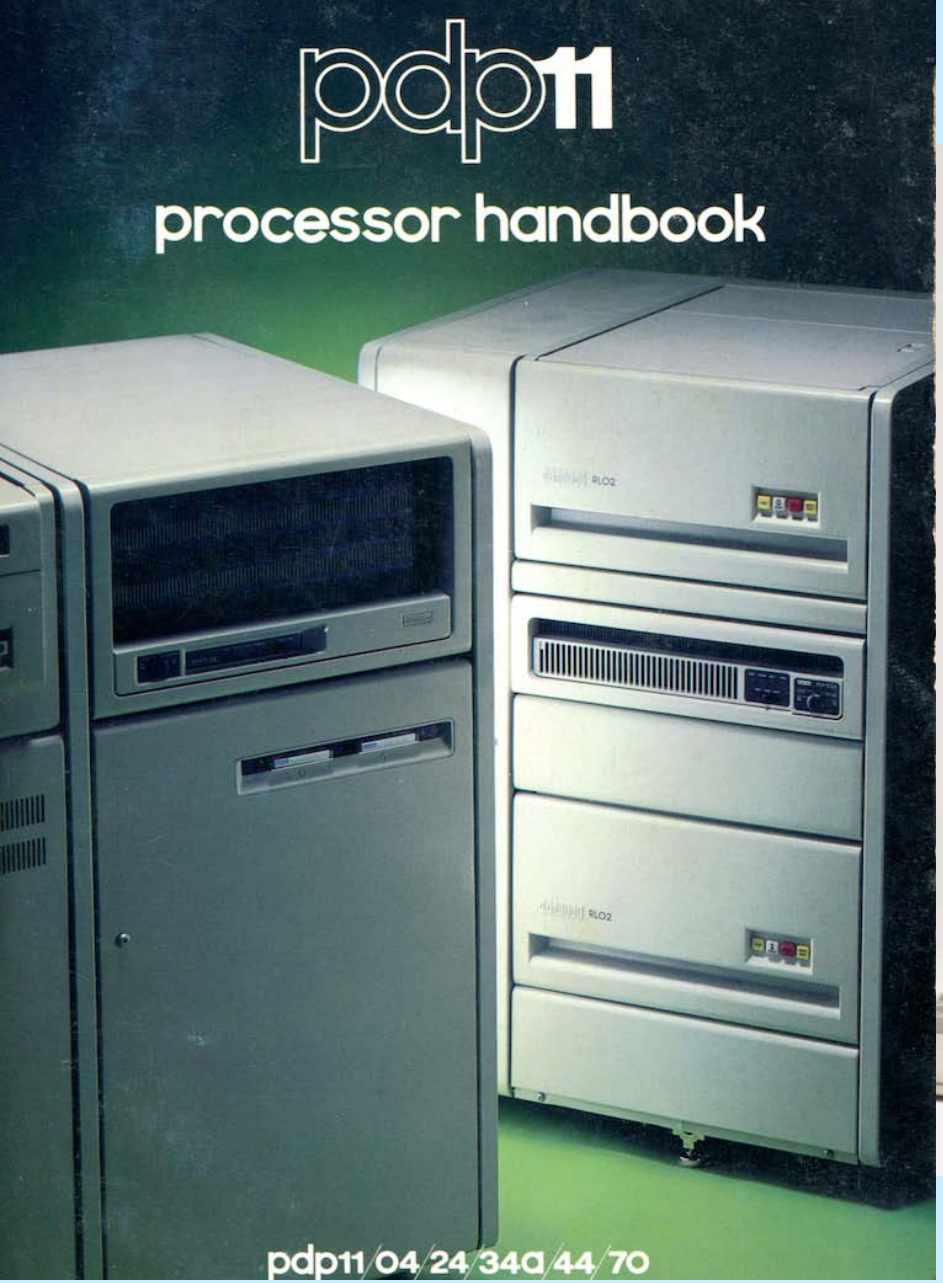
- Teletherapy units had relays and time/MU were set via mechanical thumb-wheels.


1800 Serial #
252


POSITION
DOSE RATE
TIME
WEDGE
ARC THERAPY
DEGREES
STOP ANGLE
X-RAYS
6
CONTROL
MINUTES
ENERGY
CONTROL POWER
TEST
STBY
ON
RADS-DEGREE
ARC
CW
CCW
15
DOSE RATE
MIN
MAX
ENABLE
LOWER JAW
UPPER JAW
Opening
COLL ROT
GANTRY
SPEED
CCW
OPEN
CW
CLOSE
SELECT
INDEP JAW
X-RAYS
FULL FIELD
BEAM ON

Evolution

- Teletherapy units had relays and time/MU were set via mechanical thumb-wheels.
- Computers were added as a “front-end” and electromechanical controls were hidden from the user.


pdp11
processor handbook
pdp11/04/24/34a/44/70


IBM
064 KB_

Evolution

- Teletherapy units had relays and time/MU were set via mechanical thumb-wheels.
- Computers were added as a “front-end” and electromechanical controls were hidden from the user.
- Computers became the exclusive control system.
- 3rd-party R&V systems were added as a second “smart” computer layer.

Evolution

- R&V systems evolved into Electronic Medical Records (EMR) including billing and scheduling.
- Ancillary devices (MLCs, Epics, Gating, kV imaging, etc.) were added to Linacs with additional control computers.


AP
LAT
S-I

Evolution

- CT images were transferred from radiology to RT for treatment planning. Patients were simulated on “simulators”.
- RT departments acquired their own CT-simulators. RT images are generally not transferred to PACS (radiology).
- RT imaging expanded to include daily CT, MR-simulators…


VARIAN
Emergency Stop
Preview
Prepare
Message
Warning
MV Ready
Push to Talk
Motion Enable
kV Beam On
Beam Off
MV Beam On

Evolution

- Cancer care has changed. Patients used to get either surgery, chemotherapy or cancer. Now, it is common for patients to get combined therapies, 2 or all 3 of the above. This has increased the need for (computer) communication between different departments within the hospital.

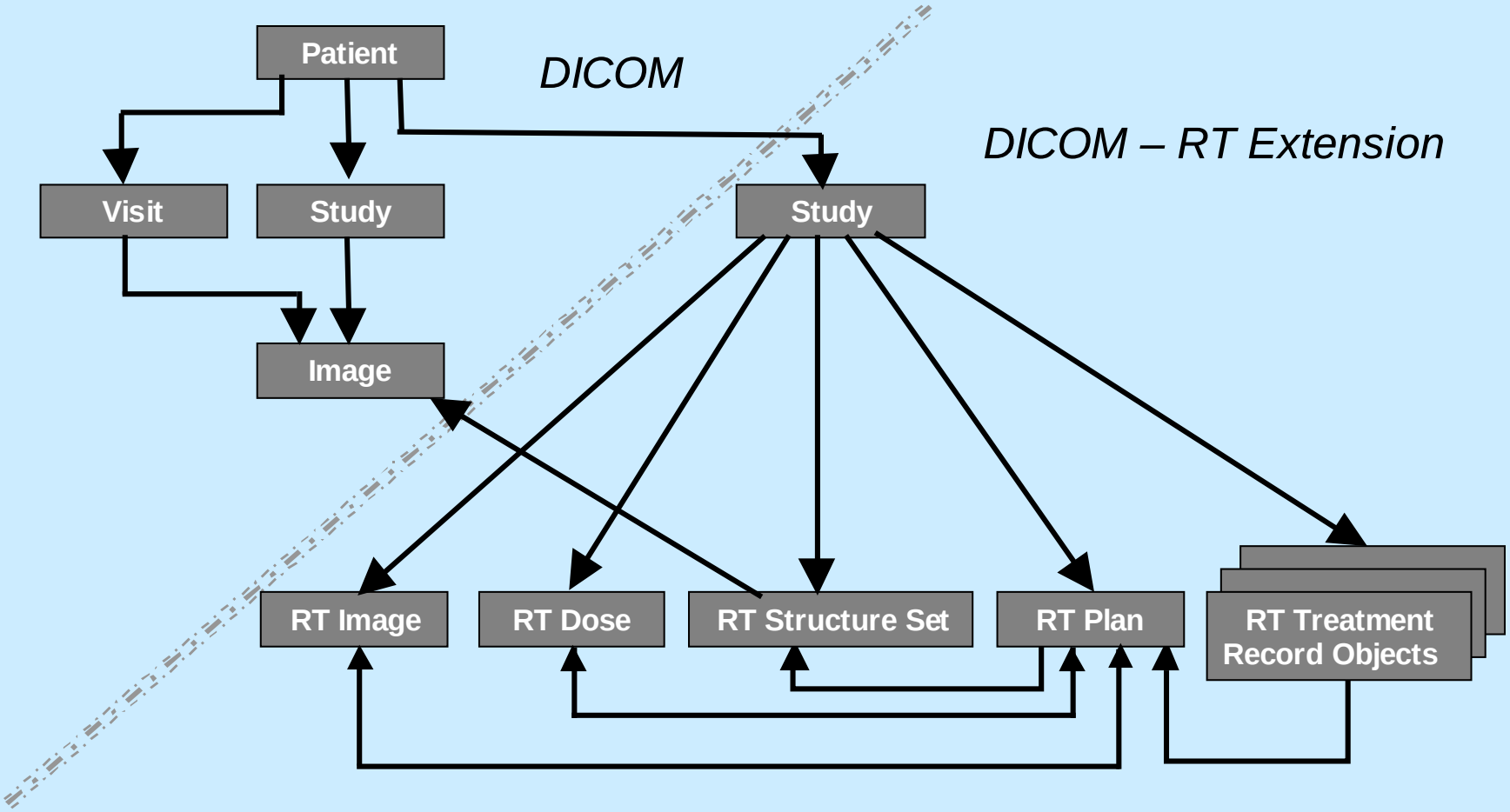
HIPAA

- Health Insurance Portability and Accountability Act
  - Patient data must be available to the patient, therefore, you must not lose it.
  - Patient data must not be available to anyone not authorized. So again, you can't lose it, but you also must not share it, inadvertently or otherwise.
- Result has significant implications for network security and data backups and archives.

Data Management

- Multiple sources of data are used in patient care:
  - Outside images brought by patient on disk
  - In-house DI imagining: CT, MR, PET…
  - RO images: 4D-CT, PET-CT, MR-sim, DRRs, portal images, kV setups, CB-CT, MVCT…
  - Treatment plans: image registrations, field information, dose distributions
- Can you retrospectively show how a patient's care was determined and carried out?
- How long can you show that?

Patient Data



Data Management

- Online Storage for current/recent patients.
  - R&V database
  - Treatment planning database
  - Imaging database
- Archives for completed patients.
  - How do you restore?
  - How are the archives protected?
  - How long will the archive last?
- Backups for disaster recovery.
  - Must test **backup** and **restore**.
  - How long will you be down after your server dies?

Data Storage

- RAID (Redundant Array of Inexpensive Disks) disks generally required. Can automatically make duplicate copy of all data, and alert user if one copy/disk fails before both copies are lost.
- Backup servers are important too. Try to eliminate “single points of failure” that could disable your clinic. It is not enough to preserve the data; you need real-time access to it.

Data Storage

- Off-site storage is required as well. If a disaster occurred in the building where the data is housed (e.g. a fire), there should be another copy in a remote location.
- Test backups. Too often software is used to backup data (even with verification), but no attempt is made to restore it. It is surprising how often restore attempts fail. Reasons can be media has shelf life, software upgrades/incompatibilities, etc.

Data Storage

- Volume:
  - How much data do you need to store this month?
  - How much data will you need to store next month?
  - How long does it take to transfer the data?
  - How fast do you need to be able to get to the data?

Protection of patient data requires all of the following EXCEPT:

20% 1. Provision of backup for all systems.

20% 2. Proper storage and retention for all electronic data

20% 3. System downtime and recovery plans for unexpected computer downtimes

20% 4. Maintenance of a support manual and how-to guide for computer systems and information

20% 5. Support for DICOM-RT

1. Protection of patient data requires all of the following EXCEPT:
   - (a) Provision of backup for all systems
   - (b) Proper storage and retention for all electronic data
   - (c) System downtime and recovery plans for unexpected computer downtimes
   - (d) Maintenance of a support manual and how-to guide for computer systems and information
   - (e) Support for DICOM-RT

   Answer: (e) -- Support for DICOM-RT

DICOM-RT is what we want, but not a requirement of HIPAA.

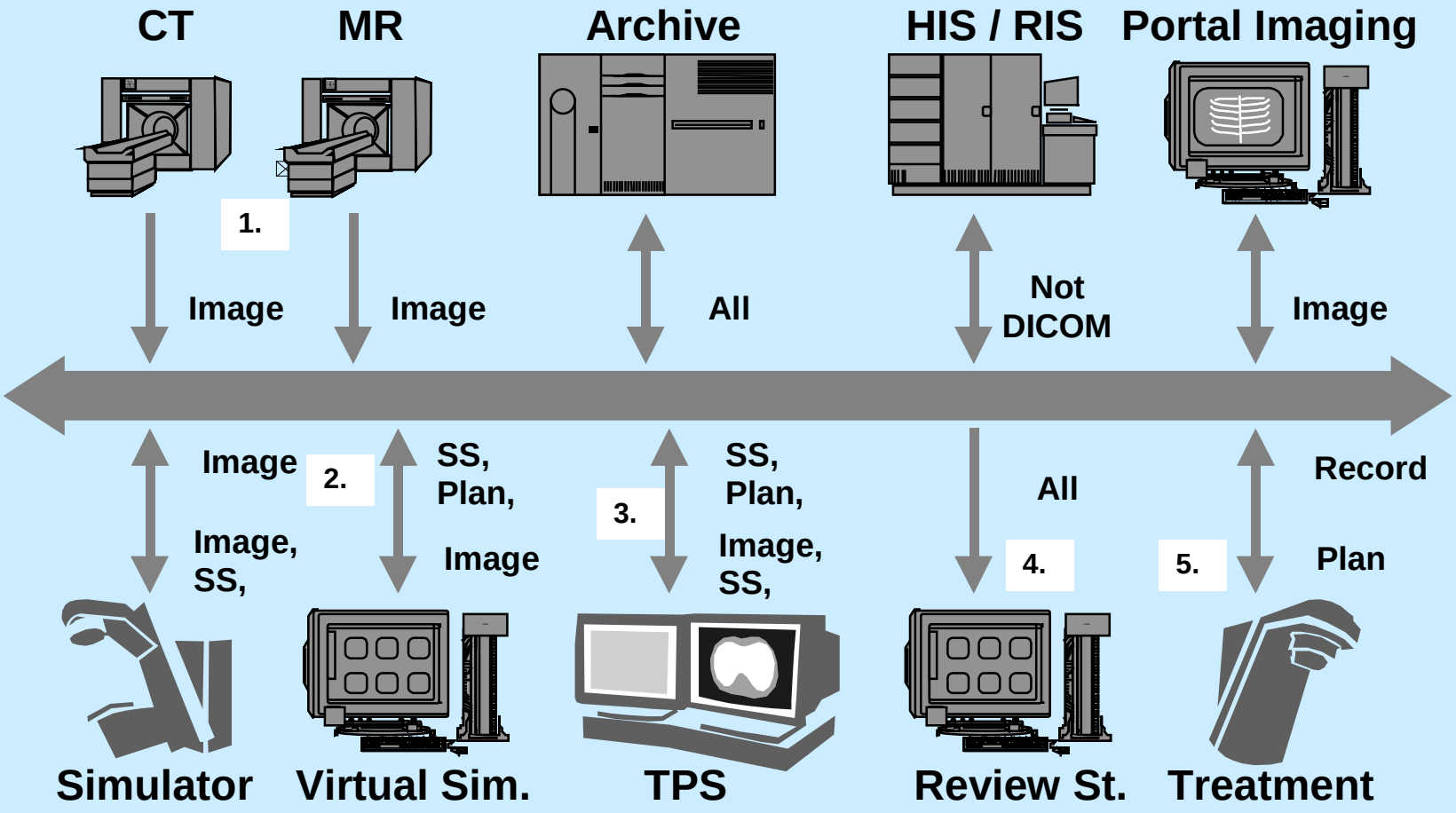
Ref 1: ACR Practice Guideline for Electronic Medical Information Privacy and Security, Rev. 2009.

Ref 2: Siochi et al. Information technology resource management in radiation oncology. JACMP 10(4), 2009.

The Network

- Generally, data can be transferred among all of the computers that are part of the clinic via a local area network (LAN).
- Computers on the LAN can also reach the internet through a hospital connection point to allow access to external e-mail, the WWW, ftp sites, etc.
- Multiple functions and multiple users raises many security issues.

The Network


CT
MR
Archive
HIS / RIS
Portal Imaging
1.
Image
Image
All
Not DICOM
Image
Image
2.
SS, Plan,
Image
3.
SS, Plan,
Image, SS,
All
4.
5.
Record
Plan
Image, SS,
Simulator
Virtual Sim.
TPS
Review St.
Treatment

The Network

- Data flow is controlled by routers and switches. Their primary job is to “route” the data from its source to its destination.
- Firewalls are hardware devices and software applications designed to restrict connectivity.
  - Limit access from outside the institution (e.g. to stop hackers)
  - Isolate segments of the LAN (e.g. improve workflow)
  - Block specific ports or applications (e.g. no ftp)
  - Intercept/block malware

Computer Threats

- Virus, worms, hackers and other threats can steal confidential information, corrupt computer systems and disable clinical functions.
- Legitimate computer use can also interfere with other clinical operations (bandwidth and network traffic).
- The bad guys can be attacking from the hallway, not just the internet.

Network Security

- A “roadmap” of your network should be organized to improve dataflow and security.
- Hospital firewall (between internet and LAN) does not protect against malware brought in via laptops, memory sticks, e-mail or WWW links.
- Hospital anti-virus software is not always compatible with clinical computers (MLC, Linux computers, etc.)

Data on Radiation oncology systems is secured by all of the following EXCEPT:

20%	1. Firewalls.
20%	2. User passwords
20%	3. Linux
20%	4. Conventional locks and keys
20%	5. Encryption technology

2. Data on Radiation oncology systems is secured by all of the following EXCEPT

(a) Firewall(s)
(b) User passwords
(c) Linux
(d) Conventional locks and keys
(e) Encryption technology

Answer: c - Linux

Security must be applied to all systems, Windows, Linux, even Macs..

Ref 1: ACR Practice Guideline for Electronic Medical Information Privacy and Security, Rev. 2009.

Ref 2: Siochi et al. Information technology resource management in radiation oncology. JACMP 10(4), 2009

LAN Topology

- RO computer systems with distinctly different functions should be organized within specific layers of security. This can be accomplished with programmable switches and/or internal firewalls.
  - Real-time clinical devices (Linac controller, MLC controller, etc.)
  - Secondary clinical devices (Treatment planning system, film scanner, etc.)
  - Non-clinical devices (e.g. office desktop computers)

LAN Topology

- Real-time clinical devices should have their own private LAN (or VLAN) for communication amongst themselves and not allow access except by other computers within the hospital.
  - E.g. MLCs must operate in real-time and cannot be interrupted by misdirected network traffic.
  - R&V system needs to monitor Linac control computer and not be slowed by web browsing or corrupted by e-mail download.

LAN Topology

- Similarly, other clinical devices should have limited connectivity outside the department (e.g. radiology yes, WWW no) for workflow efficiency, data security, and business continuity.
  - E.g. data transfer from CT-simulator to treatment planning system can be corrupted by excessive network traffic.
  - Virus downloaded via e-mail can end up on CT simulator and disrupt department workflow.

LAN Topology

- Desktop computers generally need relatively open access to the internet (unsecure). However, because they may contain clinical information and because they are on the LAN, they still need some protection.
  - E.g. ftp protocol (port 21) should be blocked because passwords are transferred unencrypted.

Good network topology can enhance all of the following EXCEPT:

20%	1. Speed of data transfers.
20%	2. Integrity of data transfers.
20%	3. Security of computer systems
20%	4. Data storage space
20%	5. Business continuity.

3. Good network topology can enhance all of the following EXCEPT

(a) Speed of data transfers
(b) Integrity of data transfers
(c) Security of computer systems
(d) Data storage space
(e) Business continuity

Answer: d – Data storage space

Network topology can affect access time for data storage, but not the amount of space available.

Ref 1: ACR Practice Guideline for Electronic Medical Information Privacy and Security, Rev. 2009.

Ref 2: Siochi et al. Information technology resource management in radiation oncology. JACMP 10(4), 2009.

Portable Devices

- Portable devices (laptops, USB hard drives, memory sticks) are a significant risk.
- They can be taken outside the hospital firewall and become infected with any number of malware files. These files are then brought inside the firewall (evading its protection) by employees. The threat is even greater if these portable devices are then connected directly to clinical computers (instead of desktop computers).

Portable Devices

- Portable devices are also more prone to theft or accidental loss. This creates the potential of exposing a patient's private information to whoever finds/steals the device.
- Carrying patient data outside the institution should be restricted to limit such losses.
  - Note: all off-site archives contain patient information that has been carried outside the institution.

Portable Devices

- Within the institution portable devices especially need physical protection: them must be locked/chained so they cannot easily be stolen.
- Portable devices should also be encrypted. Such data is scrambled and generally can only be unscrambled by someone who knows the encryption password.
- All computer systems in the institution should require physical and password protection.

Support Team

- Medical physicists
  - Computer functions, resource needs, team coordinator
- Professional RO IT
  - Specialists in various systems: network hardware, various operating systems, backup and data archiving
- Vendors
  - Tools, environment configuration, application training

HIPAA stands for:

20%	1. Health Information Portability and Accountability Act.
20%	2. Health Insurance Portability and Accountability Act.
20%	3. Health Insurance Privacy and Accountability Act
20%	4. Health Information Privacy and Accountability Act
20%	5. Health Information Privacy and Assurance Act .

4. HIPAA stands for

(a) Health Information Portability and Accountability Act
(b) Health Insurance Portability and Accountability Act
(c) Health Insurance Privacy and Accountability Act
(d) Health Information Privacy and Accountability Act
(e) Health Information Privacy and Assurance Act

Answer: b - Health Insurance Portability and Accountability Act

Remember, one “P”, two “A”s. Electronic records are supposed to increase *portability* and *accountability*. The privacy that we are all concerned about is just part of the overall act.

Ref: ACR Practice Guideline for Electronic Medical Information Privacy and Security, Rev. 2009.

References

- Institute of Medicine, *To Err is Human: Building a Safer Health System.* 2000.
- Nikiforidis et al., Med. Phys. 33, 2006.
- Kagadis et al., Med. Phys. 35 (1), 2008.
- ACR Practice Guideline for Electronic Medical Information Privacy and Security, Rev. 2009.
- Siochi and Brack, Medical Physics 36 (9), 2009.
- Siochi et al., JACMP 10(4), 2009.