HEALTH CARE INFORMATION TECHNOLOGY SECURITY

Dr. Walter O. Baggett

MBA, Ph.D.,CPA

This presentation was initially made in Ghent in 2009 and was used, along with discussion whiteboard diagrams, to describe the development of a program of research at Monash University in 2010

MANHATTAN COLLEGE

Een uniek gastcollege over self-management, empowerment, behavior change and self-efficacy in verpleegkunde en patiëntenzorg. De theoretische concepten worden gekaderd in en geïllustreerd met voorbeelden uit hun onderzoek naar o.a. chronic illness self-management, student academic integrity, information technology security in healthcare.

Prof dr. Lillie Shortridge

&

Prof dr. Walter O. Baggett

MANHATTAN COLLEGE

HEALTH CARE INFORMATION TECHNOLOGY SECURITY

Dr. Walter O. Baggett
MBA, Ph.D.,CPA

MANHATTAN COLLEGE

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule took effect on April 14, 2001)
- There must be a written management plan to assure this is done and a person designated as “responsible for the development and implementation of the policies and procedures of the entity.”

MANHATTAN COLLEGE

What Information is Covered under the (HIPAA) Privacy Policies?

(PHI- Protected Health Information)

- All clinical, financial and demographic information about a patient

- Electronic, paper copies and verbal discussions

Note: Directory Information is public (not PHI) while patient is here (unless s/he "opts out")

Protected Health Information (PHI)

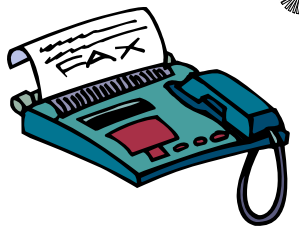
PHI - refers to:

a. Anything you see or hear that lets you know about the health of a specific individual.

b. A record of an individual's having been a patient of ours, having a lab test, a doctor's appointment, etc. is considered PHI.

What form does PHI take?

- Paper copies
- Patient files or charts
- Telephone calls and voice mail
- Verbal communication
- Fax transmissions
- Internet or Intranet transmissions
- Emails



What is not considered PHI?

- Information contained in a employee's personnel record is not considered PHI;
- This information must be kept private under our personnel policies. (HR Policy #15.4)

Who is Responsible for maintaining privacy policies?

- Nursing staff
- Employees
- Physicians
- Students
- Volunteers

Nursing ABC's

A. You should view only the information needed to care for your patients or perform your job

- If the information is for patient care or to perform your job you are not restricted from accessing the information or disclosing it another healthcare provider (Policy H-1)

Nursing ABC's

B. PHI should not be shared with anyone who does not have an official need to know, unless that person has been authorized by the patient or personal representative

- You may share information with other staff treating the patient
- You may share information with family members if the patient agrees

Nursing ABC's

C. You may share PHI if it is being used for Treatment, Payment or healthcare Operations (TPO)

Nursing ABC's

Treatment – you may use or disclose patient information (PHI) for treatment or patient care

1. With other caregivers involved in care

2. With a patient's personal representative
   - Legal Guardian
   - Agent designated by proxy (in active status)
   - Parent of a minor

3. As directed by a patient (designated contact, list of individuals, implied consent)

Nursing ABC's

Treatment

4. With patient's caregivers as needed to take care of the patient

5. With family/caregiver searching for a missing or unidentified patient, as needed to care for patient

Nursing ABC's

Operations – you may use or disclose information (PHI) for routine hospital operations

1. For hospital operations within the scope of your responsibility (e.g. supervisor's oversight)

Nursing ABC's

Other Disclosures – you may use or disclose information (PHI)

1. In response to a patient's signed authorization to release information

2. As mandated by law (reporting immunizations, etc.)

Organization for Economic Cooperation and Development

- Headquartered in Paris
- 30 Member Nations
- Economic Policies
- www.oecd.org

MANHATTAN COLLEGE

Guidelines for the Security of Information Systems and Networks

- Economic Importance of Security
- Legal & Ethical Concerns Over Security
- Increased us of Networks
- Physical & Logical Security

MANHATTAN COLLEGE

1. AWARENESS

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

- Required Management Action: Promulgate Policies & Support Staff
- Possible Measurement: Existence of Statements & Publicity

2. RESPONSIBILITY

All participants are responsible for the security of information systems and networks.

- Required Management Actions: Assign Responsibilities and Authority

- Possible Measurement: Job Descriptions and Systems/Network Managers

3. RESPONSE

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

- Required Management Actions: Required Reporting on Breaches of Security

- Possible Measurement: Reports and Help Desk Actions

4. ETHICS
Participants should respect the legitimate interests of others.

- Required Management Action: Organizational Codes of Conduct
- Possible Measurement:
  - Existence of Codes
  - Training
  - Enforcement

5. DEMOCRACY

The security of information systems and networks should be compatible with essential values of a democratic society.

- Required Management Action: Statements on the rights of Individuals
- Possible Measurement: Guidance on Information Flows and Decision Making

6. RISK ASSESSMENT
Participants should conduct risk assessments.

- Required Management Action: Reviews of Systems Risks
- Possible Measurement: Audit and Quality Control Functions

7. SECURITY DESIGN AND IMPLEMENTATION

Participants should incorporate security as an essential element of information systems and networks.

- Required Management Action: Systems Development Life Cycle Methodology
- Possible Measurement: Budgets and Plans That Reflect SDLC

8. SECURITY MANAGEMENT

Participants should adopt a comprehensive approach to security management.

- Required Management Action: Established Security Policies
- Possible Measurement: Policy Statements and Assignment of Responsibilities

9. REASSESSMENT

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

- Required Management Action: Review of Plans and Results
- Possible Measurement:

  Continuous Improvement

Content Validation Study

Measuring the Culture of Security in Healthcare
Measuring the Culture of Security in Healthcare Information Systems, Nursing in a Technological World, Conference Handbook, Queensland University of Technology, Brisbane, Australia, p. 93. June 2003 *

* Collaborating Partners:

Elmhurst Hospital Center & NewYork Medical College (USA)

MANHATTAN COLLEGE

Content Validation Study

Expert Rating Forms

following four point scale:

1. = not relevant
2. = unable to assess relevance without item revision
3. = relevant but needs minor alteration
4. = very relevant and succinct

MANHATTAN COLLEGE

Content Validation Study

Average scores for each statement ranged from a high of 4.0 to a low of 2.67. As a group, guidelines ranged from 3.31 to 3.56.

Content Validity Index (CVI):

The over-all CVI was .88

MANHATTAN COLLEGE

Scale # 1: Staff Self-Efficacy

The following questions ask how confident you are that actions you take to ensure the integrity of healthcare information systems will result in achieving the goals of a secure system. Acting to ensure the integrity of systems means things such as prescribe security procedures are followed and that breaches of security are reported and corrected. Please read each question and the circle the number that best describes how confident you are about what is being asked in the question.

	Circle one number on each line										
How confident are you that you can:	Not confident At all			Somewhat confident					Extremely confident		
1. Recognize and monitor constantly all the new technology because there are new security threats and vulnerabilities.	0	1	2	3	4	5	6	7	8	9	10

Scale # 2 Management Self-Efficacy

The following questions ask how confident you are that you can assist your staff to ensure the integrity of healthcare information systems will result in achieving the goals of a secure system. Acting to ensure the integrity of systems means things such as prescribe security procedures are followed and that breaches of security are reported and corrected. Please read each question and the circle the number that best describes how confident you are about what is being asked in the question.

	Circle one number on each line										
How confident are you that you can assist your staff to:	Not confident At all			Somewhat confident					Extremely confident		
1. Recognize and monitor constantly all the new technology because there are new security threats and vulnerabilities.	0	1	2	3	4	5	6	7	8	9	10

Scale # 3 Attitudes & Values

The following questions ask you to express your personal view of the level of support by the health care organization towards the security of its information systems. Concern for computer security means things like raising awareness, assigning responsibilities and reporting problems when you or others become aware of them. Please read each question and then circle the number that best describes how you feel about what is being asked in the question.

	Circle one number on each line										
Do you feel that in your health care organization:	Strongly Disagree			Agree					Strongly Agree		
1.People in the organization recognize that with all new technology there is a need for constant monitoring of new security threats and vulnerabilities.	0	1	2	3	4	5	6	7	8	9	10

Site # 1-Characteristics

- Westchester, NY-suburban/rural area
- 120 licensed beds-Acute care facility
- 700 employees/300 in nursing services
- NURSING STAFF
  - 58% BS
  - 30% hold national certification in specialty
- About to embark on new information system venture for clinical documentation

Descriptive Statistics

All Female	Age	Years in Health Care	Subjects
Managers	47	23.8	8
Staff	45.9	22.1	16
Combined	46.3	22.7	24

Instrument Reliability Cronbach's Alpha

Instrument	Self-Efficacy	Attitudes & Values
Managers	.98	.98
Staff	.97	.97
Combined	.97	.97

Attitudes & Values Scores

	Mean	Standard Deviation
Managers	7.07	1.82
Staff	6.78	1.54
Combined	6.88	1.61

Self-Efficacy Scores

	Mean	Standard Deviation
Managers	7.43	1.83
Staff	6.79	1.63
Combined	7.01	1.69

Correlations Within Groups
Attitudes & Values x Self-Efficacy

	r	Sign.
Managers	.51	.04
Staff	.87	.005
Combined	.65	.001

Correlations
Staff x Managers

	r	Sign.
Self-Efficacy	.13	n/s
Attitudes & Values	-.07	n/s

Appreciative Inquiry

- Begun by David Cooperrider in 1980's at Case Western Reserve University
- Positive Organizational Scholarship
- Four Phases: *Inquire, Imagine, Innovate & Implement*
- Problem Solving

Cooperrider, D.L., & Whitney, D. (1999). *Appreciate Inquiry.* San Francisco: Berrett-Koehler

MANHATTAN COLLEGE

Qualitative Validation of Self-Efficacy Scale

- Ranked self-efficacy items from highest to lowest means
- Placed top five and lowest five items on an open-ended interview guide
- Scheduled focus groups with nursing staff users and managers
- Two researchers conducted focus gr
  - One served as interviewer
  - One served as recorder

Focus Group with Staff Users

- Shared the interview guide with the focus group members
- Questions
  - What do you think contributed to these positive results?
  - What do you think contributed to these lower results?
- Themes for Positive Results
  - Open communications
  - Participatory involvement in planning
  - Trust
- Themes for Lower Results
  - Access to Assistance
    - Limited staffing in IT Department
    - Not available on weekends
    - Limited access to key people

Focus Group with Nursing Managers

- Focus group has not been held yet
- Will share the interview guide with the focus group members
- Questions
  - What do you think contributed to these positive results?
  - What do you think contributed to these lower results?
- Themes will be derived from the analysis
  - Search for organizational strong points
  - Examine weak results
- Feedback will be provided the participants
- Used in developing action plans

150 MANHATTAN COLLEGE
LASALLIAN EDUCATION
Celebrating 150 Years of Excellence

Further Validation of Scales

- Planned as part of Information Technology Security Self-Efficacy Enhancing Program Grant
- Interviews with key stakeholders
- Focus Groups
  - Staff across User Departments
  - I.T. Staff
  - Mangers across Departments
- Self-Efficacy Enhancing Learning
- Ongoing Assessment of Program