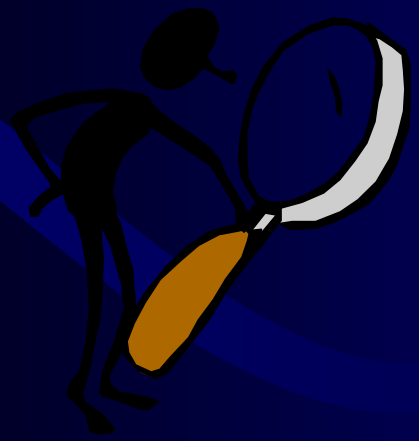
# 4.04: Preparing for Preparing for a JCAHO Survey of a Hospital's HIPAA Privacy and Security Compliance Program

Leslie C. Bender, Esq.
General Counsel & Privacy Officer
roiWebEd Company
Principal, Leslie C. Bender, PA
Timonium, MD

Cathy Casagrande
Director of Health Information Management and Privacy
Frederick Memorial Health System
Frederick, MD



# JCAHO's Mission

The Mission of the Joint Commission on Accreditation of Healthcare Organizations is -

- **t**o continuously improve the safety and quality of care provided to the public through the provision of health care accreditation and related services that support performance improvement in health care organizations.
- www.jcaho.org

# JCAHO's Objectives

- The Joint Commission evaluates and accredits more than 16,000 health care organizations and programs in the United States.
- An independent, not-for-profit organization, JCAHO is the nation's predominant standards-setting and accrediting body in health care.
- Since 1951, JCAHO has developed state-of-the-art, professionally based standards and evaluated the compliance of health care organizations against these benchmarks.

# JCAHO's Standards vs. HIPAA

- JCAHO's standards are broader than HIPAA's and cover all types of patient information
- JCAHO's standards blend what HIPAA separates into Privacy Standards and Security Standards
- JCAHO's standards and elements of performance cover broader categories than individual standards or implementation specifications in HIPAA
- JCAHO surveys "Confidentiality and Security" under the heading of "Information Management" – which will allow them to assess your HIPAA compliance program and reality

# JCAHO Survey

- The new survey starts with a self-assessment grid to score your compliance
- Self-assessment grid
  - a.k.a. Scoring Grid
  - Not required
  - Tool for self-assessment

# Scoring

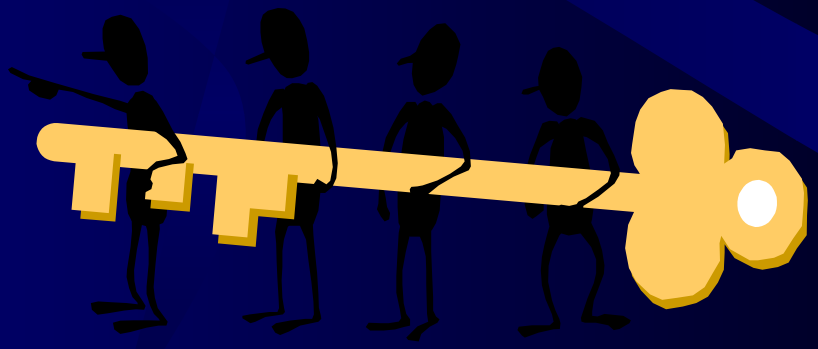
- Hospitals are scored against Standards
- Score:
  - ❑ Compliant
  - ❑ Not Compliant
- Accreditation decisions are based on simple counts of standards scored “not compliant”

# Key Measure

- Elements of performance (EPs)
- Evaluated on the following scale:
  - 0 Insufficient compliance
  - 1 Partial compliance
  - 2 Satisfactory compliance
  - NA Not applicable
- Measure of success:
  - Quantifiable measure that can be used to determine whether an action has been effective and is being sustained

# Scoring

- *Key Points*
  - Compliance with each element of performance (EP)
  - Three scoring criterion categories
    - A – structural requirement (i.e., policies, plans)
    - B – structural or process requirements
    - C - Number of times your organization does or does not meet a particular EP



# Scoring

Track Record of Achievements

| Score | | Initial Survey | Full Survey |
|---|---|---|---|
| 2 | 90-100 | 4 months or more | 12 months or more |
| 1 | 80-89 | 2 to 3 months | 6 to 11 months |
| 0 | < 80 | < 2 months | < 6 months |

# JCAHO Standards on Confidentiality and Security

- Standard IM.2.10 "Information privacy and confidentiality are maintained."
- JCAHO defines –
  - privacy as "an individual's right to limit the disclosure of personal information" and
  - confidentiality as "the safekeeping of data/information so as to restrict access to individuals who have need, reason, and permission for such access."

# IM.2.10 Elements of Performance

- 9 elements of Performance for IM.2.10 including:
  - Developed written processes based on and consistent with applicable laws addressing privacy and confidentiality
  - Policies have been effectively communicated to staff
  - Effective processes for enforcing policy
  - Monitor compliance with the policy
  - Use monitoring results for improving privacy and confidentiality
  - Patients are aware of uses and disclosures that may or will be made
  - Removal of identifiers encouraged
  - PHI is used for purposes identified to patients or as required by law and not further disclosed without patient authorization
  - Hospital preserves confidentiality of information and “requires extraordinary means to preserve patient privacy”k

# IM.2.20

- JCAHO IM.2.20 "Information security, including data integrity, is maintained."

# IM.2.20 Elements of Performance

- 7 Elements of Performance including:
  - Developed written process based on and consistent with applicable law that addresses information security, including data integrity
  - Effective communication of policy, and any changes, to applicable staff
  - Effective process for enforcing the policy
  - Monitors compliance with policy
  - Monitoring results and technology developments used to improve information security, including data integrity
  - Develops and implements controls to safeguard data and information, including the clinical record, against loss, destruction, and tampering (controls on next slide)
  - Policies and procedures, including plans for implementation and for electronic information systems, address: data integrity, authentication, non-repudiation, encryption as warranted, and auditability, as appropriate to the system and types of information, e.g., patient information and billing information

# IM.2.20 – "Controls" in Element of Performance 6

- JCAHO lists the following controls for safeguarding data and information:
  - Developing and implementing policies when removal of records is permitted
  - Protecting data and information against unauthorized intrusion, corruption or damage
  - Preventing falsification of data and information
  - Developing and implementing guidelines to prevent the destruction of records
  - Developing and implementing guidelines for destroying copies of records
  - Protecting records in a manner that minimizes the possibility of damage from fire and water

# IM.2.30

- JCAHO IM.2.30 "The hospital has a process for maintaining continuity of information."

# IM.2.30 Elements of Performance

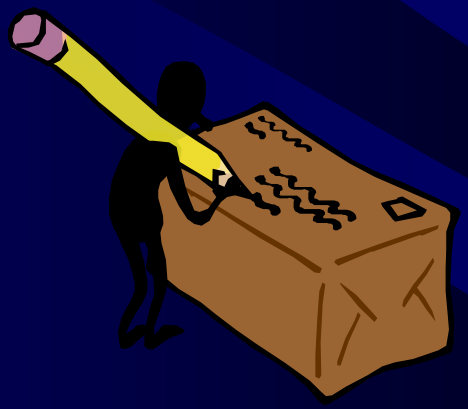
- 3 Elements of Performance for IM.2.30 including the following:
  - Business continuity/disaster recovery plan
  - Periodic testing to ensure business interruption backup techniques are effective
  - Electronic systems – business continuity/disaster recovery plan addresses the following:
    - Plans for scheduled/unscheduled interruptions, including end user training
    - Contingency procedures
    - Plans for minimal interruptions during scheduled downtime
    - Emergency service plan
    - Back up system
    - Data retrieval – including from storage and information presently in active systems

# Information Management Processes

- JCAHO's standards related to Information Management Processes dovetail with the HIPAA Security Standards and are intended to assess how well a hospital assures the integrity, confidentiality and availability of patients' information.

# IM.3.10

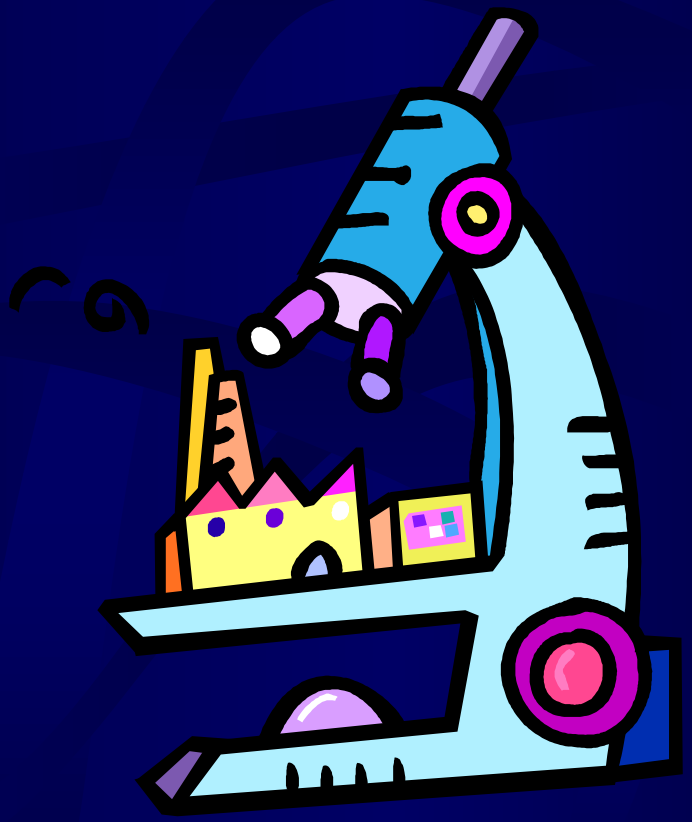
- The hospital has processes in place to effectively manage information, including the capturing, reporting, processing, storing, retrieving, disseminating, and displaying of clinical/service and non-clinical data and information.



# IM.3.10 Elements of Performance

- 3 Elements of Performance including:
  - Uniform data definitions and data capture methods
    - Minimum data sets, terminology definitions, classifications, vocabulary, and standardized nomenclature
    - Industry standards are used when possible
  - Abbreviations, acronyms, and symbols are standardized throughout the hospital and there is a “don’t use” list
  - Quality control systems are used to monitor data content and collection activities
    - Method used assures timely and economical data collection with the degree of accuracy, completeness, and discrimination necessary for their intended use

# The JCAHO Survey



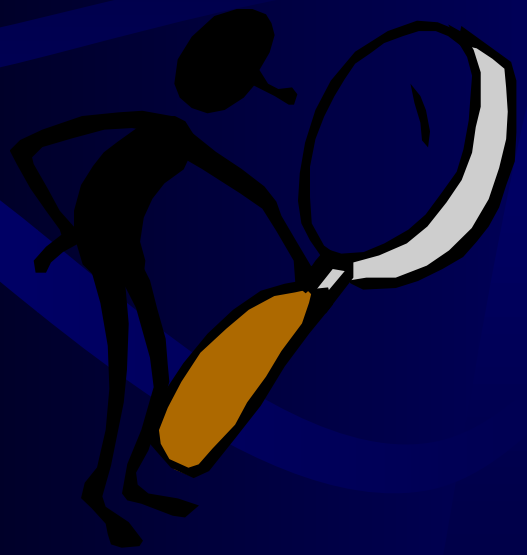
# JCAHO Survey

- Tuesday Afternoon – Friday Morning

»Tracers!

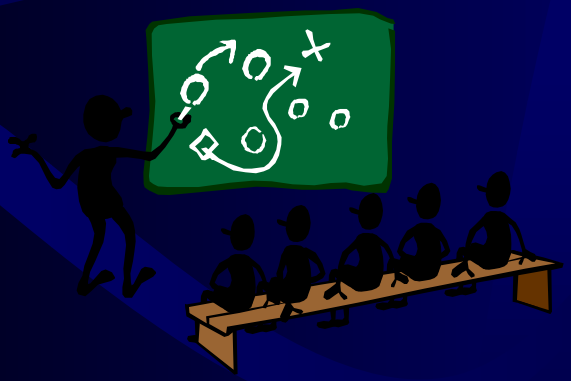
»Tracers!

»Tracers!



# Tracer Methodology

- Medical Record drives the survey
- Based on priority focus areas and clinical service groups (top DRG's)
- Identified by picking from lists for the surveyor during the survey
- Follow or “trace” the “patient” throughout the system

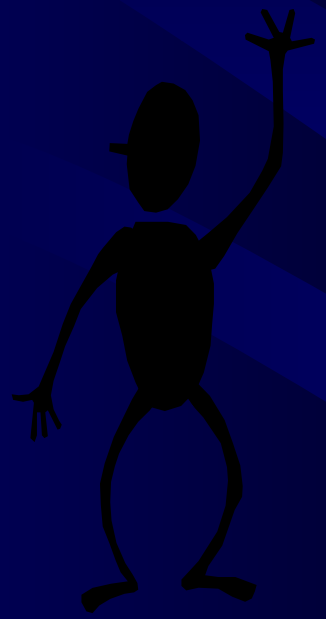


# JCAHO's Priority Focus Areas

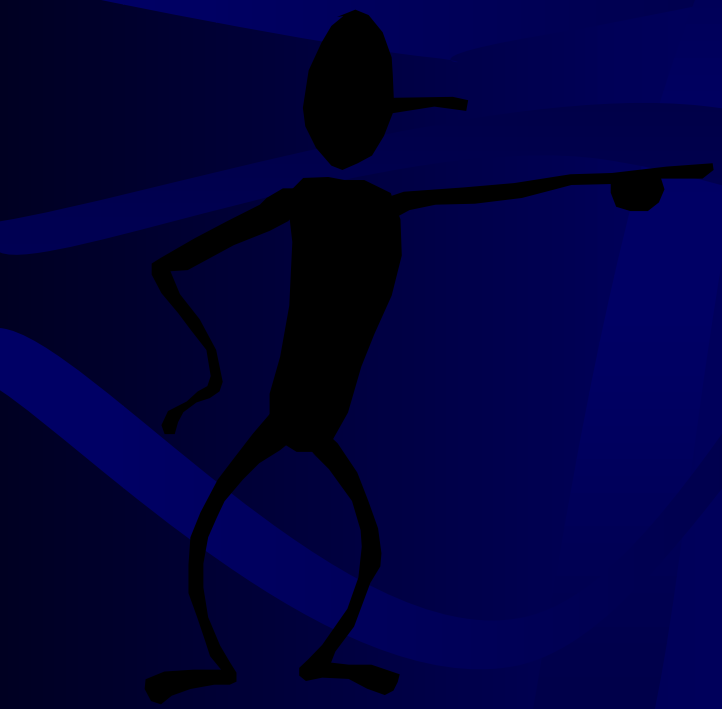
- Analytical procedures
- Communications
- Credentialed and Privileged Practitioners
- Equipment use
- Infection Control
- Information Management
- Organization Structure
- Orientation and Training
- Physical Environment
- QI Expertise and Activity
- Patient Safety
- Staffing

# Examples of Hospital Top DRG's

- Obstetrics
- Normal Newborns
- General Medicine
- Gastroenterology
- Orthopedics
- General Surgery



# JCAHO Guidance for Completing the Grid



- Sample size – JCAHO recommended sample sizes -
  - 30 cases for population size of 100
  - 50 cases for population size of 101 to 500
  - 70 cases for population of size of more than 500

# JCAHO Grid

| Standard/Element | Compliant Standard | Scoring Criterion Category (A,B,C) | Element Score (2) | Element Score (1) | Element Score (0) | Measure of Success | Rate of FMH Compliance | Needs Measure - None at present | Comments |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.10 Privacy & Confidentiality* | C | | | | | | | | |
| EP 1 written process to address confidentiality | | B | 2 | | | HIPAA P/P's. ROI Web. | | | |
| EP 2 effective communication of privacy policy | | B | 2 | | | Compliance w/HIPAA ed; MOX, Pulsebeat, posters. ROI Web inc p/p's. | | 93% | Student affiliations include HIPAA |
| EP 3effective process for enforcing policy | | C | 2 | | | Audits by IM2 Cmte. HP262, HR510 | | 93% | Audits completed monthly - Education, Jackons, Respond Quarterly trend |
| EP 4 monitors compliance w/hosp policy | | C | 2 | | | Audits by IM2 Cmte. HP262 | | 90% | Audit follow-up require documentation copy to show completion |
| EP 5 use monitoring and IT to improve privacy | | C | 2 | | | Fax, Meditech. | | 90% | Wireless reg & other devices bring device to patient. Also add PIN project Live in 60 days |
| EP 6 individuals informed of PHI uses and disclosures | | C | 2 | | | Privacy Notice | | 93% | Monthly report of compliance of signed acknowledgements of NOP |
| EP 7 deidentifies encouraged | | B | 2 | | | Reports to HSCRC, Premier, research protocols | | | Need to assess research data abstraction. Some ID included (Premier, diabetes, others) BA agreement |
| EP 8 PHI disclosed as described, req'd by law, or w/auth | | C | | 1 | | P/P | | | ...ing of disclosures. 30 charts reviewed mont... Tool to assess knowledge of acct. |
| EP 9 sensitive data | | C | 2 | | | Conf. data flag/PCI. | | | |
| *IM.2.20 Information Security* | C | | | | | | | | |
| EP 1 written process for info security and data integrity | | B | 2 | | | IT policies | | | |
| EP 2 policy effectively communicated to staff | | B | 2 | | | EMR training. Double-key logon. MOX, Pulsebeat | | | |
| EP 3 effective process for enforcement | | C | 2 | | | Access diminished. ID check to issue password. | | | Project started to improve this process. Data avail after 1/6/04 (live date). |
| EP 4 monitors compliance w/hosp policy | | C | 2 | | | Meditech backup logs. Weekly system integrity checks | | | Weekly Integrity checks, Trends documented, Help Desk is tracking |
| EP 5 use monitoring and IT to improve security | | C | 2 | | | System timeouts; Symbol locks Controlled access to data cente | | | |
| EP 6 controls to safeguard data | | B | 2 | | | Audit per user and device | | | |
| EP 7 p/p address listed items | | C | 2 | | | EMR p/p's. Data is archived. Au... trails. Amendments only. | | | |
| *IM.2.30 Continuity of Information* | C | | | | | | | | |
| EP 1disaster recovery plan | | B | 2 | | | | | | |
| EP 2 disaster rec plan tested periodically | | B | 2 | | | | | | |
| EP 3 plans for sched and unsched electronic downtime | | B | 2 | | | | | | |


| Standard/Element | Compliant Standard | Scoring Criterion Category (A,B,C) | Element Score (2) | Element Score (1) | Element Score (0) | Measure of Success | Rate of FMH Compliance | Needs Measure - None at present | Comments |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.10 Privacy & Confidentiality* | C | | | | | | | | |
| EP 1 written process to address confidentiality | | B | 2 | | | HIPAA P/P's. ROI Web. | | | |
| EP 2 effective communication of privacy policy | | B | 2 | | | Compliance w/HIPAA ed; MOX, Pulsebeat, posters. ROI Web inc p/p's. | | 93% | Student affiliations include HIPAA |

# JCAHO Privacy and Confidentiality

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.10 Privacy & Confidentiality* | C | | | | | | | | |
| EP 1 written process to address confidentiality | | B | 2 | | | HIPAA P/P's. ROI Web. | | | |
| EP 2 effective communication of privacy policy | | B | 2 | | | Compliance w/HIPAA ed; MOX, Pulsebeat, posters. ROI Web inc p/p's. | | 93% | Student affiliations include HIPAA |
| EP 3effective process for enforcing policy | | C | 2 | | | Audits by IM2 Cmte. HP252, HR510 | | 93% | Audits completed monthly - Education, Jackons, Respond Quarterly trend |
| EP 4 monitors compliance w/hosp policy | | C | 2 | | | Audits by IM2 Cmte. HP252 | | 90% | Audit follow-up require documentation copy to show completion |

# JCAHO Privacy and Confidentiality

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.10 Privacy & Confidentiality* | C | | | | | | | | |
| EP 5 use monitoring and IT to improve privacy | | C | 2 | | | Fax, Meditech. | | 90% | Wireless reg & other devices bring device to patient. Also add PIN project Live in 60 days |
| EP 6 individuals informed of PHI uses and disclosures | | C | 2 | | | Privacy Notice | | 93% | Monthly report of compliance of signed acknowledgements of NOP |
| EP 7 deidentifies encouraged | | B | 2 | | | Reports to HSCRC, Premier, research protocols | | | Need to assess research data abstraction. Some ID included (Premier, diabetes, others) BA agreement |
| EP 8 PHI disclosed as described, req'd by law, or w/auth | | C | | 1 | | P/P | | | Accting of disclosures. 30 charts reviewed monthly. Tool to assess knowledge of acct. |
| EP 9 sensitive data | | C | 2 | | | Conf. data flag/PCI. | | | |

# JCAHO Information Security

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.20 Information Security* | C | | | | | | | | |
| EP 1 written process for info security and data integrity | | B | 2 | | | IT policies | | | |
| EP 2 policy effectively communicated to staff | | B | 2 | | | EMR training. Double-key logon. MOX, Pulsebeat | | | |
| EP 3 effective process for enforcement | | C | 2 | | | Access diminished. ID check to issue password. | | | Project started to improve this process. Data avail after 1/6/04 (live date). |

# JCAHO Information Security

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.20 Information Security* | C | | | | | | | | |
| EP 4 monitors compliance w/hosp policy | | C | 2 | | | Meditech backup logs. Weekly system integrity checks | | | Weekly Integrity checks, Trends documented, Help Desk is tracking |
| EP 5 use monitoring and IT to improve security | | C | 2 | | | System timeouts; Symbol lockouts. Controlled access to data center | | 90% | Enhanced intrusion detection for network coming. CISCO follow-up |
| EP 6 controls to safeguard data | | B | 2 | | | Audit per user and device | | | Double-key. Wireless encryption. Firewall. Network access request process. Inc HH/H |
| EP 7 p/p address listed items | | C | 2 | | | EMR p/p's. Data is archived. Audit trails. Amendments only. | | | Phys portal w/digital certificates for encryption. |

# Continuity of Information

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *IM.2.30 Continuity of Information* | C | | | | | | | | |
| EP 1disaster recovery plan | | B | 2 | | | | | | Disaster Rec Plan. Ranked critical systems, prioritized for recovery |
| EP 2 disaster rec plan tested periodically | | B | 2 | | | | | | Backups tested. Trending started. |
| EP 3 plans for sched and unsched electronic downtime | | B | 2 | | | | | | Going to more redundant system. Use off shifts as sched downtimes. SAN solution |

# Conclusions and Recommendations

- Even if your survey is not imminent, JCAHO's grid may be a valuable tool for QI or other purposes to evaluate internally how well your program is designed and is actually working
- Having your supporting materials well organized and readily available will not only assist you in meeting JCAHO's needs but will help you meet the extensive documentation requirements within HIPAA's privacy and security standards (note that the Security Standards do require hospitals to perform a self-assessment and to build, enhance, repair, or recreate a compliance program around the results)

# Thank you.