

## Auditing for Privacy Compliance:

### A Case Study

September 13, 2004

*Baltimore, MD*

**Mariann Yeager, MBA**

**Emerson Strategic Group, Inc.**

703.519.0817 tel

703.623.1924 cel

[myeager@emersonsg.com](mailto:myeager@emersonsg.com)

[www.emersonsg.com](http://www.emersonsg.com)



# WEDI SNIP Audit White Paper

## Auditing for Privacy Compliance

---

### Purpose

- **Share strategies for organizing audit program**
- **Discussing various approaches given size and complexity of organization**
- **Build framework that adapts to change**

### Scope

- **Auditing compliance with HIPAA Privacy policies and procedures**
- **Safeguards – §164.530(c)**

**<http://www.wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/P-Auditingv10.pdf>**



# WEDi SNIP White Paper

## Auditing for Privacy Compliance

---

What is an Audit?

Why Audit?

Audit Process

- **Structuring an audit program**
- **Who should conduct the audit**
- **Audit team**
- **Avoiding Pitfalls**
- **Don't forget buy-in**
- **What to Audit**
- **How frequently**

Audit Methodology

- **Blind or informed audit**
- **Self-audit tool**
- **Physical walkthrough**
- **Interviews**
- **Checklist or scorecard**
- **Output samples**

Auditing Results

- **Packaging the Results**
- **Who should hear the results**
- **Handling violations and non-compliance**



# Auditing for Privacy Compliance

## A Case Study

# Case Study

---

- Covered Entity Profile
- HIPAA Implementation Efforts
- Audit Objectives
- Audit Methodology
- Identified Issues
- Recommendations

# Covered Entity Profile

---

- Plastic Surgery Practice Plan = Covered Entity
  - **Separate legal entity from School of Medicine**
  - **Sub-specialty within Surgery**
  - **Each practice Administrator responsible for P&L, operations, compliance, etc.**
  - **Will migrate into one CE with other surgery groups within next 6 months - 2 years**
- Numerous locations
- Some research (handful of studies)
- Primarily OHCA within hospital / clinics
  - **Facility, Reception, Nurse Manager, Nurses and Billing Staff are generally hospital**
- Some separate non-OHCA locations

# HIPAA Implementation Efforts

---

- Administrator = Privacy Official
- Accountable to Surgery Administrator and School Compliance Office
- Diligent Implementation Effort:
  - **Used automated tool - assessment and template policies and procedures (P&P)**
  - **Detailed review with nurses, researchers and medical secretaries**
  - **Tailored P&P to their workflow**
  - **General awareness training by School of Medicine and hospitals**
  - **Additional functional training within practice plan**
  - **Good documentation**
  - **Thoughtful implementation**



# Audit Objectives

---

- Assess how they are doing:
  - **Are their day-to-day practices compliant?**
  - **Is the HIPAA manual adequate?**
- Identify risks and exposure
- Use objective third party
- Identify changes and improvements
- Determine what they can do to keep compliance effort on track
- Ensure they are making the most of existing investment in compliance





# Audit Methodology

---

- Review documentation
  - **Forms, policies and procedures, Notice, Accounting, etc.**
- Conduct visual walk through
  - **Safeguards, logistics and processes**
- Conduct interviews with key people
- Complete Questionnaire
- Covers all privacy rule requirements
- Document key findings and recommendations in summary report
- Review with Administrator and Compliance Office

# Environmental Factors

- Shadow charts stored in Administrative Offices
- Door open – but in restricted area across from Administrator's office
- Transported to/from clinic by Medical Secretary
- Safeguarding carts key



Records Room

# Environmental Factors

- Staffed by hospital employees in OHCA locations
- Reliance on Hospital Notice/ Acknowledgement
- Patient Rights requests generally handled by clinic staff vs. Plastic Surgery staff



Patient Check-In

# Environmental Factors

- Staffed by hospital employees in OHCA locations
- Carts used to transport records
- Open area
- Incidental disclosures common
- Training key



Medical Secretary Work  
Area

# Environmental Factors

- Staffed by practice plan employees
- Schedule follow up appointments
- Backs up to check in desk
- Shared fax and printer
- OHCA in its truest sense



Outpatient Checkout



# Identified Issues

---

1. Other covered entities in OHCA sometimes non-responsive in resolving issues
2. No procedures for verifying identity – particularly over the phone
3. No procedures for mitigation in the event of a breach
4. Authorizations missing key elements
5. Not documenting accounting of disclosures
  - **Disclosures made by physicians to Health Dept., Professional Boards, abuse, etc.**
  - **Patient authorization in all other instances**





## Identified Issues - Cont.

---

6. Unsure whether non-OHCA locations are properly documenting Notice Acknowledgement
7. Develop routine training for existing workforce
8. Lack of understanding of de-identification
9. Not tracking whether there are individual requests – e.g. restrictions on uses and disclosures of PHI



# Recommendations

---

1. Develop procedures for documenting disclosures (e.g. Health Dept., Professional Boards, abuse, etc.)
2. Develop checklist to verify that authorizations supplied by other parties contain all required elements
3. Develop procedures for verifying identity and mitigation
4. Train staff - escalating issues with OHCA hospitals and on new procedures and provide routine training (e.g. reminders, FAQs, etc.)





## Identified Issues - Cont.

---

5. Establish regular monitoring activities:
  - Verify that non-OHCA locations are properly documenting Notice Acknowledgement
  - Tracking whether patients are exercising their requests
  - Verifying that procedures are being followed

## Auditing for Privacy Compliance:

### A Case Study

September 13, 2004

*Baltimore, MD*

**Mariann Yeager, MBA**

**Emerson Strategic Group, Inc.**

703.519.0817 tel

703.623.1924 cel

[myeager@emersonsg.com](mailto:myeager@emersonsg.com)

[www.emersonsg.com](http://www.emersonsg.com)