



CaroMont Health

**7 Strategies for a Successful Patient Privacy
Monitoring & Compliance Program
22nd National HIPAA Summit**

Shallie J. Bryant
Deputy Privacy & Security Officer



About CaroMont Health

- We are a nationally recognized leader and valued partner in promoting individual health and vibrant communities
 - 3,800 employees
 - 452 medical staff
 - 268 volunteers
- Gaston Memorial Hospital, 435 beds
- CaroMont Medical Group, a network of 45 primary & specialty physician offices in 5 counties and 2 states
- Courtland Terrace, 96 bed skilled nursing facility
- Gaston Hospice

Proactive vs. Reactive

- What is your current environment?
- Understand the organizational workflow
 - **Employee responsibility**
 - Framework of system
- Understand what types of activity to monitor
 - Fire drill vs. the real thing
 - Policies & procedures?
 - NOPP?
 - Inappropriate access – snooping?



Privacy Program - Structure

Compliance Program Structure

- Standards & Policies
- Training & Education
- Auditing & Monitoring
- Reporting
- Response & Prevention
- Enforcement & Discipline
- Compliance Officer

Privacy Program Structure

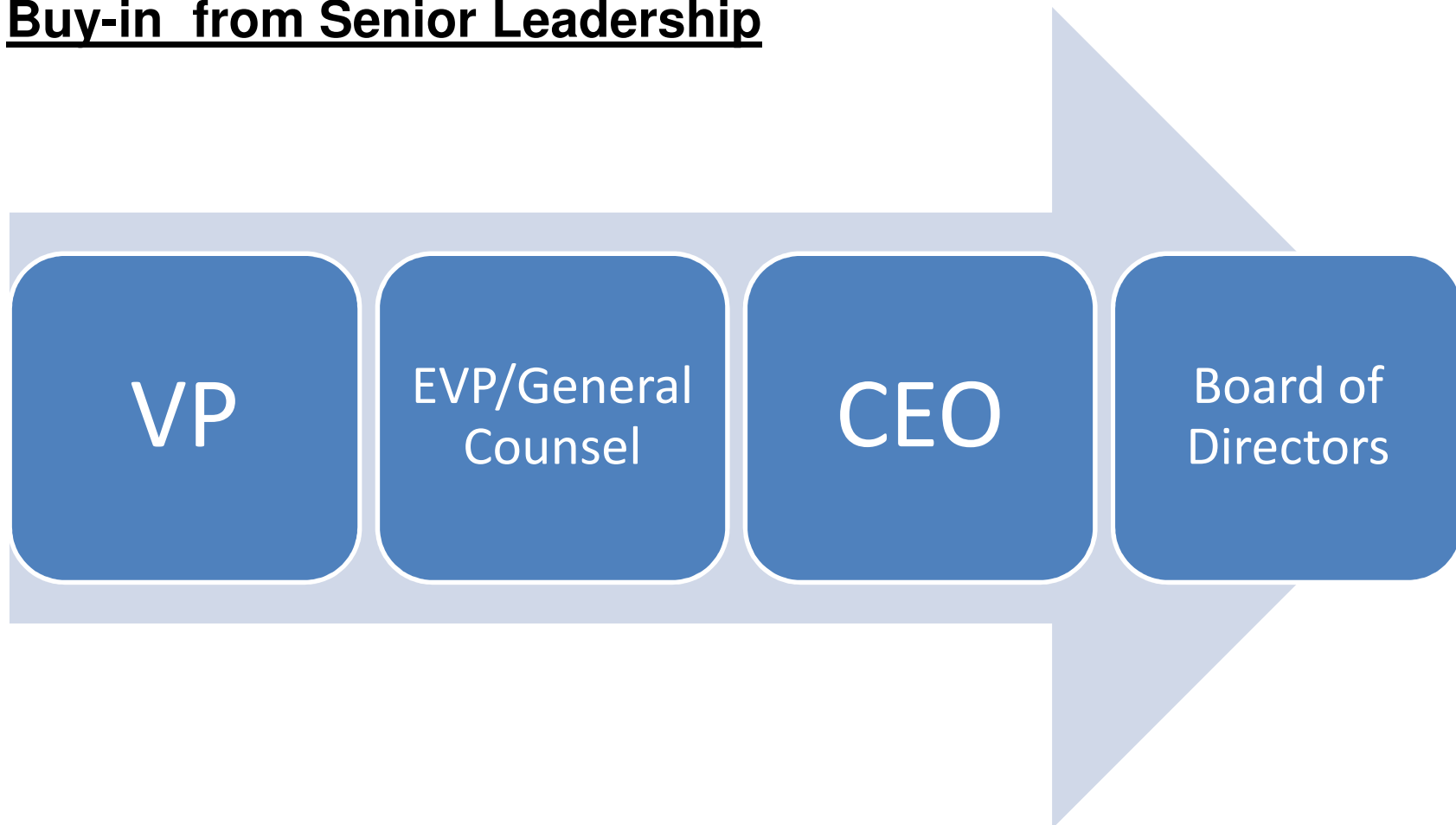
- Policies & Procedures
- Process to Receive Complaints
- Mitigation of Harmful Effects
- Safeguards to Protect Privacy
- Training & Education
 - Training Workforce

Key Points

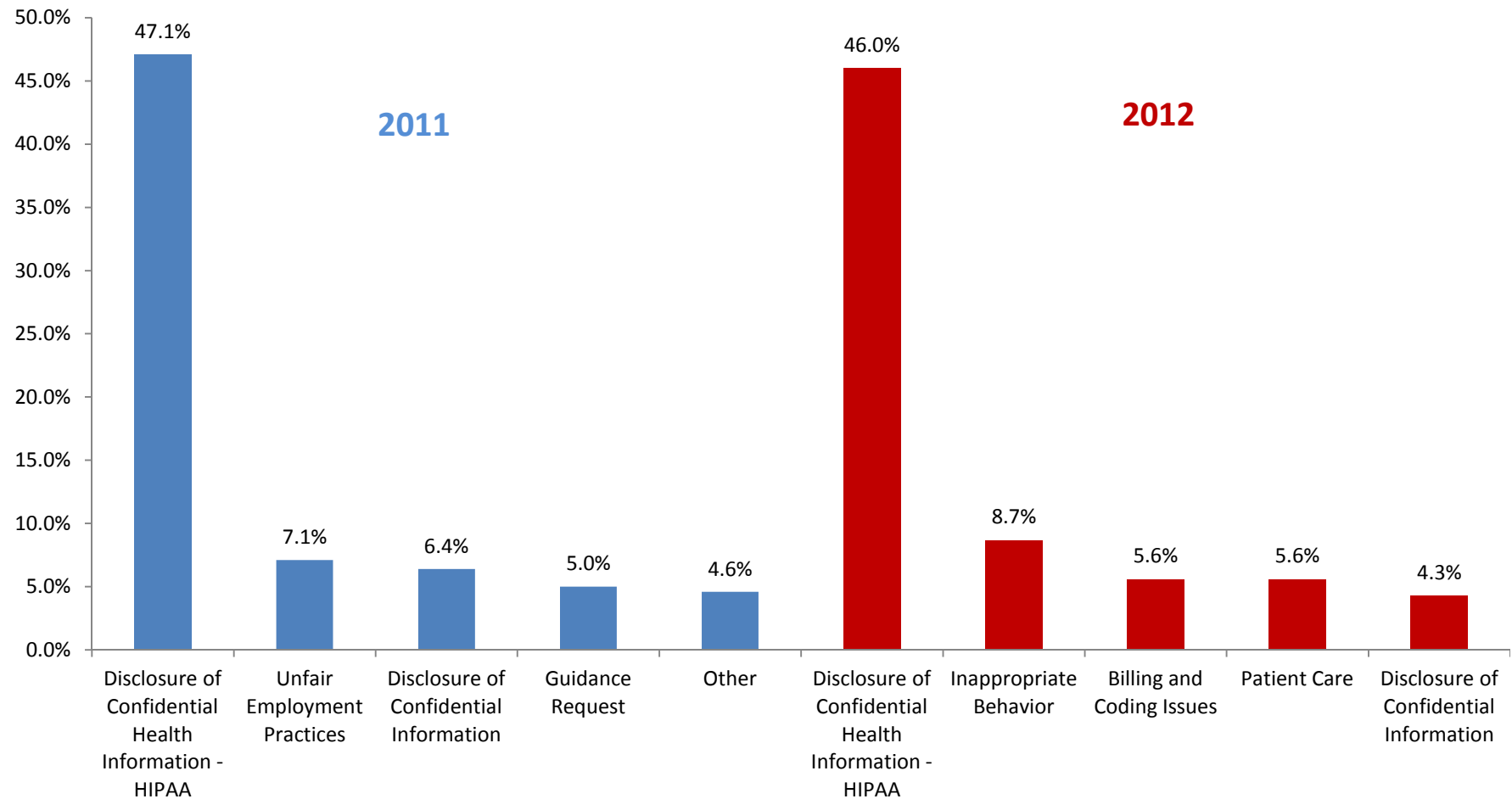
- How is your organization identified under HIPAA?
- CaroMont Health = Affiliated Covered Entity
 - Single Notice of Privacy Practices
 - Centralized Governance Structure
 - Standard
 - Training & education
 - Investigation & response
 - Disciplinary actions consistent across the organization

Strengths

Buy-in from Senior Leadership



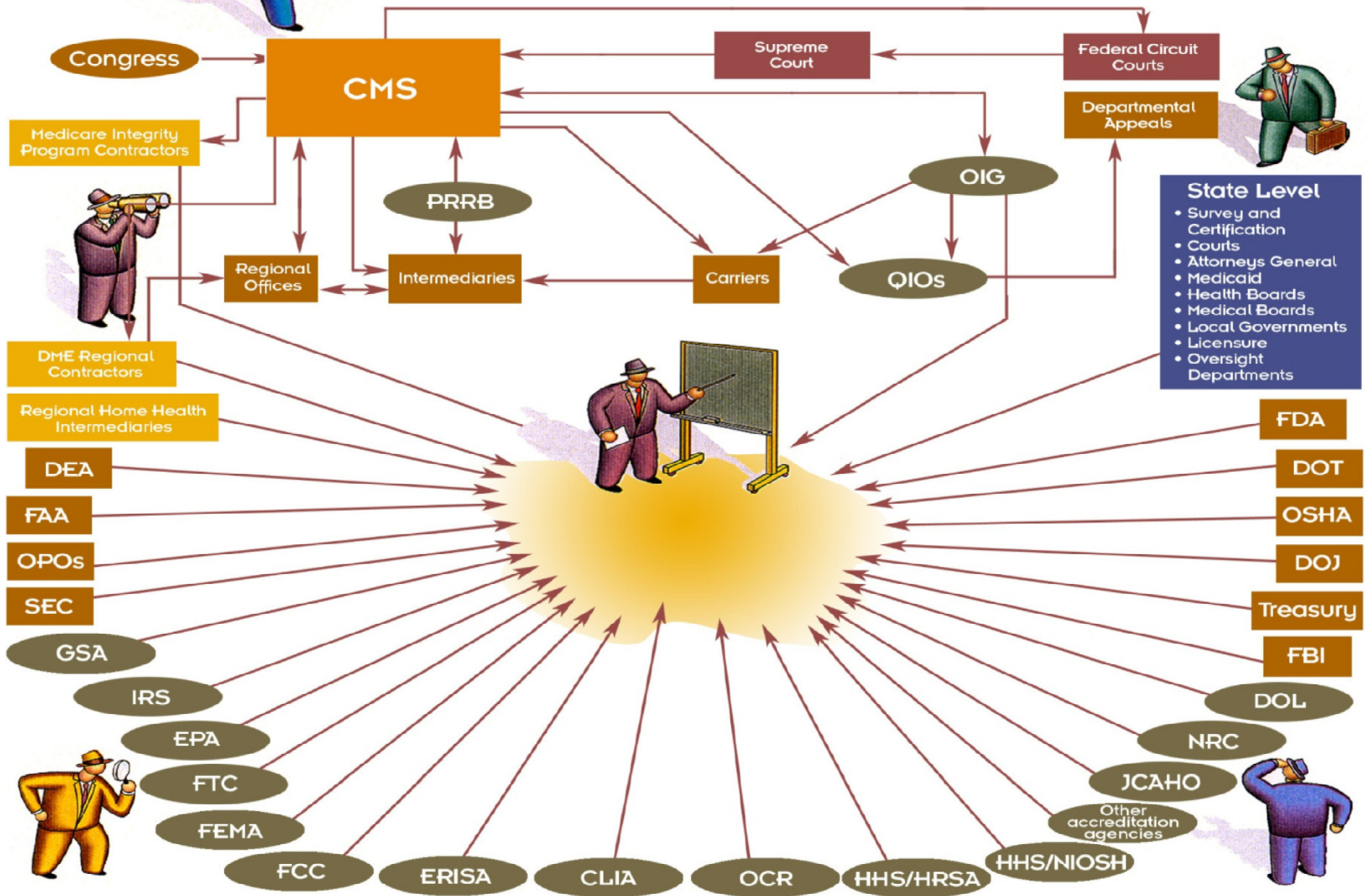
Benchmark Past Reports



Weaknesses

- Limited Staff
- Absence of Privacy Culture
- Lack of Privacy Program Infrastructure
- No sense of Privacy – Multiple Areas of Risk
 - Small town (*everybody* is a family member or friend)

Oversight of the Health Care Industry



Opportunities (cont.)

Top OCR Privacy Issues

- Impermissible uses & disclosures
- Lack of safeguards
- Failure to provide access to individual
- Use & disclosure of more than minimum necessary
- Failure to provide NOPP
www.hhs.gov/ocr/privacy

Top CaroMont Privacy Issues

- Impermissible uses & disclosures
 - **Fax, mail, voicemail containing PHI disclosed to the wrong patients**
 - **Snooping**
- Lack of safeguards

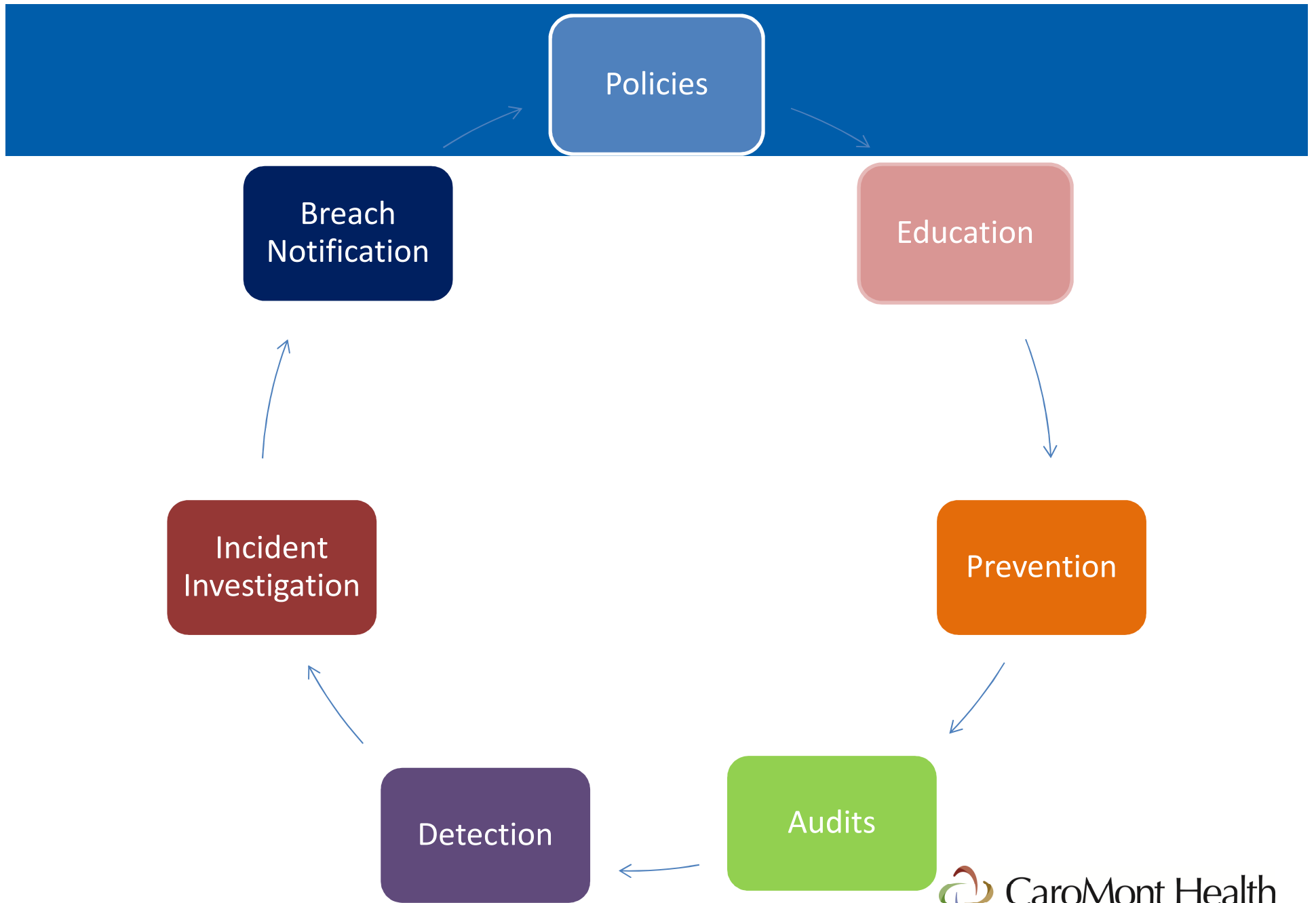
Potential Threats

- Privacy & Security violations getting more media attention
 - Local newspaper across the street from hospital
- Erosion of patient trust and reputational harm
- Budget constraints
 - Do more with less!
- Enforcement Landscape
 - The Omnibus HIPAA HITECH Final Rule
 - \$50, 000 HIPAA Breach settlement involving less than 500 patients
 - Provider settles HIPAA case for \$1.5 million for potential violation

Primary Analysis

- **Assessment of our privacy compliance program at CaroMont Health revealed:**
 1. More focus needed to be placed on education and awareness
 - Who to contact for privacy issues/guidance
 2. HIPAA privacy policies
 - Revise our NOPP
 3. Occurrence reporting
 4. Proactive clinical system auditing & monitoring

7 Strategies for a Successful Patient Monitoring & Compliance Program



Policies

- **Create? Revise? Update?**

Policies that follow industry standards and fit the need of your organization, big or small.

- Code of Conduct
- Breach Notification Policy
- Notice of Privacy Practices Requirements
- User Confidentiality Policy /Agreement
- Taking Photographs and Making Recording/Audio of Patients
- Protecting PHI of High-Profile Patients

 CaroMont Health Administrative Policy	Number:	159.00
	Effective Date:	5/27/99
	Revised:	11/2010, 12
	Author:	Mike Johns
	Approved:	Doug Lucki
	Authorized	Doug Lucki

Email Usage

POLICY

Rules and guidelines exist which govern the use, access and disclosure of electronic mail messages created, sent, or received by CaroMont Health employees.

PURPOSE

To ensure the proper and effective use of the corporate email system.

RESPONSIBILITY/SCOPE

Each employee who uses the email system is responsible for knowing and complying with this email policy.

PROCEDURE/GUIDELINES

- The email system hardware is the property of CaroMont Health. Additionally, all messages composed, sent, or received on the email system are and remain the property of the company. They are not the private property of any employee.
- The use of the electronic mail system is intended for the conduct of company business. However, incidental or infrequent personal use of email is permitted.
- The electronic mail system is not to be used to create any disruptive or harassing messages. Among those which are considered disruptive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses

someone's age, race, sexual orientation, religious or political beliefs, national origin or disability.

- The electronic mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
- In order to protect the security of confidential information sent via email over the internet, employees should use the "secure mail:" feature of Groupwise. To use this feature, user should enter "Secure Mail:" as the first part of the subject of the message.
- CaroMont Health reserves and intends to exercise the right to review, audit, intercept, access, and disclose to the proper authorities all messages created, received, or sent over the electronic mail system for any purpose. The contents of electronic mail properly obtained for legitimate business purposes may be disclosed within CaroMont Health to the proper authorities without the permission of the employee.
- The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.
- Notwithstanding the company's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees should not attempt to gain access to another employee's messages without the latter's permission.
- Any employee who discovers a violation of this policy shall notify the Chief Information Officer/AVP or their supervisor.
- CaroMont Health will comply with court subpoenas requesting access to company email.
- Any employee who violates this policy or uses the electronic mail system for improper purposes shall be subject to disciplinary action, up to and including termination of employment.
- Employee must not use email to erode the productivity of other staff members – examples include chain letters and solicitations.

Education & Awareness Initiatives

- Education, training, and awareness are essential to an effective compliance program
- We have created an organization-wide, systematic approach that includes:
 - Compliance training at general corporate orientation
 - Dedicated intranet page
 - Two articles in our monthly PR/Marketing publication
 - Celebration of corporate compliance & ethics week

Awareness Initiatives - Orientation

- Opportunity to discuss compliance with all new workforce members including:
 - Employees
 - Providers
 - Volunteers
 - Students
- This venue allows for instruction directly from corporate responsibility department staff

Awareness Initiatives - Orientation

- **The presentation includes information about the:**
 - Corporate responsibility program at CaroMont Health
 - HIPAA/Privacy
 - Social media guidelines
 - Compliance scenarios/video clips
 - Q & A's
 - [Compliance Babies](#)

Different Methods for Delivering Messages

Celebration of Corporate Compliance & Ethics Week

“Are you Smarter than a Privacy Expert?”

Display Board game where each player selected their questions off the display board and had to answer the privacy scenarios



Education & Training

- CBLs - Computer-Based Modules
- Be visible
- In person training
 - Privacy Marathon – 30 minute live session once a month
 - Created to meet the need of employees (what they need to know to do their jobs)
- Newsletters
- HIPAA privacy & security basics
 - Who Xs two
 - Snooping guideline
 - Social media usage

Newsletter –CaroMont Connections

CAROMONT

c o n n e c t i o n s

MONTHLY COMMUNICATIONS

FAMILY, FRIENDS INVOLVED IN T

Certain disclosures are permitted. These include disclosures to family members or friends.

If the patient objects, then we are not permitted to disclose the information to the patient's family or friends.

HEALTHCARE PROVIDERS MAY G

- 1) A family member or relative
- 2) A personal friend of the patient
- 3) Any other person identified by the patient

BEFORE DISCLOSING, HEALTHCARE PROVIDERS MUST

If the individual has capacity to make decisions, the healthcare provider must:

- 1) Obtain the individual's agreement
- 2) Provide the individual with the information in a understandable manner. Note: To "inform" means to provide information to the individual in a way that the individual can understand and use to make a decision. This includes providing information about the patient's condition, the proposed treatment, and the risks and benefits of the treatment.

IF PERMITTED, THE DISCLOSURE MUST BE

- 1) Purposes directly related to the patient's care
- 2) Purposes related to payment or business operations
- 3) To notify, assist in notifying, or arrange for the care of the patient

SPECIAL RULE IF PATIENT LACKS CAPACITY

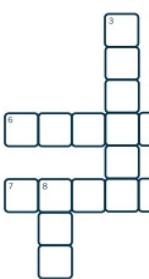
If the individual does not have capacity to make decisions, the healthcare provider may disclose the information to the patient's family or friends if:

- 1) The disclosure is in the patient's best interests
- 2) Disclose only the information necessary for the family or friend to understand the patient's condition and the proposed treatment
- 3) To notify, assist in notifying, or arrange for the care of the patient

Stay tuned for next month's HIPAA TIP. If you have any questions, please contact the Privacy Office at 704.834.2895.

CORPORATE RESPONSIBILITY

This month's Corporate Responsibility crossword puzzle is available in the newsletter. The puzzle is a fun way to learn more about CaroMont Connections and the resources, can be found in the newsletter. The puzzle is a fun way to learn more about your crossword puzzle (www.caromont.com) or interface mail newsletter. Good luck!



ACROSS

- 2 Set of rules outlining proper practices for
- 5 Health Insurance
- 6 An examination of
- 7 Last name of CaroMont
- 9 Where policies can

HIPAA TIPS: FAXING COMMON MISTAKES

The Privacy Rule requires that covered health care providers communicating with patients by phone, fax, mail, or email must take appropriate use or disclosure. These safeguards are designed to protect the privacy of PHI.

Scenario examples:

1. When faxing PHI to a number that is not regularly confirmed by the fax number with the intended recipient.
2. When verbally discussing PHI with another provider without safeguarding the information by lowering his or her voice.

Occasionally, patients become concerned about their particular medical condition, or is being treated by a healthcare provider. As a general rule, we recommend the following guidelines:

- Never send postcards or folded cards which contain PHI.
- Always send sealed envelopes.
- Try to limit information on the exterior of the envelope. Use professional judgment when indicating a potential treatment condition or name.
- Always address envelopes to the specific patient.

It is always permissible to:

1. Contact a patient directly by phone to discuss PHI.
2. It is always permissible to leave a voicemail in the household.

However, certain principles apply and must always be followed:

- Verification of the patient's identity is necessary. This includes the patient's name, birth date, and last date of service.
- When leaving a voicemail or message with a family member, use a number to return your call.
- If the patient is unable to answer and a family member is calling from the facility name and either a name or address is requested, determine why the patient is unable to answer and use professional judgment to determine if it is appropriate to disclose the "minimum necessary" information.
- Physician-to-patient, e-mail, communications, or other electronic communications should be secured with encryption.
- The Health Information Portability and Accountability Act (HIPAA) via unsecured network. The communication should be via another secure method.

For any questions or comments, email shalle.bryant@caromont.com

HIPAA TIPS: FAXING BEST PRACTICES FOR SENDING AND RECEIVING

As health care professionals, we frequently use the fax machine to transmit confidential business information and Protected Health Information (PHI). We sometimes forget best practices we have learned during training and our legal duty under HIPAA on steps to properly safeguard PHI—including using fax machines to send or receive patient information.

The HIPAA Privacy Rule permits physicians and other health care professionals to disclose PHI to another health care provider for treatment purposes. However, we must have in place reasonable and appropriate safeguards to protect the privacy of PHI that is disclosed using a fax machine.

Faxing Basics 101

1. Your fax machine should be located in a secure location, where unauthorized individuals cannot see sent/received fax information.
2. Use a standardized fax cover sheet that:
 - a. Identifies the sender, recipient, number of pages, date and time the fax is sent.
 - b. Includes a confidentiality statement and information about what to do if it is received in error.

Before sending the fax:

1. Confirm the number you have for the recipient is correct.
2. Confirm in the display window that you dialed the number correctly.
3. Confirm any pre-programmed numbers are correct.

If you send a fax to the wrong number:

1. Notify your manager and the Corporate Responsibility Office immediately! Changes in the HIPAA Privacy & Security Rule greatly enhance a patient's privacy protections and strengthens the government's ability to enforce the law.
2. The potential breach can be investigated quickly and appropriate actions can be taken on reporting and notification.
3. Attempt to retrieve all copies of the fax or ensure that the recipient has destroyed the information in the fax.

Protecting patient information is the responsibility of all CaroMont Health employees and business associates. To better protect the security of confidential fax transmissions, please follow the above. For more information, contact the Corporate Responsibility Office at 704.834.2895. Stay tuned for next month's HIPAA TIPS where we will discuss other methods of communicating with patients.

last PAGE

last PAGE

last PAGE

last PAGE

CaroMont Health

next PAGE

Prevention

- Proactive Review of clinical system
- VIP Record Lockdown
 - Employee
 - Board
 - Sr. Leadership
- **Audit Alerts**
- Education and Awareness
- Audits Protocol
- Disciplinary Action



ERROR: stackunderflow
OFFENDING COMMAND: ~

STACK: