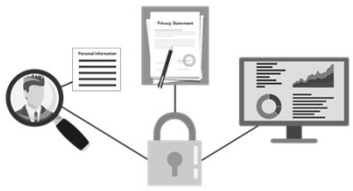
Auditing the Trifecta:

Compliance ⇔ Privacy ⇔ Security

Presented By:
Debi Weatherford, Executive Director Internal Audit, Piedmont Healthcare
Debra Muscio, SVP, Chief Audit, ERM, Privacy, Security, Ethics & Compliance Officer, Community Medical Centers



1

1

Agenda

- About our Organizations
- Auditing the Trifecta: Compliance, Privacy, Security
- Comments and Questions

2

2

About Piedmont Healthcare

Piedmont HEALTHCARE 3

3

About Piedmont

Atlanta 1905 (1957 location)

Fayette 1997

Mountainside 2004

Newnan 2006

Henry 2012

Newton 2015

Athens Regional 2016

Rockdale 2017

Columbus Regional Midtown & Northside Campuses 2018

Walton 2018

4

Who We Are

Healthcare marked by compassion and sustainable excellence in a progressive environment, guided by physicians, delivered by exceptional professionals, and inspired by the communities we serve. Piedmont is a not-for-profit, community health system comprised of the following entities:

- Piedmont Athens Regional
- Piedmont Atlanta Hospital
- Piedmont Columbus Regional
- Piedmont Fayette Hospital
- Piedmont Henry Hospital
- Piedmont Mountainside Hospital
- Piedmont Newnan Hospital
- Piedmont Newton Hospital
- Piedmont Rockdale Hospital
- Piedmont Walton Hospital
- Piedmont Heart Institute
- Piedmont Physicians
- Piedmont Clinic
- Piedmont Healthcare Foundation

11 HOSPITALS	2000+ CLINICALLY INTEGRATED PHYSICIANS	22,000 EMPLOYEES	550+ PIEDMONT CLINIC PRACTICE LOCATIONS	24 URGENT CARE LOCATIONS	28 RETAIL CLINICS

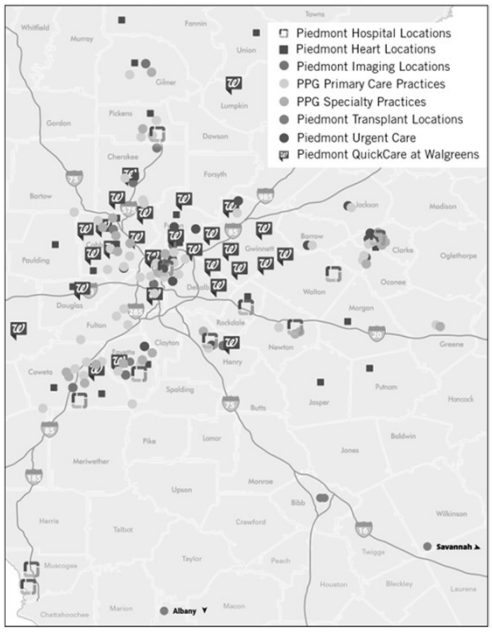
Piedmont provides a wide variety of services including, but not limited to:

- Heart
- Cancer
- Transplant
- Primary Care
- Neurology
- Women's Services
- Brain Tumor
- Urology
- Emergency
- Bariatrics
- Breast Health
- Diabetes
- Imaging
- Orthopaedic
- Rehabilitation
- Respiratory
- Robotic Surgery
- Sixty Plus Older Adult
- Sleep
- Spine
- Surgical
- Urgent Care
- Wound Care and Hyperbaric

5

About Piedmont

- Founded in 1905 by two physicians
- Areas of clinical expertise include: cancer, heart, neuroscience, transplant and women's services
- Serves the metro Atlanta area as well as communities in Fayette, Coweta, Henry, Newton, Pickens, Clarke, Rockdale, Walton, Muscogee (and surrounding) counties
- Named to AJC's List of Top Work Places, 2016, 2017 & 2018
- AlwaySafe program: systemwide safety behaviors and prevention tools
- Epic: industry-leading EMR and practice management system provides better care by facilitating quality improvements and enhances the patient experience



6

About Community Medical Centers

Private, not-for-profit, locally-owned – $199 million in community benefit outreach

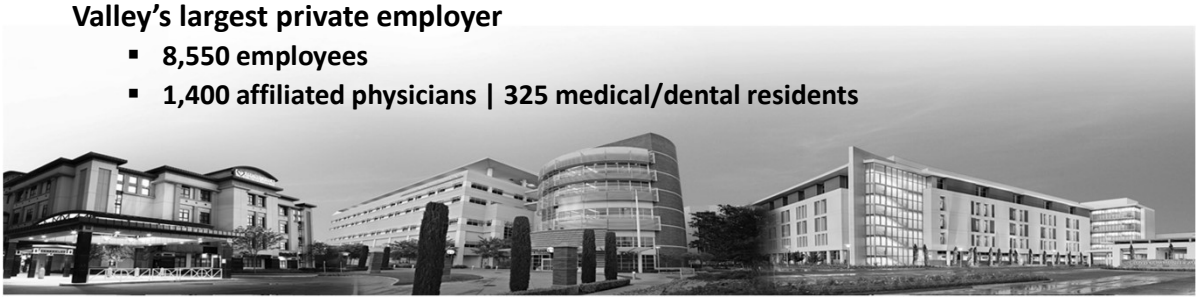
40+ years UCSF partnership on graduate medical education

Largest healthcare provider in California's central San Joaquin Valley

- **1,129 licensed beds** in 3 hospitals, inpatient behavioral health hospital and subacute care center
- **179,452 ER visits | 55,726 admissions | 9,621 babies born** last year

Valley's largest private employer

- **8,550 employees**
- **1,400 affiliated physicians | 325 medical/dental residents**



7

7

Serving 15,000-square-mile region

- ❑ **Only Level 1 trauma and comprehensive burn center** between Los Angeles and San Francisco
- ❑ **Level 3 NICU and high-risk birthing center** serves 5-county region

with unique health challenges

- ❑ **Concentrated poverty** – more than 35% of children live in poverty
- ❑ **100+ languages spoken,** 43% adults don't speak English well
- ❑ **Higher than California average rates for obesity, diabetes, lung disease and asthma**
- ❑ **48% of population on Medi-Cal (Medicaid)**
- ❑ **10% of Fresno County babies born premature** – higher than some third-world countries
- ❑ **Lowest doctor-to-patient ratios in California**

8

8

Community Medical Centers highlights

- Founded in 1897 when doctors joined with successful boarding house
- Becker's *Top 150 Places to Work in Healthcare* list & Advisory Board's *Workplace of the Year* 3x
- 3-year Health Ethics Trust certification for our compliance and ethics
- GetWell Network's national Leadership and Overall Achievement Awards
- Epic EMR integration throughout CMC, connecting more than 1,000 private physicians in region
- 9 consecutive Healthgrades' Outstanding Patient Experience Awards to Fresno Heart & Surgical
- 3 consecutive Beacon Awards for Critical Care Nursing
- Top Performer Distinctions on Key Quality Measures by the Joint Commission for two hospitals & Advanced Stroke certification for another hospital
- Among 2 of 5 hospitals in California with Perinatal Certification for best practices and outcomes for mothers and babies

9

Community Medical Centers Facilities & Affiliations

Fresno Heart & Surgical Hospital

Community Regional Medical Center

Clovis Community Medical Center

Community Subacute & Transitional Care Center

UCSF Benioff Children's Hospitals

Community Behavioral Health Center

Community Cancer Institute

10

10

Remember Your Shared Goals

What can compliance, privacy, security, and legal teams do to build an effective incident response program that is consistent and is developed as a collaborative effort between their respective teams?

Here are a few places to start……. And how to audit them

11

11

Remember Your Shared Goals

- Compliance
- Privacy
- Security
- Legal
- Risk Management
- Internal Audit

- Roles do not have mutually exclusive areas of influence or responsibility.
- How is the shared burden of risk management, issue evaluation and incident response addressed, monitored and evaluated?

12

12

Remember Your Shared Goals

- Part of building a more collaborative atmosphere starts with understanding one another's roles and main focus.

Each of these perspectives together round out a full view of regulatory compliance.

- Understanding legal risks, implementing privacy policies and procedures, safeguarding data and applying the appropriate controls for that data – each are critical aspects of a strong program.

13

13

Compliance

Compliance Hot Topics for Today:

- Conflicts of Interest
- Devicemaker-Doctor Relationships
- Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers
- Privacy
- Security

14

14

Conflicts of Interest

Board directors are the first-line defense against avoiding conflicts of interest.

It's important for board directors to be trained on the types of situations that could be considered conflicts of interest and situations that could give the appearance of a conflict of interest. Board directors also need education about how the organization evaluates a conflict of interest and how best to manage it.

The whole board is ultimately responsible for providing oversight for conflicts of interest. They should be diligent about identifying and handling conflicts of interest.

15

15

Conflicts of Interest

16

16

Conflicts of Interest

Best practices that boards can follow to ensure proper management of conflicts of interest:

- Enlist the help of a disinterested party to perform a confidential review of current conflict of interest policies and procedures.
- Share findings of the review with the board.
- Use the review as an educational opportunity to learn more about handling conflicts of interest.
- Update your current conflict of interest policies and procedures.
- Set up a process for the board chair to handle conflict of interest matters and for a staff member who is responsible as part of their duties to perform the administrative functions involving conflict of interest policies and procedures, such as following up on the submission of conflict of interest forms where information is missing, inaccurate or incomplete.
- Staff should follow procedures implicitly so that directors don't feel singled out.

17

17

Conflicts of Interest
Audits and Targeted Reviews

A technique for internal audit to consider is random and targeted reviews of travel and entertainment expenses, especially in high-volume areas and high-risk departments. These may uncover suspicious spending that indicates a possible conflict. Expense reports can also suggest potential conflicts of interest. Surveying vendors and suppliers can reveal situations where a disgruntled contractor or prospective seller believes a competitor has been unfairly favored. Continual monitoring can help identify red flags and highlight risk areas for more focused review.

There are tools available to the internal auditor to support the company's management of related-party transactions and conflicts of interest. More frequently, we see the use of analytic technology emerging as a tool to detect potential conflicts of interests. A data match can be performed between employee and vendor data files to identify relationships that suggest possible conflicts and control weaknesses. The matching would look for employees and vendors with the same address, tax ID number, or bank account.

18

18

Devicemaker - Doctor Relationships

U.S. Justice Department intervened in a whistleblower suit against Life Spine for allegedly paying kickbacks in the form of consulting fees, royalties and intellectual property acquisition fees to induce physicians to use the manufacturer's spinal implants, devices and equipment.

Source: Modern Healthcare Vol. 49/No.33

19

19

Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers

Many organizations utilize Automated Clearing House (ACH), an electronic funds transfer system that facilitates payments in the United States. The process relies on the accuracy of the ACH Direct Deposit Authorization Form to transfer payments to each vendor.

- Are your controls effective to detect an impersonator that requests a change to the ACH Direct Deposit Authorization Form?
- Are controls in place to prevent wire transfers requested by an unauthorized individual?

20

20

Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers
Internal Control Questionnaire

1. Do you have documented policies and procedures that address ACH payments and wire transfers?
2. Is a process in place to verify and validate not only requested changes in the electronic funds transfer system, but also any related accounts?
3. How are requests for and actual changes to wire transfers handled?
4. Who has access to make a wire transfer? How is this access monitored and managed?
5. How is the ACH Direct Deposit Authorization Form independently verified?
6. How are Treasury and Accounts Payable involved in new vendor setup and changes to vendors details?
7. What mechanism is in place to notify Accounts Payable and Finance leadership of changes to vendor records?

21

21

Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers
Internal Control Questionnaire

8. Are you independently verifying the ACH Direct Deposit Authorization Form with a "known" contact at the requesting company? If so, how is this documented and where is the documentary evidence maintained?
9. Do you require a bank letter, and independently verify the validity of the letter with the bank? If so, how is this documented and where is the documentary evidence maintained?
10. Is prenoting of the account implemented, and validation with the known contact conducted? An ACH prenote is a financial transaction with a $0.01 value submitted via the ACH network. Its purpose is to validate the banking information before committing the funds to transfer.
11. Where are all verification documents maintained and housed?
12. Is a routine vendor notification implemented to alert stakeholders of changes to vendor records?
13. What monitoring is in place to review rejected payments and vendor accounts to effectively track required payments and rejected payments? What is the communication protocol regarding these rejected payments?

22

22

Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers
Internal Control Questionnaire

14. Are you checking on a daily basis to review notifications –
    - When the funds were returned or the account closed?
    - When the banking information changed?
15. What are your insurance coverage limits if an inappropriate payment is made as a result of a request from an impostor? Do you have additional approval of changes that are equal to or exceed this amount?
16. What escalation parameters and actions are to be taken when suspected inappropriate activities are found? Who is on the Incident Response Team?

23

23

Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers
Internal Control Questionnaire

17. Do you have a documented Social Engineering Fraud Incident Response Plan? A social engineering fraud is a confidence scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information provided to the employee in a written or verbal communication such as an email, fax, letter or even a phone call.

    a) How are these groups involved:
        i. Information Security
        ii. Finance
        iii. Legal
        iv. Risk Management
        v. Compliance
        vi. Internal Audit

24

24

Vendor Controls for Automated Clearing House (ACH) Payments and Wire Transfers
Internal Control Questionnaire

b) How are these events handled:

i. Responsibility for internal investigation of events surrounding any incident

ii. Notification of FBI, Secret Service or other Law Enforcement agencies

iii. Communication with impacted vendors, if any

iv. Communication with banking/financial partners

v. Notification of insurance carriers

vi. Preservation of physical or electronic evidence

25

25

Privacy

26

26

Privacy Act Change Repercussions

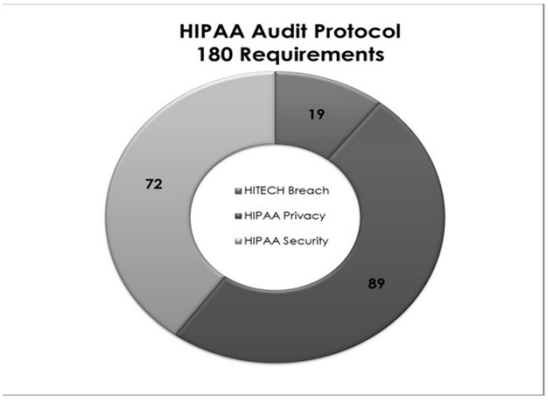
The California Consumer Privacy Act allows any consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with.

In addition, the California law allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach.

27

27

Auditing Privacy and Security



Top 10 violations that result in significant fines:

1. Database breaches
2. Third-party disclosure of PHI
3. Improper disposal of PHI
4. Mishandling medical records
5. Employees disclosing information
6. Not performing an organization-wide risk analysis
7. Employees legally accessing patient files
8. Lost or stolen devices
9. Lack of training
10. Not encrypting PHI on portable devices

To learn more about OCR's Phase 2 Audit program, visit website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

28

28

RULE

HIPAA Privacy Rule	HIPAA Security Rule	HIPAA Breach Notification Rule
• Sets national standards for when PHI may be used or disclosed • Gives individuals certain rights with respect to their PHI	• Includes standards that covered entities must implement to protect their electronic PHI (ePHI)	• Requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS) and, in some cases, the media, following a breach of unsecured PHI

29

29

Patient Rights and Covered Entity Responsibilities under Privacy Rule

Examples:

- General Privacy Compliance
- Notice of Privacy Practices
- Minimum Necessary
- Business Associates
- Appropriate Communications
- Media Relations
- Marketing
- Fundraising
- Research
- Security
- Authorizations
- Verbal Authorizations
- Required or Permitted Disclosures without Authorization
- Patient's Right of Access
- Patient's Right to Amend
- Patient's Right to Accounting
- Restriction Requests
- Psychotherapy Notes

30

30

Potential Privacy Breaches
(Examples)

1. Using Electronic Health Record (EHR) to keep track of medical problems and care of estranged family members.
2. Using the EHR to check on patients you used to care for, but are now discharged or moved to another floor.
3. Announcing a patient's name or diagnosis loudly in a lobby area.
4. Verbal disclosure of lab results to others who are interested, but who have no job related need to know.
5. Visiting a patient on a restricted unit, such as Maternity, without his/her permission.
6. Visiting a co-worker who is hospitalized, without his/her permission.
7. Borrowing someone's password to access records or lending someone your password.
8. Accessing a computer that is logged on under another's password.

31

31

Potential Privacy Breaches
(Examples cont.)

9. Disposing of anything with a patient's name on it in regular trash.
10. Mailing or giving Discharge Instructions or medications to the wrong patient.
11. Faxing PHI without a FAX COVER SHEET and/or to the wrong Fax number.
12. Accessing charts of ex-husbands or ex-girlfriends, etc., out of curiosity or concern, or to use in a custody battle.
13. Accessing a chart to see why a co-worker is in the emergency department.
14. Disclosing patient presence in the hospital after they had "opted out" of the facility's directory.
15. Leaving paper charts or census sheets open and unattended. Leaving PHI in the hall, restroom or library.
16. Talking about your patients in a public place like the cafeteria, hairdresser's or in a grocery store.

32

32

HIPAA Security vs. Privacy

- **Privacy rule** identifies what is to be protected and outlines the individual's rights to control access to their **Protected Health Information (PHI)**.
- **Security rule** requires Covered Entities (CE) to protect PHI in electronic form.
  - The security rule only applies to PHI maintained or transmitted in electronic form, called ePHI
- ***You can have security without privacy but you cannot have privacy without security.***

Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which US Department of Health and Human Services (HHS) has adopted standards.

33

33

Information Security – By Definition

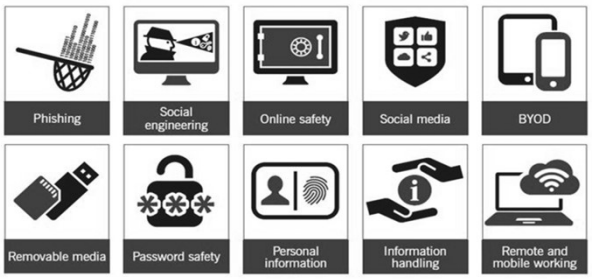
- Information Security is the process by which an organization protects information and its critical elements including the systems, media, and people, along with the facilities that process, store and transmit that information.
- In Healthcare: Enable and not disable empowerment of information for doctors and staff first.

34

34

Creating a Resilient Cyber Environment

Protecting everything is not only impractical it's financially not feasible for most organizations.



- Focus on the basics first.
  - Patch Management
  - Access Management
  - Valid Backups
  - Are existing logs being monitored on the Firewalls, Backups, Anti-virus reporting, CPU surges, others?
- What environment can be developed to withstand attack?

35

35

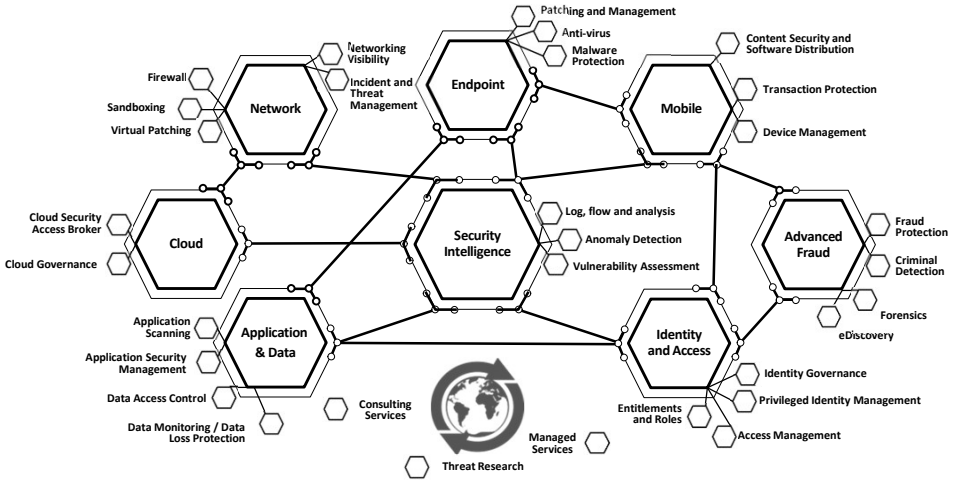
Knowing Your Cybersecurity Landscape

- Digital Eco-System
  - Thinking Locally and Globally
  - Sharing Threat Information in our community
  - We are electrons apart from bad actors not miles
- Understanding the existing Cybersecurity Portfolio
  - What are the Existing Protections?
  - Are the existing Cybersecurity Assets in a Healthy State?
  - What's missing from the Portfolio?

36

36

IT Security Portfolio – An Example



= Substantial solution in place and mature

= Solution or maturity at risk

= No substantial or mature solution in place

37

37

Security

- Create an Internal Control Questionnaire for vendor controls
- Access Provisioning – controls for badges, restricted areas, parking decks, software programs, conference call lines, WebEx
- Assembling and analyzing all security assessments that also impact disaster preparedness/business continuity – such as Epic Unplanned Outage Readiness (there is a need to cross-reference and map security assessments and risk assessments, as there is a lot of activity in different areas that affects this)

38

38

Security Rule Safeguards

Technical – controls around protecting information

Technical Safeguards
Technical Safeguards focus on the technology that protects PHI and controls access to it. The standards of the Security Rule do not require you to use specific technologies and are designed to be "technology neutral."

1. Access Control
2. Audit Controls
3. Integrity
4. Authentication
5. Transmission Security

Physical – secure location and backups

Physical Safeguards
Physical Safeguards are a set of rules and guidelines that focus on the physical access to PHI.

1. Facility Access Control
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Administrative – secure and appropriate granting and termination of access

Administrative Safeguards
Administrative Standards are a collection of policies and procedures that govern the conduct of the workforce and the security measures put in place to protect PHI.

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation of Business/Law Changes
9. BAA Contracts and Other Agreements

39

39

Information Security Compliance DOs and DON'Ts

- Don't be tricked into giving away confidential information
- Don't use an unprotected computer
- Do lock your computer and mobile device when not in use
- Do be vigilant and report suspicious activity
- Do password protect sensitive files and devices
- Do always use hard-to-guess passwords
- Do be cautious of suspicious emails and links
- Do not plug in personal devices like USB flash drives and smartphones
- Do not install or download unauthorized programs on work computer

40

40

Email Security

- **Phishing** – emails that falsely claim to be from a legitimate organization or source with malicious fraudulent intent.
  - If you receive a phishing email, DO NOT respond, instead delete the email immediately. **Conduct phishing exercises on employees to educate.**
- **Spam** – unsolicited, unwanted bulk or junk email.
  - This form of email has become a favorite of attackers attempting to draw in the unsuspecting victim. **Add an email header to alert that the email is from an external sender.**
- **Email Encryption**
  - When you transmit any ePHI or private information (sensitive or confidential) to and/or from a NON-Work email address, it MUST be manually encrypted.
  - Any email that has ePHI in an attachment, such as an Excel or Word file, also needs to have the attachment password protected before it is sent out.

41

41

Comments and Questions

42

42