21st Annual Compliance Institute – Breakout Session P22

Auditing Emerging Compliance Risk Areas

Presented by:

Debi Weatherford, Executive Director, Internal Audit
Piedmont Healthcare

Anthony Lesser, Senior Manager, Deloitte & Touche

slide 1

Agenda

• About our organizations
• Overview of emerging compliance audit issues
• Pharmacy and the 340B Drug Pricing Program
• Cybersecurity
• Provider-Based Services and Provider-Based Physician Billing
• Disaster Recovery and Business Continuity

slide 2

---

slide 3

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 Medical Center
- Piedmont Atlanta Hospital
- Piedmont Fayette Hospital
- Piedmont Henry Hospital
- Piedmont Mountainside Hospital
- Piedmont Newnan Hospital
- Piedmont Newton Hospital
- Piedmont Heart Institute
- Piedmont Physicians
- Piedmont Clinic
- Piedmont Healthcare Foundation

7 HOSPITALS	3,200+ MEDICAL STAFF	16,500+ EMPLOYEES	MORE THAN 190 PRIMARY CARE PHYSICIANS IN MORE THAN 40 OFFICES	177 SPECIALISTS IN 54 OFFICES

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

slide 4

About Piedmont

- Founded in 1905 by two physicians
- 1,218-bed health system
- 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 and Clarke (and surrounding) counties
- AlwaySafe program: systemwide safety behaviors and prevention tools to reduce the number of serious safety events
- Epic: industry-leading EMR and practice management system provides better care and enhances the patient experience

- Piedmont Hospital Locations
- Piedmont Heart Locations
- Piedmont Imaging Locations
- PPG Primary Care Practices
- PPG Specialty Practices
- Piedmont Transplant Locations
- Piedmont Urgent Care

slide 5

About Piedmont

Atlanta 1905 (1957 location)   Fayette 1997   Mountainside 2004

Newnan 2006   Henry 2012   Newton 2015

Athens Regional 2016

slide 6

About Deloitte

Deloitte LLP and its subsidiaries have approximately 225,400 professionals with a single focus: serving our clients and helping them solve their toughest problems. We work in four key business areas—audit, advisory, tax and consulting—but our real strength comes from combining the talents of those groups to address clients' needs. *Fortune* and *BusinessWeek* consistently rank our organization among the best places to work, which is good news for our talent and our clients alike. When the best people tackle the most compelling challenges, everyone wins.

A global organization

- Largest accounting firm in the world[1], with approximately 225,400[2] employees in 674 offices throughout the world[2]
- Fiscal Year 2015 revenues of $35.2 billion (USD)[3]
- Deloitte serves 93% of the 2015 Fortune 500 Global List

Consulting

Audit   Tax

Advisory

Leadership

- Deloitte ranked #1 globally in Consulting by Gartner (2014)[4]
- Deloitte ranked #1 globally, Security Consulting by Gartner (2014)[5]
- Deloitte named a global leader in Analytics by Gartner (2014)[6]
- Deloitte named the global leader in Mobility IT Strategy Consulting by Kennedy (2014)[7]
- Deloitte named a global leader in Talent Management Consulting by Kennedy (2014)[8]
- Deloitte named a Leader in Supply Chain Strategy and Planning by Kennedy (2014)[9]
- Deloitte named a global Leader in SAP Implementation Services by Gartner (2015)[10]
- Deloitte named a leader in IT Infrastructure Transformation Consulting by Kennedy(2015)[11]

About Deloitte's Healthcare Practice

Reach & Accolades

- ✓ Serve leading companies across the health care industry with an unparalleled "ecosystem" view
  - **90%** of the Fortune 500 Life Sciences & Health Care companies
  - **10** of the 10 largest Health Care systems
  - **9** of the 9 largest for-profit Health Care systems
  - **8** of the 10 largest Pharmacy Benefit Managers
  - **Leading** Health Care distributors around the world
- ✓ Ranked **#1** globally in Health Care Risk Consulting based on revenue and capabilities by Kennedy

About Our Practice

- ✓ Over **7,300** practitioners the Life Sciences and Health Care industry in over 90 countries
- ✓ Deloitte has several strategic services such as **Health Analytics Solutions** supporting Clinical, Operational, Revenue Cycle, Financial Performance, and Value Based Care Excellence, and the **Center for Health Solutions**, the research arm of Deloitte LLP that informs stakeholders in health care about emerging trends, challenges, and opportunities

Breadth of Offering

Strategy & Market Capture | M&A and Restructuring | Customer Insights | Health Care Reform | Process Assessment / Re-engineering | Shared Services, Finance & Cost Management

Thought Leadership

The value of patient experience

Health care consumer engagement: No "one-size-fits-all"

Enterprise Contact Center: A strategic opportunity for health care providers

Engaging with tomorrow's patients: The new health care customer

---

340B Practice Overview

Drug Manufacturer Assessment Knowledge

Deloitte has 7 accepted manufacturer audit work plans by the Office of Pharmacy Affairs (OPA) and maintains regular visibility into the 340B life sciences market.

340B Program Experience

Decades of combined experience in the 340B Program including:
- Implementation
- Assessment
- Remediation
- Growth and improvement

Breadth of Experience

A multitude of compliance services including:
- Compliance program development
- Program monitoring and analytics development
- Corrective action plan development
- Disclosures and repayments

Subject Matter Experts

Nationally recognized team of experts that routinely present at conferences and industry events throughout the country. Deloitte's Health Care practice was also ranked #1 by Kennedy Information, Forrester, and Modern Healthcare.

Expansive Compliance Services

A deep roster of experienced industry supply chain and regulatory and compliance specialists, many of whom are former 340B Program administrators, regulators or leaders in the health care provider and pharmacy space

Technical Capabilities

We represent some of the largest and complex healthcare organizations in the country. We have worked extensively with multiple electronic medical record systems, 340B software systems, and retail pharmacy chains. We understand the challenges affecting the 340B provider market

Emerging Compliance Audit Areas

• Pharmacy 340B
• Cybersecurity
• Provider-Based Services and Provider-Based Physician Billing
• Disaster Recovery and Business Continuity
• Drug Diversion/Impairment in the Work Place
• Social Media
• Medical Devices/Networked Biomedical Devices
• Construction
• Philanthropy
• Revenue Cycle

slide 10

Speaker Biography

Tony Lesser
Senior Manager
Deloitte & Touche
Office: 312 486 3829
E-mail: alesser@deloitte.com

Experience and qualifications

Tony is a senior manager in Deloitte & Touche's Governance, Regulatory and Risk Strategy practice. He has over twelve years of experience and expertise in the healthcare industry, mostly working with healthcare providers. His work on the national level has allowed him to achieve experience and success across many different sectors and platforms in the industry. Tony has been nationally recognized for his contributions and expertise in the federal 340B Drug Pricing Program. He has published multiple articles in trade publications covering many topics related to 340B and regularly presents at various national events.

Prior to joining Deloitte, Tony worked for a large health plan, where he designed and implemented 340B pharmacy benefit programs between healthcare providers and pharmacies. Tony also previously served in a senior management position for a HRSA contractor, where he oversaw all 340B technical assistance and support provided by the federal government. He gained frontline experience working for one of the largest public hospital systems in the United States, where he managed a department responsible for contracting, billing, and inventory management for the health system's $100 million pharmaceutical budget.

Education and certifications
• MHA, Trinity University
• BS, Texas A&M University
• American College of Healthcare Executives (ACHE), Health Care Compliance Association (HCCA), Healthcare Financial Management Association (HFMA)

slide 11

CYBER SECURITY

slide 12

12

Overview

- Information Security
- The Case for Change
  - In the News …
  - Wishful Thinking?
- Cyber Security
  - Knowing Your Cybersecurity Landscape
  - Digital Eco-System
  - Understanding the existing Cybersecurity Portfolio

slide 13

13

Information Security – By Definition

- Information Security is the process by which an organization protects information and its critical elements including the systems, media, the people, and the facilities that process, store and transmit that information.

- In Healthcare: Enable and not disable empowerment of information for doctors and staff first.

slide 14

14

The Case For Change

Basic IT Security protections are no longer enough to combat the current threat environment. Internal and external threats may defeat existing protections already in place today. IT Security technologies more broadly have evolved into a much larger context than antivirus and firewalls in order to combat a newer and expansive list of potential vulnerabilities now in existence.

Privacy, confidentiality and IT assets may not be as protected as once thought. Without sophisticated monitoring, surveillance, anomaly detection and constant vulnerability assessments their relative health status is unknown and could be at risk. The new face of security breaches have changed and new threats require a far more comprehensive understanding of subtle changes in information movement. Active detection using a comprehensive integrated set of IT Security tools is essential and core to the organizations ability to detect, intervene and eradicate IT Security Breaches in the future.

slide 15

15

Cyber Security

- What is it
- Threats
- Consequences if not addressed
- Actions
- At Work and At Home
- Campus Services

slide 16

16

What is Cyber Security

- Cyber Security is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.

- Having a Cyber Security Program policy, which establishes that all devices connected to the health system electronic communications network must meet certain security standards.

- As part of this policy, all campus units provide annual reports demonstrating their level of compliance.

- Further, there are services in place to help all students, faculty and staff meet the Cyber Security standards. Specific information about these services is provided in this tutorial.

slide 17

17

In the News:
Two Cybersecurity Stories of Note

- Level 3, which provides internet and voice services to businesses was attacked in retaliation for the rumor of Julian Assange from WikiLeaks being harmed. It is estimated that during this attack's peak, 70% of the Internet in the US and UK was virtually rendered useless. Vendors were offline during the attack and service was restored once the attack ceased. The attack only ended after Julian Assange appealed for the attack to stop.

- Texas-based Rainbow Children's Clinic was the victim of a ransomware attack on its IT systems in August, which affected more than 33,000 patients. A hacker put notice on the clinics website and then launched a ransomware attack that began encrypting data stored on the clinic's server. Later it was discovered that some patient records have been irretrievably deleted. Destruction of records represents a new escalation in attacks on health systems.
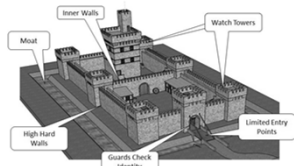
slide 18

18

Wishful Thinking?

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco

slide 19

19

Run From Castle Or Think!

The bad actors are coming in the front door.. Via Social Engineering and Phishing

slide 20

20

Creating a Cyber Resilient Environment

- Protecting everything is not only impractical it's financially not feasible for most organizations.
- Focus on the basics first:
  - Patch Management
  - Valid Backups
  - Are existing logs being monitored on the Firewalls, Anti-virus reporting, others?
- What environment can be developed to withstand attack?
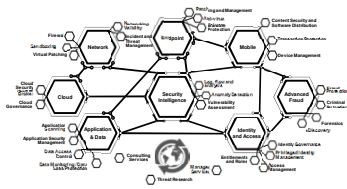
slide 21

21

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?
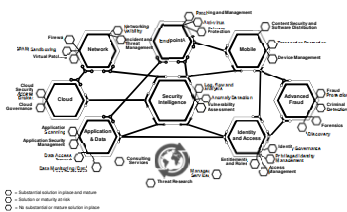 - What's missing from the Portfolio?

slide 22

22

IT Security Portfolio – Integrated Solutions Strategy

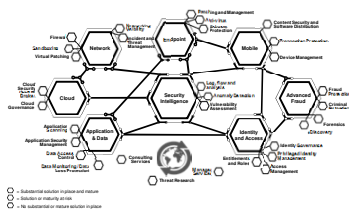slide 23

23

IT Security Portfolio – An Example

slide 24

24

IT Security Portfolio – An Example

○ = Substantial solution in place and mature
○ = Solution or maturity at risk
○ = No substantial or mature solution in place

slide 25

25

SIEM
(Security Information and Event management)

- The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views
- Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

slide 26

26

SIEM- Components

- Data aggregation : Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- Correlation : Looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.
- Alerting: The automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.
- Dashboards: Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.
- Compliance: Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.
- Retention: Employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance and eDiscovery requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.
- Forensic analysis: The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.
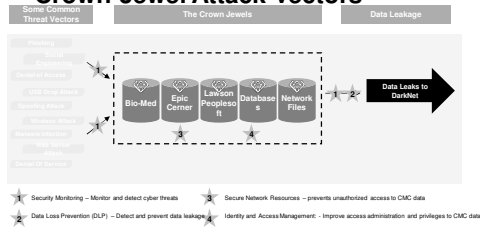
slide 27

27

Protecting the Crown Jewels

- Determine the mission critical systems
  - Epic/Cerner, PACS, the Network, the Telephone Systems, Lawson/Peoplesoft
    » Protect
    » Monitor
    » Vulnerability Identification and Remediation
    » Focus your efforts and have the highest security standards enforced

  - Build out from the center of Patient Care, Revenue Cycle and Infrastructure is one example

slide 28

28

"Crown-Jewel Attack Vectors"

Some Common Threat Vectors	The Crown Jewels	Data Leakage

Bio-Med | Epic Cerner | Lawson Peoplesoft | Databases | Network Files

Data Leaks to DarkNet

Security Monitoring – Monitor and detect cyber threats   Secure Network Resources – prevents unauthorized access to CMC data

Data Loss Prevention (DLP) – Detect and prevent data leakage   Identity and Access Management: - Improve access administration and privileges to CMC data

slide 29

Other Considerations…

- Exclude whole regions of the world who you do not do business with
  - Have a process for doctors without borders, be reasonable.
- Have your Cybersecurity Portfolio "test attacked" by an independent group.
- Go on the offensive and become hunters on your own network.

slide 30

30

What's the Big Deal

- Data breaches are becoming more prevalent and costly.
- Laws are in a state of flux.
- HIPAA adds extra requirements and consequences.
- New technologies present new and varied problems.
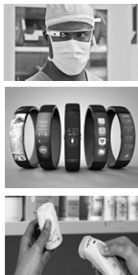- Amount and transmission of data is increasing at unprecedented rates!

slide 31

31

Data – New Hardware

- Google Glass
- Health wearables
- Apple Healthkit
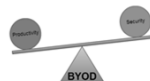- Google Fit
- Pill Scanning Technology

slide 32

32

BYOD Policy Components

- No expectation of privacy in the workplace
- Prohibit sharing of devices
- Must report lost or stolen devices
- Prohibit use of cloud-based storage of proprietary data
- Obtain employee consent to monitoring
- Obtain employee consent to remote wiping
- Instruction to employee to preserve data

slide 33

33

Compliance Strategy

- Understand the legal environment
- Survey the risk landscape
- Assess the benefit of cyber insurance
- Prepare for the inevitable data breach
- Organize data security teams
  - IT
  - Legal
  - Communications
  - Human Resources

slide 34

34

Consequences

- You may face a number of other consequences if you fail to take actions to protect personal information and your computer. Consequences include:

  Loss of confidentiality, integrity and/or availability of valuable university information, research and/or personal electronic data

  Loss of access to the campus computing network

  Lawsuits, loss of public trust and/or grant opportunities, prosecution, internal disciplinary action or termination of employment

slide 35

35

Top Seven Cyber Security Actions

1. Install OS/Software Updates
2. Run Anti-virus Software
3. Prevent Identity Theft
4. Turn on Personal Firewalls
5. Avoid Spyware/Adware
6. Protect Passwords
7. Back up Important Files

slide 36

36

Install OS/Software Updates

- Updates-sometimes called patches-fix problems with your operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS X) and software programs (e.g., Microsoft Office applications).
- Most new operating systems are set to download updates by default. After updates are downloaded, you will be asked to install them. Click yes!
- To download patches for your system and software, visit:
  - » Windows Update: http://windowsupdate.microsoft.com to get or ensure you have all the latest operating system updates only. Newer Windows systems are set to download these updates by default.
  - » Microsoft Update: http://www.update.microsoft.com/microsoftupdate/ to get or ensure you have all the latest OS and Microsoft Office software updates. You must sign up for this service.
  - » Apple: http://www.apple.com/support
  - » Unix: Consult documentation or online help for system update information and instructions.
- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.

slide 37

37

Run Anti-Virus Software

- To avoid computer problems caused by viruses, install and run an anti-virus program like Sophos.

- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the Last updated: date.

- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.

slide 38

38

Prevent Identity Theft

- Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people's information as you would your own.

- Never send personal or confidential information via email or instant messages as these can be easily intercepted.

- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. These often do not include a personal salutation. Never enter personal information into an online form you accessed via a link in an email you were not expecting. Legitimate businesses will not ask for personal information online.

- Order a copy of your credit report from each of the three major credit bureaus-Equifax, Experian, and Trans Union. Reports can be ordered online at each of the bureaus' Web sites. Make sure reports are accurate and include only those activities you have authorized.

slide 39

39

Turn on Personal Firewalls

- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Microsoft Vista and Mac OSX have built-in firewalls. For more information, see:
    - » Mac Firewall (docs.info.apple.com/article.html?path=Mac/10.4/en/mh1042.html)
    - » Microsoft Firewall (www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx)
    - » Unix users should consult system documentation or online help for personal firewall instructions and/or recommendations.
- Once your firewall is turned on, test your firewall for open ports that could allow in viruses and hackers. Firewall scanners like the one on http://www.auditmypc.com/firewall-test.asp simplify this process.
- Firewalls act as protective barriers between computers and the internet.
- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent your computer from responding to these calls.

slide 40

40

Avoid Spyware/Adware

- Spyware and adware take up memory and can slow down your computer or cause other problems.
- Use Spybot and Ad-Aware to remove spyware/adware from your computer. Individuals can get Spybot and Ad-Aware for free on the Internet Tools CD (available from IT Express in Shields Library).
- Watch for allusions to spyware and adware in user agreements before installing free software programs.
- Be wary of invitations to download software from unknown internet sources.

slide 41

41

Protect Passwords

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, password1, iloveyou1, (yourname1), baseball1.
- Change your passwords periodically.
- When choosing a password:
    - ▪ Mix upper and lower case letters
    - ▪ Use a minimum of 8 characters
    - ▪ Use mnemonics to help you remember a difficult password
    - ▪ Store passwords in a safe place. Consider using KeePass Password Safe (http://keepass.info/), Keychain (Mac) or an encrypted USB drive to store passwords. Avoid keeping passwords on a Post-it under your keyboard, on your monitor or in a drawer near your computer!

slide 42

42

Back Up Important Files

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so you can easily create a back up copy.
- Save copies of your important documents and files to a CD, online back up service, flash or USB drive, or a server.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- Test your back up media periodically to make sure the files are accessible and readable.

slide 43

43

Cyber Security AT HOME

- Physically secure your computer by using security cables and locking doors and windows in the dorms and off-campus housing.
- Avoid leaving your laptop unsupervised and in plain view in the library or coffee house, or in your car, dorm room or home.
- Set up a user account and password to prevent unauthorized access to your computer files.
- Do not install unnecessary programs on your computer.
- Microsoft users can download the free Secunia Personal Software Inspector (https://psi.secunia.com/), which lets you scan your computer for any missing operating system or software patches and provides instructions for getting all the latest updates.

slide 44

44

Cyber Security AT WORK

- Be sure to work with your technical support coordinator before implementing new Cyber Security measures.
- Talk with your technical support coordinator about what Cyber Security measures are in place in your department.
- Report to your supervisor any Cyber Security policy violations, security flaws/weaknesses you discover or any suspicious activity by unauthorized individuals in your work area.
- Physically secure your computer by using security cables and locking building/office doors and windows.
- Do not install unnecessary programs on your work computer.

slide 45

45

CAMPUS Cyber Security SERVICES

Protect Campus Network

Services	Software
▪ Campus email virus filtering ▪ Campus firewall services ▪ Email attachment filtering ▪ Vulnerability scanning ▪ Intrusion prevention system	▪ Free anti-virus software: Sophos Anti-virus ▪ Free encryption software: Pointsec for PC ▪ Free change management software: Tripwire

slide 46

46

The Internet is Hard to Secure

- Extreme complexity, minimal understanding
- High global connectivity
- Weak attribution (who's doing what?)
- Hard to tell malicious uses from legitimate ones

slide 47

47

Additional Information

- According to S.I. 1901 "Cyber Security Research and Education Act of 2002":
  - "The term cyber security infrastructure includes--
    - (A) equipment that is integral to research and education capabilities in cyber security, including, but not limited to--
      - (i) encryption devices;
      - (ii) network switches;
      - (iii) routers;
      - (iv) firewalls;
      - (v) wireless networking gear;
      - (vi) protocol analyzers;
      - (vii) file servers;
      - (viii) workstations;
      - (ix) biometric tools; and
      - (x) computers; and
    - (B) technology support staff (including graduate students) that is integral to research and education capabilities in cyber security."

slide 48

48

Mobile Device Security Resource Center for Providers and Professionals

Tips and information providers and professionals can use to:

- Protect and secure health information when using a mobile device
- Understand their organization's mobile device policies and procedures
- Five steps organizations can take to manage mobile devices

slide 49

49

Materials Available Online

Materials available for download on **HealthIT.gov/mobiledevices** include:

- Fact sheets
- Posters
- Brochures
- Postcard

slide 50

50

Helping Providers Integrate Privacy & Security Into Their Culture

- Designed to help health care practitioners and practice staff understand the importance of privacy and security of health information at various implementation stages

- Developed with assistance from the American Health Information Management Association (AHIMA) Foundation, with input from OCR and OGC

- Being updated to reflect HITECH changes

Guide to
Privacy and Security
of Health Information

slide 51

51

Cyber Security for Medical Devices:

- Common focus on individual medical devices is important… but misleading.
- Most medical systems can be secured simply by disconnecting them from the network.
- Unfortunately what would be lost, and what really needs to be protected, is the secure transfer of clinical information between medical systems.
- The right information, before the right people, at the right time, improves patient treatment. Security improvements must not impede that information flow.

slide 52

52

Constraints on Manufacturers

- Manufacturers rarely need to get approval from FDA with regards to Cyber Security fixes. However, they always need to validate safe & effective operation after changes, including 3rd party patches.
- No one can predict impact of 3rd party changes on clinical operations in advance. Therefore, verifying and validating seemingly minor changes may take significant time.
- Determining impact of patch, or any other design change, usually requires deep understanding of medical device.
- Everyone would like to move faster, but there is no magic way to avoid necessary validation.

slide 53

53

Healthcare Provider

- Traditional IT assumptions and procedures need to accommodate unique medical device realities.
- Generic IT security best practices, indiscriminately applied to medical devices without manufacturer coordination, can pose patient security risk. For example:
  - Automatic patching can and has broken medical devices,
  - Network vulnerability scans can disrupt clinical operations,
  - Antivirus software can disrupt time-sensitive clinical operations,
  - Misidentification of clinical data as a virus may interfere with clinical care,
  - Authentication schemes must fail-open (let the user in) instead of fail-closed (lock the user out).

slide 54

54

Ongoing Communications

- Cooperation between hospital IT staff and clinical personnel is critical since both parties have essential knowledge. It is dangerous when they work independently.
- Cooperation between healthcare providers and equipment manufacturers is also critical; for the exact same reasons.
- Treat security problems and concerns like any other problem with a medical device. They are hazards that need to be appropriately addressed.
- Don't reinvent the wheel or set up special channels -- use established support mechanisms.

slide 55

55

Do Not wait until you have to REACT
BE PROACTIVE

- Review Your Policies
- Monitor the Cyber Risks
- Foster an Organizational Commitment to Security
- Conduct Regular Audits
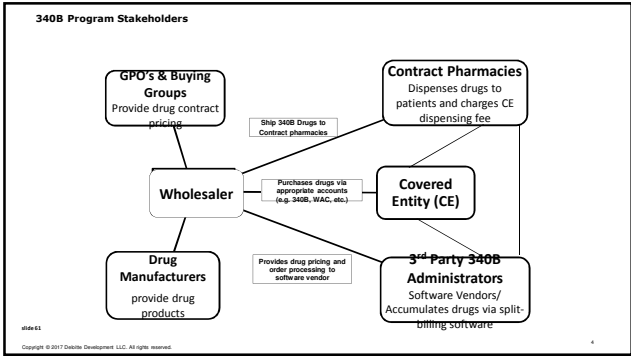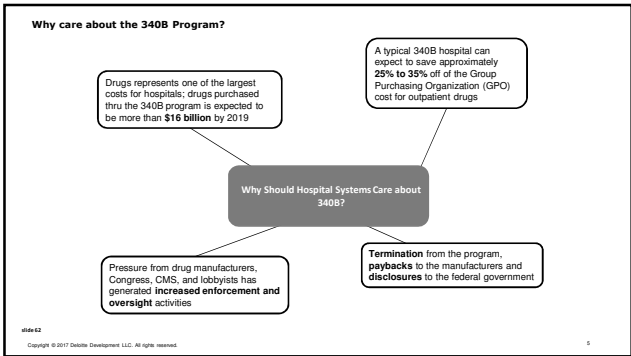- Understand the Legal Compliance Environment
- Train Your Team Members

Cyber Security Policy
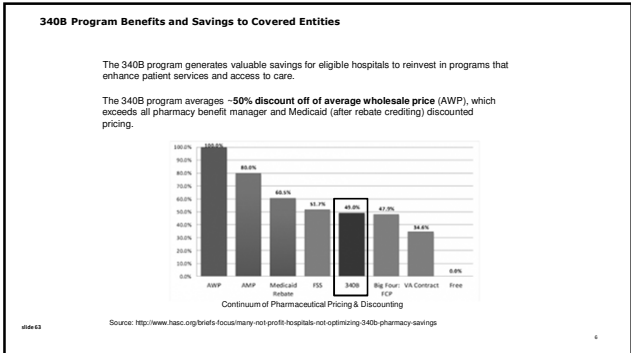
slide 56

56

WRAP UP

Q & A

QUESTIONS ANSWERS

slide 57

57

340B Drug Pricing Program

58

340B Drug Program Summary

- The 340B program requires drug manufacturers to provide outpatient drugs to qualified and participating healthcare organizations at significantly reduced prices
- The 340B Program provides the deepest discount on pharmaceuticals in the country, trailing only the Department of Defense and Veterans Healthcare Administration contracts
- Up to 2,048 hospitals and health systems participated as covered entities in 2014[2]
- 340B Entities accounted for over **$7 billion**[1] in drug spend in 2013, roughly **2%** of total spend across the United States

The **Veterans Health Care Act of 1992** requires pharmaceutical manufacturers whose drugs are covered by **Medicaid** to provide discounts on outpatient covered drugs purchased by specific public health services that serve the nation's most vulnerable patient populations.

The program has come under increasing levels of scrutiny since its **expansion after the PPACA in 2010.**

The OIG previously filed reports indicating **inconsistent operational practices** across covered entities and **limited oversight** by HRSA.

HRSA has attempted to issue formal guidance in the past; however, many unanswered questions and "gray" areas remain.

[1]Source: http://www.medpac.gov/documents/reports/may-2015-report-to-the-congress-overview-of-the-340b-drug-pricing-program.pdf?sfvrsn=0

[2]http://www.pharmacypracticenews.com/Article/PrintArticle?articleID=27580

59

340B Program Operations Illustration

In House:
1. Medication administered within eligible hospital/clinic
2. Outpatient or "mixed use" environment
3. Managed By split billing software
4. ER, Observation, Infusion, etc.
5. Purchases represent **cost savings** to the covered entity

Revenue
Prescriptions that "leave" the hospital that are dispensed at outpatient retail locations

Savings
Drugs Dispensed within the hospital and/or clinic sites

Contract Pharmacy:
1. Prescriptions dispensed at retail pharmacies for patients of eligible 340B entities
2. Usually requires technology solution to serve as an intermediary
3. Software vendor usually manages any new pharmacy chain(s)
4. Discharge medications, clinic prescriptions
5. Profit sharing model – **revenue generating**

3

340B Program Stakeholders

GPO's & Buying Groups
Provide drug contract pricing

Contract Pharmacies
Dispenses drugs to patients and charges CE dispensing fee

Ship 340B Drugs to Contract pharmacies

Wholesaler

Purchases drugs via appropriate accounts (e.g. 340B, WAC, etc.)

Covered Entity (CE)

Drug Manufacturers
provide drug products

Provides drug pricing and order processing to software vendor

3rd Party 340B Administrators
Software Vendors/ Accumulates drugs via split-billing software

slide 61

4

Why care about the 340B Program?

Drugs represents one of the largest costs for hospitals; drugs purchased thru the 340B program is expected to be more than **$16 billion** by 2019

A typical 340B hospital can expect to save approximately **25% to 35%** off of the Group Purchasing Organization (GPO) cost for outpatient drugs

Why Should Hospital Systems Care about 340B?

Pressure from drug manufacturers, Congress, CMS, and lobbyists has generated **increased enforcement and oversight** activities

Termination from the program, **paybacks** to the manufacturers and **disclosures** to the federal government

slide 62

5

340B Program Benefits and Savings to Covered Entities

The 340B program generates valuable savings for eligible hospitals to reinvest in programs that enhance patient services and access to care.

The 340B program averages **~50% discount off of average wholesale price** (AWP), which exceeds all pharmacy benefit manager and Medicaid (after rebate crediting) discounted pricing.

Continuum of Pharmaceutical Pricing & Discounting

slide 63

Source: http://www.hasc.org/briefs-focus/many-not-profit-hospitals-not-optimizing-340b-pharmacy-savings

6

Slide 6

Key Program Prohibitions

Diversion	Covered entity shall not resell or otherwise transfer the drug to a person who is not a patient of the entity
Duplicate Discount	Covered entity is prohibited from accepting a discount for a drug that would also generate a Medicaid rebate to the State. Billing requirements vary from state-to-state, but greater clarity will come in 2017.
GPO Exclusion	DSH hospitals, children's hospitals, and free-standing cancer hospitals may not obtain covered outpatient drugs through a GPO or other group purchasing arrangement.
Orphan Drugs	Free-standing cancer hospitals, rural referral centers, sole community hospitals, and critical access hospitals may not purchase selected rare disease drugs at 340B prices.

slide 64

6

Slide 8

Illustrative 340B Program risk universe

Inventory Management	Dispensing	Covered Entity/ Vendor Partnership
• Multiple distribution channels • Drug shortages • 340B replenishment variability • Inventory swell and reduced turnover • Tracking, monitoring, and auditing of inventory • Non-contract spend volatility • Accurate fulfillment of prescription orders • Accuracy of electronic product tracking information (tracking and pedigree) • Reconciliation of medication transfers (i.e. borrow/loan)	• Drug diversion to non-340B patients • Clarity and consistency of 340B "patient definition" • Drug Enforcement Administration (DEA) compliance • State Board of Pharmacy Regulations • Replenishment/virtual inventory models • Uninsured/Charity programs • Reconciliation of return-to-stock medication • Patient freedom of choice • GPO purchasing compliance	• High software costs • Third-party vendor sophistication and performance • Vendor selection • Operational contractual terms • Patient Health information exchange/data breaches • Reliance on third-party software systems • Reliance on third-party product tracking information
Technology	**Billing & Reimbursement**	**Legal/Regulatory/ Corporate Compliance**
• Complexity and variability of hospital IT systems • Data Integrity • Interface issues between hospital and vendor systems • Downtime procedures • Billing errors and data loss • Software maintenance activities	• Medicaid carve-in/carve-out • Managed Medicaid billing compliance • Reimbursement/Coverage Shifts due to 340B volume • Payment Collection processes • Medicaid Payor verification and management • Payer Auditing Activity • Variability of 340B prices • Losses incurred on high-yield prescriptions • Facility eligibility – integration with Medicare Cost Report	• 340B Omnibus Guidance • DEA Tracking and Pedigree regulations • MEDPAC cost-sharing recommendation • Anti-kick back regulations • Patient Records Management/Retention • Litigation and Dispute Res. • Antitrust • Contract compliance • HRSA, Manufacturer audit requests • Public disclosure of audit results/reputational risks • OIG Investigations • 340B Registration

slide 65

8

Slide 9

340B Drug Program: "Patient Definition"

- Drugs must be administered to a *qualified patient*:
  - Covered entity has established a relationship with the individual, such that the covered entity maintains records of the individual's health care; and
  - Individual receives health care services from a health care professional who is either employed by the covered entity or provides health care under contractual or other arrangements such that responsibility for the care provided remains with the covered entity; and
  - Individual receives health care service(s) from the covered entity which is consistent with the services(s) for which grant funding or federally-qualified health center look-alike status has been provided to the entity.
- 340B Program is intended for *Outpatient use only*
- Drugs must be administered in a hospital point of service that would qualify as a *"reimbursable cost center"* on the Medicare cost report:
  - Includes qualified outpatient facilities (e.g., physician clinics, surgery centers)
  - Provider-based reimbursement changes may affect new clinic enrollment

slide 66

9

Duplicate Discounts

- Covered entities may not receive a 340B discount for drugs that are subject to a Medicaid rebate:
  - Providers required to inform HRSA (by providing their Medicaid billing number) at the time they enroll if they plan to purchase and dispense 340B drugs for their Medicaid patients and bill Medicaid
  - Follow procedures established by State Medicaid agencies
- State Medicaid program may:
  - Require Covered Entities to *carve out Medicaid* patients from 340B so the State can claim the rebate
  - Allow Covered Entities to use 340B drugs for Medicaid patients, and *reduce Medicaid payment* to the Covered Entity
  - Allow Covered Entities to use 340B drugs for Medicaid patients, and *pay an increased dispensing fee*
- New CMS rules in effect beginning Summer 2017.
  - States must develop policies related to managed Medicaid
  - "acquisition cost" must be used as billing price for drugs

slide 67

Contract Pharmacies

Covered entities **must** conduct the following oversight activities for their contracted pharmacies:

Contract Pharmacy Oversight Requirements
1. Conduct independent annual audits and/or adequate oversight mechanism.

2. Documentation requirements:
  a. Develop written 340B Program policies and procedures involving contract pharmacy oversight
  b. Maintain auditable records at both covered entity and contract pharmacy
  c. Ensure written contract pharmacy agreement lists each contract pharmacy individually and is in place before registering contract pharmacy in 340B Program
  d. Contract pharmacy may not be utilized for purposes of the 340B Program until it has been registered, certified, and pharmacy is listed on the covered entity's 340B database record

3. Ensure that 340B drugs are only provided to 340B-eligible patients.
4. Carve-out Medicaid at contract pharmacies – or develop an alternative arrangement to work in collaboration with the state Medicaid agency to ensure duplicate discounts do not occur and report this to HRSA.
5. Maintain accurate information in the HRSA 340B database, including covered entity contact information, contract pharmacy information, and Medicaid billing information.

Source: http://www.hrsa.gov/opa/updates/contractpharmacy02052014.html

slide 68

Contract Pharmacies Expansion

- HRSA allows CEs to use an in-house pharmacy and contract with a retail pharmacy.
- Starting in 2010, HRSA allows CEs to utilize multiple contract pharmacies which greatly expands access to 340B drugs.
- Since 2010, percentage of CEs that use contract pharmacies has risen from 10% to 22%.

The number of unique pharmacies serving as contract pharmacies has grown by 770% and the total number of contract pharmacy arrangements has grown by 1,245%.

Source: US Department of Health and Human Services: Health Resource and Services Administration. *Notice Regarding 340B Drug Pricing Program-Contract Pharmacy Services.* 10272-10279. Federal Register Notices Vol.75 , No 43. March 5, 2010.
http://www.hrsa.gov/opa/programrequirements/federalregisternotices/contractpharmacyservices030510.pdf

slide 69

Sample 340B Roles and Responsibilities

| Role	Responsibility
340B Authorizing Official	• Responsible as the authorizing official in charge for the compliance and administration of the program in many cases • Responsible for attesting to the compliance of the program through recertification • Accounts for savings and use of funds to provide care for the indigent under the indigent care agreement
Pharmacy Lead	• Accountable agent for 340B compliance • Agent of the authorizing official responsible to administer the 340B Program to fully implement and optimize appropriate savings and ensure that current policy statements and procedures are in place to maintain program compliance • Maintains knowledge of the policy changes that affect the 340B Program, including, but not limited to, HRSA rules and Medicaid changes • Coordinates knowledge of any change in clinic eligibility/information
Pharmacy 340B Manager	• Accountable manager for 340B compliance program and day-to-day manager of the 340B operations • Responsible for maintenance and testing of tracking software • Responsible for documentation of policies and procedures • Manages 340B purchasing, receiving, and inventory control processes • Ensures compliance with 340B Program requirements for qualified patients, drugs, providers, vendors, payers, and locations • Reviews and refines 340B cost savings report, detailing purchasing, and replacement practices as well as dispensing patterns
Pharmacy Informatics / Information Technology Lead	• Supports the pharmacy software and selection of tracking software to manage the 340B Program • Defines process and access to data for compliant identification of outpatient utilization for eligible patients • Archives the data to make them available to auditors when audited

slide 70

13

Sample 340B Roles and Responsibilities (cont.)

Role	Responsibility
Reimbursement Lead	• Responsible for communication of all changes to the Medicare cost report regarding clinics or revenue centers • Responsible for communication of all changes to Medicaid reimbursement for pharmacy services/products that affect 340B status • Responsible for modeling all managed care contracts (with/without 340B) • Engages pharmacy in conversations that affect reimbursement
Accounting/ Finance	• Responsible for annual or semiannual physical inventory of pharmacy items • Responsible for establishment of "inventory average" process approved by the external audit firm (reference policy or type of process used, e.g., FIFO) • Logs and reports program revenue
Corporate Compliance Officer	• Designs the annual plan to cover all changes in the 340B Program from the preceding year • Monitors action plans relative to compliance violations and works with legal counsel related to any potential disclosures or repayments
Clinical Coordinators/ Care Organization	• Conduct 340B Program education related to outpatient pharmacies in order to improve patient access to medications • Monitors clinical outcomes relative to 340B program

slide 71

14

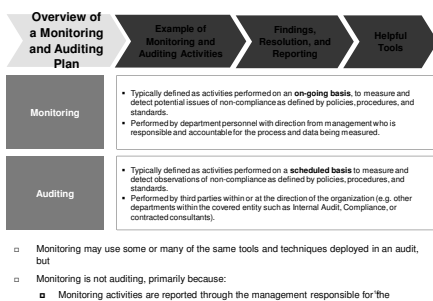**Sample 340B Roles and Responsibilities (cont.)**

Role	Responsibility
Pharmacy Buyer	• Responsible for establishing three distribution accounts and maintaining those accounts: non-GPO account, 340B account, and GPO account • Responsible for establishing and maintaining direct accounts for GPO ("own use") class of trade, as well as direct 340B accounts • Responsible for ordering all drugs from the specific accounts as specified by the process employed • Responsible for segregation, removal, and/or return of 340B drugs, including reverse distributor transactions • Responsible for reconciliation of lend and borrow transactions

slide 72

15

Internal Monitoring and Auditing

Overview of a Monitoring and Auditing Plan	Example of Monitoring and Auditing Activities	Findings, Resolution, and Reporting	Helpful Tools

Monitoring	• Typically defined as activities performed on an **on-going basis**, to measure and detect potential issues of non-compliance as defined by policies, procedures, and standards. • Performed by department personnel with direction from management who is responsible and accountable for the process and data being measured.
Auditing	• Typically defined as activities performed on a **scheduled basis** to measure and detect observations of non-compliance as defined by policies, procedures, and standards. • Performed by third parties within or at the direction of the organization (e.g. other departments within the covered entity such as Internal Audit, Compliance, or contracted consultants).

□ Monitoring may use some or many of the same tools and techniques deployed in an audit, but

□ Monitoring is not auditing, primarily because:

   ■ Monitoring activities are reported through the management responsible for the covered entity business

slide 73

Sample Areas to Monitor and Audit

Findings, Resolutions, and Reporting	Example of Monitoring and Auditing Activities	Helpful Tools	Overview of a Monitoring and Auditing Plan

Area to Monitor/Audit	How?	Area to Monitor/Audit	How?

1. Patient Definition	Policies and Procedures Review
	Eligible Provider Review
	340B Pharmacy Claims Review
		5. Contract Pharmacy
		  a. Patient Eligibility
		  b. Contracting
			340B Pharmacy Claims Review
			340B Contract Pharmacy Contracts Review

2. Covered Drug Definition	Policies and Procedure Review 340B Pharmacy Claims Review	**6. Diversion**	Pharmacy Claims Review
3. Duplicate Discounts	340B Pharmacy Claims Review Eligible Payer Review	**7. 340B Registration & Recertification**	OPA 340B Database and Recertification Review Cost Report Review

4. Exclusions
  a. GPO
  b. Orphan Drug
	Pharmaceutical Inventory Review
	Orphan Drug Prohibition Review
		8. Surescripts Provider Identified Number (SPI)	Verify number exists and is active for each electronic prescriber

slide 74

74

Findings, Resolutions, and Reporting	Example of Monitoring and Auditing Activities	Helpful Tools	Overview of a Monitoring and Auditing Plan

|				
● **Policies and Procedures Review**	Review documented policies **and procedures, including performing** walk-throughs, to validate 340B Program compliance is being followed	Monitoring - Annually	Covered entity Child sites	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
OPA 340B Database and Recertification Review	Review accuracy of pharmacy information to confirm correct registration with the OPA 340B database, and latest Recertification submission.	Monitoring - Quarterly	Covered entity Child sites Contract pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
$ **Cost Report Review**	Review Cost Report information and validate 340B-eligible locations can be mapped to appropriate line items	Monitoring - Annually	Covered entity Child sites	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit

slide 75

75

Example of Internal Monitoring and Auditing Plan Components/Areas

Findings, Resolutions, and Reporting	Example of Monitoring and Auditing Activities	Helpful Tools	Overview of a Monitoring and Auditing Plan

Eligible Provider Review	Review accuracy of eligible provider list per facility to confirm proper designation.	Monitoring - Bi-weekly	Pharmacies Contract pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
Eligible Payer Review	Review accepted payers to validate they are in alignment with Medicaid "Carve-in" or "Carve-out" status and applicable Medicaid billing.	Monitoring - Monthly	Covered entity Child sites Contract pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
340B Pharmacy Claims Review	Review 340B pharmacy claims per facility to confirm compliance with 340B Program requirements.	Monitoring - Monthly	Administered/dispensed outpatient locations and pharmacies Contract pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
340B Contract Pharmacy Contracts Review	Review executed contracts with contract pharmacies and contract pharmacy administrators to confirm compliance with contract pharmacy contract elements	Monitoring - Annually	Contract pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit

slide 76

76

Example of Internal Monitoring and Auditing Plan Components/Areas

Findings, Resolutions, and Reporting	Example of Monitoring and Auditing Activities	Helpful Tools	Overview of a Monitoring and Auditing Plan

Reversals Review	Review of adjustments to confirm all submitted 340B reversals have been completed.	Monitoring - Monthly	Contract Pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
Pharmaceutical Inventory Review	Review of pharmaceutical purchases orders, invoices, and true-ups. Scope includes split billing software and accumulators.	Monitoring - Monthly	Administered/dispensed outpatient locations and pharmacies Contract Pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit
Orphan Drug Prohibition Review (if applicable)	Review 340B captured prescriptions, originating from the Covered Entity, from both pharmacy and contract pharmacy location(s) to confirm drug(s) are not dispensed as 340B for treating diagnosis related to the primary indication of the orphan drug (if applicable)	Monitoring - Monthly	Administered/dispensed outpatient locations and pharmacies Contract Pharmacies	Monitoring - 340B Compliance Team Auditing – Internal Audit or Contracted External Audit

slide 77

77

Overview of a Monitoring and Auditing Plan	Example of Monitoring and Auditing Activities	Findings, Resolutions, and Reporting	Helpful Tools

Common Monitoring/ Auditing Findings	• Diversion to ineligible patients 　• Lack of documented encounter / missing assessment notes 　• "Moon-Lighting" and ineligible prescribers 　• Filled date vs. written date • Medicaid FFS processed inappropriately • Lack of self-disclosure of known issues to HRSA\OPA
Monitoring / Auditing Findings/ Resolutions	• Quantify issue(s) 　• Clearly defines the global impact of the actual findings on your program • Internal Audit finding & resolution documentation 　• Sample info 　• Discovery 　• Resolution 　• Proactive steps • Communicate to all applicable parties 　• Compliance Officer/Committee
Reporting Discoveries from Monitoring & Auditing	• Entity eligibility issues 　• Report to HRSA\OPA 　• Stop purchasing • Patient or covered drug eligibility issues 　• Work with manufacturers to determine repayment steps

slide 78

78

Findings, Resolutions, and Reporting

| Overview of a Monitoring and Auditing Plan | Example of Monitoring and Auditing Activities | Findings, Resolutions, and Reporting | Helpful Tools |

Program Manager Job Description

Drug Purchasing Program

Drug Purchasing Program Appendix

79

Creating Tools Can Be Useful to Support 340B Compliance

| Overview of a Monitoring and Auditing Plan | Example of Monitoring and Auditing Activities | Findings, Resolutions, and Reporting | Helpful Tools |

340B Monitoring Metrics

Monitoring	%	Jan	Feb	Mar
OPA 340B database review	99	100	100	96
Eligible Provider review	100	100	100	100
340B pharmacy claims review	99	98	99	100
Pharmacy 1	96	90	95	98
Pharmacy 2	99	100	100	95
Contract Pharmacy 1	93	80	90	100
Contract Pharmacy 2	96	90	95	100
Reversals review	100	100	100	100
Pharmacy 1	96	90	95	98
Pharmacy 2	99	100	100	95
Contract Pharmacy 1	93	80	90	100

80

Creating Tools Can Be Useful to Support 340B Compliance

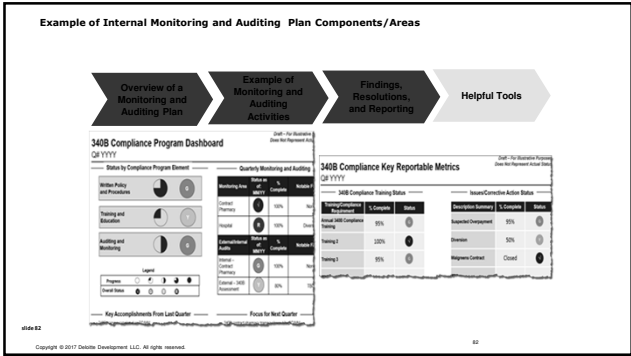| Overview of a Monitoring and Auditing Plan | Example of Monitoring and Auditing Activities | Findings, Resolutions, and Reporting | Helpful Tools |

340B Issues and Action Items Register

81

Example of Internal Monitoring and Auditing Plan Components/Areas

---

Questions?

---
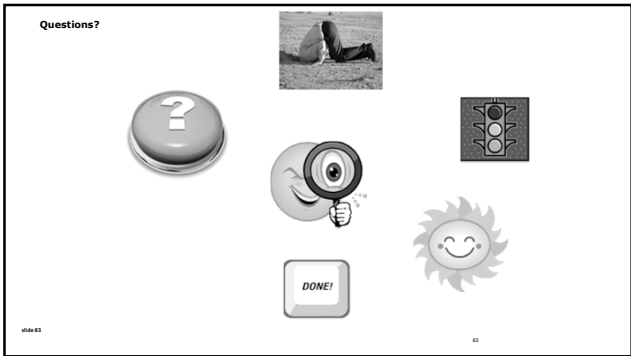
84 Provider-Based Services and Provider-Based Physician Billing

Agenda

- Background
- OIG Initiatives
- Provider-Based Considerations
- Monitoring Techniques to Protect Status
- Auditing for Compliance with Regulatory Requirements
- Key Controls
- Questions/ Comments

slide 85

85

Background – Provider-Based Regulations

- Current Provider-Based Status requirements are governed by the regulations at 42 C.F.R. § 413.65
  - Describes the criteria and procedures for determining whether a facility or organization is provider-based.
- Further explained in Program Memorandum Transmittal A-03-030
- Relationship between a main provider and another facility, department or related entity, whereby the other entity is considered a subordinate part of the main provider

slide 86

86

Background - What is Provider-Based Status?

- Refers to services rendered in an integrated hospital outpatient clinic or location
  - On-campus - within 250 yards of the main hospital (measured in a straight line)
  - Off-campus within 35 miles of the main provider

- General Rule – requirements apply to a facility if its status as provider-based or freestanding affects Medicare payment amounts and/or beneficiary liability for services furnished in the facility

slide 87

87

Background - Potential Advantages

- Net income benefits to the hospital for provider-based entities related to the ability to bill the hospital facility charge
- May result in higher combined reimbursement from Medicare and Medicaid
  - Commercial Payors – Problematic provisions
- Reimbursement for Medicare bad debts
- Access to hospital resources otherwise not available

slide 88

Background - Potential Advantages

- Provider may qualify as a "child site" for purposes of the 340B Drug Discount Program

- An outpatient clinic that qualifies as provider-based may be included in the commercial payor contracts applicable to services furnished in the main provider
  - Rates may be higher than those paid in freestanding outpatient clinics

slide 89

Background - Potential Disadvantages

- Negative impact on patients
  - Potentially higher charges and higher co-payments
  - Patients will receive two bills:
    - Facility Charge
    - Professional or Physician Fee Charge
  - Commercial Insurance and Other Payers
    - Higher Deductibles and Co-payments
- Greater billing complexities
- Potentially higher practice costs due to different wage scales/benefits
- Loss of physician control of hospital-based practice staff

slide 90

Background – On Campus and Off Campus

- Licensure
  - The department of the provider, the remote location of a hospital, or the satellite facility and the main provider are operated under the same license, except:
    - » in areas where the State requires a separate license for the department of the provider, the remote location of a hospital, or the satellite facility, or
    - » in States, where State law does not permit licensure of the provider and the prospective department of the provider, the remote location of a hospital, or the satellite facility under a single license.
  - 42 C.F.R. § 413.65(d)(1)

slide 91

91

Background – On Campus and Off Campus

- Clinical Services
  - The clinical services of the facility or organization seeking provider-based status and the main provider are integrated
    - » 42 C.F.R. § 413.65(d)(2)
    - » Clinical privileges of the professional staff
    - » Monitoring and oversight by the main provider
    - » Reporting relationship of the Medical Director
    - » Medical staff committees or other professional committees
    - » Integrated medical records (unified retrieval system)
    - » Integration of inpatient and outpatient services

slide 92

92

Background – On Campus and Off Campus

- Financial Integration
  - Financial operations are fully integrated within the financial system of the main provider
    - » 42 C.F.R. § 413.65(d)(3)
    - » Shared income and expense
    - » Cost reported in a cost center of the provider
    - » Financial status incorporated and readily identified in the main provider's trial balance

slide 93

93

Background – On Campus and Off Campus

- Public Awareness
  - Held out to the public and other payors as part of the main provider
    - » 42 C.F.R. § 413.65(d)(4)
    - » All information (advertisements, signage, web-sites, patient registration forms, letterhead) should reflect that the site is part of the main provider
    - » The name of the site should include the name of the main provider
    - » CMS has said it is not sufficient for advertisements to show that the site is part of, or affiliated with, the provider's network or health care system

slide 94

94

Background – On Campus

- Anti-dumping rules
- Bill physician services with Correct Site of Service Indicator – off-campus outpatient hospital (19) or on-campus outpatient hospital (22) versus office (11)
- Comply with all terms of the hospital's provider Agreement
- Hospital outpatient departments (other than RHCs) treat all Medicare patients for billing purposes, as hospital outpatients
- Subject to applicable payment window provisions (does not apply to CAHs)
- Meet all applicable hospital health and safety rules for Medicare-participating hospitals

slide 95

95

Background – On Campus

- Joint Ventures
  - Partially owned by at least one provider
  - Located on the main campus of the main provider who is a partial owner
  - Be provider-based to the main provider on whose campus the facility or organization is located
  - Meet all other provider-based requirements

slide 96

96

Background – Off Campus

- Operation under the ownership and control of the main provider
  - 100% owned by the main provider
  - Same governing body as the main provider
  - Operate under the same organizational documents as the main provider (bylaws, etc.)
  - Final responsibility lies with the main provider for:
    » Administrative decisions
    » Final approval of contracts, personnel actions/policies and medical staff appointments

slide 97

97

Background – Off Campus

- Administration and Supervision
  - Maintain the same reporting relationships as other departments of the main provider
    » Facility or organization is under the direct supervision
    » Operated under the same monitoring and oversight, operated just as any other provider
    » Administrative functions are integrated with those of the provider (billing services, records, human resources, payroll, employee benefit package, salary structure, and purchasing services)

slide 98

98

Background – Off Campus

- Location
  - Within 35 mile radius of the campus of the main provider
  - Exceptions
    » Owned and operated by a provider with DSH > 11.75%
    » Facility or organization demonstrates a high level of integration with the main provider (75% zip code test)
    » RHC located in a rural area attached to a hospital with less than 50 beds

slide 99

99

Background – Off Campus

- Management Contracts
  - A facility or organization that is not located on the campus of the potential main provider must meet all of the following criteria:
    - » Main provider employs the staff
    - » Administrative functions are integrated with those of the main provider
    - » Main provider has significant control over operations
    - » Management contract is held by the main provider itself

slide 100

100

Background – Off Campus

- HCPCS Modifier for Hospital Claims:
  - Modifier "PO"
    - » Short descriptor – "Serv/proc off-campus pbd"
    - » Long descriptor – "Services, procedures and/or surgeries furnished at off-campus provider-based outpatient departments" Also includes drugs and lab tests packaged into an OPPS service
  - Reported with every code for outpatient hospital services furnished in an off-campus provider-based department of a hospital
  - Not required to be reported for remote locations of a hospital defined at 42 C.F.R § 413.65 satellite facilities of a hospital defined at 42 C.F.R § 422.22(h), or for services furnished in an emergency department (Modifier not required for Critical Access Hospitals)

slide 101

101

Background – Off Campus

- Professional Claims – POS Codes
  - POS code 19 (Off-campus outpatient hospital)
    - » Services furnished in an off-campus PBD hospital setting
  - POS code 22 (On-Campus outpatient hospital)
    - » Outpatient services furnished in on-campus, remote, or satellite locations of a hospital
  - POS code 23 (Emergency Room-hospital)

slide 102

102

OIG Initiatives

- HHS OIG Work Plan FY 2014:
  - Impact of provider-based status on Medicare billing
  - Comparison of provider-based and free standing clinics (new)

- HHS OIG Work Plan FY 2015:
  - Medicare oversight of provider-based status
  - Comparison of provider-based and free-standing clinics

  …..extent to which such facilities meet CMS's criteria
  ….provider-based status can result in additional Medicare payments and increase beneficiaries' coinsurance liabilities

slide 103

103

OIG Initiatives

- HHS OIG Work Plan FY 2016:
  - Medicare oversight of provider-based status (Revised)
    - *Determine the number of provider-based facilities that hospitals own and the extent to which CMS has methods to oversee provider-based billing*
    - *Determine extent to which provider-based facilities meet requirements described in 42 CFR Sec. 413.65*
  - Comparison of provider-based and free standing clinics

slide 104

104

OIG Initiatives

- HHS OIG Work Plan FY 2017:

  - CMS is taking steps to improve oversight of provider-based facilities, but vulnerabilities remain.

  - We will review and compare Medicare payments for physician office visits in provider-based clinics to determine the difference in payments for similar procedures.

  - We will assess the potential impact on Medicare and beneficiaries of hospitals claiming provider-based status for such facilities.

slide 105

105

OIG Initiatives

October 15, 2014
Our Lady of Lourdes Memorial Hospital
$3.373 million settlement

"improperly submitted claims for hyperbaric oxygen therapy over a six year period as if such services were furnished in a provider based mobile unit, event though the unit did not comply with the requirements….."

slide 106

106

OIG Initiatives

TrailBlazer Health Enterprises, LLC (Texas)
$1,051,477 settlement

Medicare overpaid physicians due to incorrect place of service coding.

slide 107

107

Provider-Based Considerations

- Emphasis on provider-based self attestations for all locations
  - Attestation limits the recoupment time frame if future issues are encountered
  - Documentation submitted for facilities located on and off campus
  - Main provider lists each facility and states its exact location
  - Must be site specific – specific offices or suites
  - Provider-based physician billing sample CMS 1500 claim forms that denote the appropriate site of service (line 24B)

- Site of service rules the billing
  - Where the service was rendered governs billing
  - EKG performed in provider-based site but read remote must have provider-based site of service code

slide 108

108

Provider-Based Considerations

- Notice of co-insurance liability per 42 C.F.R. § 413.65(g)(7)
  - All off-campus locations billing as provider-based must have the Medicare Coinsurance form in place.
  - Patients are notified of the coinsurance liability for the service provided by the hospital and also for any physician service
  - An Advance Beneficiary Notification (ABN) does not meet the requirement of providing written notice of beneficiary liability
  - Hospital must provide written notice to the beneficiary, before the delivery of the services, of the amount of the beneficiary's potential financial liability
  - CMS provided "Off Campus Medicare Outpatient Coinsurance Notice" shows a patient signature line while the actual regulation does not specify the requirement that the patient sign the acknowledgement

slide 109

109

Provider-Based Considerations

- Separate license/certificate required for each service or separate location
- Periodic review and update of documentation – how often, by whom, utilize shared folder
- Name of the site should include the name of the hospital (CMS rejected a provider-based entity's application because it was named "John Hopkins at Greenspring" and not "Johns Hopkins Hospital at Greenspring" *Rejected by Appeals Board but an expensive battle*

slide 110

110

Provider-Based Considerations

- Hospital role in physician proper billing – Requirement for billing of physician services with the appropriate site-of-service indicator

Federal Register/Vol. 65, No 68 (18519) Response to comment:

We agree that physicians (or those to whom they assign their billing privileges) are responsible for appropriate billing, but note that physicians who practice in hospitals, including off-site hospital departments, do so under privileges granted by the hospital. Thus, we believe the hospital has a role in ensuring proper billing.

slide 111

111

Provider-Based Considerations

- Sharing of same space – What happens when a Medicare patient of the freestanding clinic must be seen during the block of time when it is a provider-based clinic and the treating physician insists that the provider waive its facility charge?

A site must not treat some Medicare patients as hospital outpatients and others as physician office patients.

slide 112

112

Provider-Based Considerations

- Shared Space Concerns
  - Lack of proper signage and distinction of what space is provider-based vs. freestanding
  - Change in space from when the hospital attested to compliance with provider-based rules and received CMS approval
  - Business license should reflect hospital use of portion of the space for hospital-based

slide 113

113

Provider-Based Challenges – What's New

- ❑ Effective 1/1/2017 CMS stopped paying hospital outpatient PPS rates for off-campus provider-based departments that began after the date the Bipartisan Budget Act of 2015 "Section 603" was signed into law.

- ❑ Going forward payments will be under the Medicare Physician fee schedule or the ambulatory Surgical Center payment system

- ❑ Payment changes do not effect on-campus provider-based departments or emergency departments

slide 114

114

Provider-Based Challenges – What's New

❑ CMS issued preliminary guidance clarifying the 21st Century Cures Act provisions impacting off-campus provider-based hospital outpatient departments that had concrete plans for construction when the Bipartisan Budget Act of 2015 was passed on November 2. The Cure Law -
  ❑ Extended the grandfather date
  ❑ Clarified that the required attestation and cerification documents must be received by February 13, 2017
  ❑ Issued sub-regulatory guidance on how hospitals can request a relocation exception

slide 115

115

**Provider-Based Challenges –
Approach to What's New**

❑ Review how you bill for provider-based locations based on new regulations:

  ❑ Commercial payers – billing as provider-based or clinic
  ❑ Medicaid – review Medicaid and Managed Medicaid plans
  ❑ Medicare Advantage – do you contracts follow CMS

slide 116

116

Monitoring Techniques to Protect Status

- Annual review of documentation related to provider-based status
- Development of monitoring reports for employed physician provider-based billing
- Determine monitoring technique for non-employed provider-based physician billing

slide 117

117

Auditing for Compliance - Regulatory Requirements

- Provider-Based Status
  - Request a listing of all locations billing as provider-based for the hospital
  - Obtain and review a copy of the attestation for each location
  - Review the confirmation letter from CMS
  - Policies and procedures exist, are followed, and comply with regulations
  - Analyze sample documentation
    » Licensure/Business License/Occupational Tax Application
    » Clinical staff integration
    » Financial integration
    » Public awareness/signage
    » Patient Notifications of Coinsurance
    » Provider-based entity operates under the hospital license and is 100% owned by the hospital
    » Common bylaws and same governing body

slide 118

118

Auditing for Compliance - Regulatory Requirements

- Billing of Physician Services with the Appropriate Site-of-Service Indicator
  - Communication Protocol
  - Physician Audit Process:
    » Employed Physicians – structure reports to ensure appropriate site of service location is reflected on bill
    » Non-Employed Physicians
      - Request billing forms from sample of patients seen at provider-based facility
      - Meet with physician office manager to jointly review a sample of physician billing from list of patients seen at provider-based facility

slide 119

119

Key Controls

- Policies/Procedures

- Shared Folder with Documentary Evidence Routinely Monitored and Reviewed

- Physician Training and Education (signed attestations that they understand provider-based billing rules and will include the correct place of service code on all patient billing claims)

- Monitoring for Compliance

- Right to audit clause in all provider-based physician contracts (employed and non-employed)

slide 120

120

40

Questions/Discussion

slide 121

121

Business Continuity/Disaster Recovery

slide 122

An Overview of BCP and DRP

• https://www.youtube.com/watch?v=cxE940f7iq0

slide 123

BCP

Business Continuity Planning (BCP) is the processes and procedures that are carried out by an organization to ensure that essential business functions continue to operate during and after a disaster. The ultimate goal is to help expedite the recovery of an organizations critical functions. This includes disaster recovery, but also includes critical contingencies for personnel and business processes.

slide 124

Key Elements of BCP

• Critical business functions have been identified and prioritized.
• Recovery time objectives have been determined for critical assets.
• Recovery point objectives have been established for critical applications.
• A comprehensive risk assessment has been conducted on critical facilities.
• Succession plans exist for key employees or consultants.
• A technology backup strategy exists and is tested regularly.
• Multiple sources are available for critical supplies and processes.
• People are identified, educated and trained on their duties during a disaster.
• Tools and training are in place to provide advanced warning of incidents.

slide 125

DRP

Disaster Recovery Plan (DRP) is the process an organization uses to recover access to their software, data and/or hardware that are needed to resume the performance of normal business after the event of a disaster. The DRP takes care of the technology and supports the business. It lays out the process necessary to bring key IT resources - both data and systems back online.

slide 126

Key Elements of DRP

- Remote storage and back up of data in a place that can be accessed from anywhere with an internet connection.
- Alternate communication lines for phones and email server.
- Backup people to spearhead implementation of the plan.
- An offsite location that will handle the company's computers, telecommunications, and environmental infrastructure so that critical business functions and information systems are able to resume as quickly as possible.
- List jobs that will be performed at the offsite location and who will be performing them. Be sure to have a list of the equipment they'll need to do their jobs.

slide 127

Benefits of BCP and DRP

- Allows your organization to avoid certain risks or mitigate the impact of unavoidable disasters by:
    - Minimizing potential economic loss
    - Decreasing potential exposures
    - Reducing the probability of occurrence
    - Improving the ability to recover business operations
- Helps minimize disruption of mission critical functions – and recover operations quickly and successfully – in the event of a crisis by:
    - Reducing disruptions to operations
    - Ensuring organizational stability
- Assists in identifying critical and sensitive systems
- Provides for a pre-planned recovery by minimizing decision making time
- Eliminates confusion and reduces the chance of human error due to stress reactions
- Protects your organization's assets and employees
- Minimizes potential legal liability
- Reduces reliance on certain key individuals and functions
- Provides training materials for new employees
- Reduces insurance premiums
- Satisfies regulatory requirements

slide 128

Assess Readiness for Business Continuity and Disaster Preparedness*

- Can you identify your critical business activities that satisfy your customers' expectations and support your overall business operations?
- Can you identify the critical business information needed for these activities to succeed?
  Do you have information on the frequency, impact and causes of downtime?
- Does this information allow you to identify and rank your most vulnerable business activities?
  Are your legacy systems and IT resources adequately protected against hacker intrusion and viruses?
- Have you developed a checklist, by functional area, of what your organization will need to continue business effectively in the case of a disruption or emergency?
- Have you and your IT colleagues been successful in placing business continuity on the board agenda?
- Have you worked with your IT colleagues to develop an approved business continuity plan that accounts for all aspects of business continuity and recovery?
- Is your business continuity plan regularly tested?
- Do you have a change control process in place to keep your continuity plan current with process, organizational and technology changes?
- Are you confident that if a disaster were to strike this very minute, your organization could recover quickly and smoothly to prevent damage to your business?

slide 129

"Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans", Yusufali F. Musaji, **ISACA Journal**

Audit Steps

Define the Scope of the Audit – What are the goals and objectives of the audit?

Planning – Identify and contact the primary source or auditee. Determine audit approach, such as review all plans or a sample of the plans. Develop audit checklists, questionnaires, audit programs and determine audit tests.

Fieldwork – Examine the individual BCP or DR program. Interview key stakeholders and participants in the program. Review planning and other IT related documents. Look for defined recovery times, verify if evidence meets the business goal. Review test plans and results.

Analysis – Analyze the results of tests performed and formulate recommendations.

slide 130

Reporting – Prepare and present a formal report to management.

Additional Fieldwork Steps

- Perform a health check – Review the plans and interview key stakeholders
- Assess completeness and comprehensiveness over all aspects of the BCP or DR program
- Assess the completeness of the business impact analysis (BIA)
- Observe BCP or DR tests
- Participate as formal observers of mock drills
- Compare what was planned and achieved against management's expectations. Compare to industry best practices
- Review Business Continuity Plan Attestations (see example)

slide 131

Examples of Key Findings

- No governance or steering committee has been established over BCP or DR
- Lack of a comprehensive enterprise wide Business Continuity Plan
- DR has not been fully tested
- No comprehensive listing of all application are tiered for criticality
- Business is not sure if recovery time objective and recovery point objective defined by Disaster Recovery Plan meets their needs
- Contact information and links noted within the Emergency Operations Plan and DR are not current
- Proximity of Data Center to the nearest facility has not been evaluated
- No formal agreement with a vendor is in place to purchase hardware if existing equipment is destroyed during a disaster
- Corporate policies that directly impact BCP and DR are not clearly defined and conflicted with facility policies (i.e. inclement weather policy)

slide 132

- Accountable leader for business continuity plan attestations

Are all stakeholders at the table……

slide 133