Connecting the Dots for Security Optimization

Sharon Parker, RN, CVRN,CHTS-CP, PCMH-CCE
Chief Quality Officer
May 8th, 2019

Mission

APHCA:

APHCA is a Catalyst for High Performance and Operational Excellence across its Integrated Community Health Care Network.

Session Overview

1. Leveraging Compliance Program for an Integrating Approach to Security Optimization
2. SWOT Analysis
3. Critical Planning Areas
4. Next Steps

Leveraging the Compliance Program

Section 6401, ACA – providers of medical care ***shall*** establish a compliance program as a condition of enrollment in Medicaid, Medicare, or CHIP

Core elements of compliance program established by HHS (with OIG)

Effective Compliance

Core Elements of Compliance Program

1. Designate Compliance Officer
2. Written standards and policies to implement and govern compliance operations
3. Training and education programs
4. Effective, clear, open lines of communication and internal reporting
5. Regular internal audits and monitoring
6. Response method and plan for detected issues
7. Publicize and enforce disciplinary standards

Effective Compliance

Health Center Risks Related to Security for Compliance Integration

1. Network and System Operation
2. IT Management and Oversight
3. HIPAA, HITECH and Beyond
4. HRSA Program Requirements
5. FTCA
6. Operations
7. Financial
8. Billing, Coding, Reimbursement
9. Other

System and Security Risks

HIPAA and HITECH Risks

Cybersecurity Risks – continue to increase; choice target for attackers – 111.8 million patients were affected in 2015 by hacking events (1/3 of entire US population)

IT System Management – internal risks are increasing due to hardware, software, consistency in oversight and maintenance

HIPAA and HITECH Risks

HIPAA (1996) and HITECH (2009) – established minimum standards; compliance with HIPAA does not equate to secure

Words not associated with HIPAA – hacking, cloud, file sharing, portal, network interruptions, wireless, Wi-Fi, system administrator, smartcard, USB, storage area network (SAN), texting, social media, patch management, phishing, identity theft, telemedicine, remote access

HITECH – focus on enforcement of HIPAA; IT environmental shifts well beyond what was contemplated in the implementation of HIPAA, HITECH

HIPAA and HITECH

5 largest fines ever imposed by OCR occurred in 2016

Highest risks areas with related fines and CAPs:

1. Failure to conduct accurate and thorough risk ***analysis*** to include all IT equipment, applications and data systems storing PHI
2. Failure to implement risk management and incident response plans

HIPAA and HITECH

3. Failure to implement policies and procedures and retain for 6 years

Distinguish, document, and education on the difference between system/technical policies and organizational policies; requirement for both (technical includes control settings that define how application and systems will behave)

HIPAA and HITECH

4. Failure to ***reasonably*** safeguard e-PHI
5. Failure to encrypt devices and media
6. Failure to have appropriate BAAs
7. Vendor management and oversight

February 1, 2017 – OCR fines Medical Center in Dallas $3.2 million for HIPAA noncompliance and impermissible disclosure of unsecure ePHI stemming from two data breaches caused by lack of encryption

System Management and Oversight

Duty to prevent, detect, assure, and recover

1. **Prevent** – effective use and management of firewalls, endpoint security (antivirus), multi-level filtering; patch management of operating systems and applications; user access rights and privileges
2. **Detect** – data logs, instruction detection, data loss prevention, event logging, use behavior monitoring
3. **Assure** – quarterly vulnerability scans, annual penetration testing, data backup system, periodic testing of backups, BAAs, oversight of BAAs and vendors
4. **Recover** – incident response plan, disaster recovery plan, testing and ongoing monitoring protocol

System Management and Oversight

Staffing/workforce limitations

- Lack of, inconsistent monitoring, management of firewalls, endpoint security (antivirus), multi-level filtering; patch management of operating systems and applications; user access rights and privileges
- Lack of data back up system, plan and routine testing protocol
- Lack of disaster recovery system, routine testing
- Lack of incident response plans to include detection, analysis, containment, eradication, recovery, reporting/lessons learned; attention to documentation at each phase of incident response)

HRSA Performance Expectations

1. Continued Readiness - Health centers should be operated in continued readiness state of compliance; focus on high performance (clinical encounter approach)
   - No tolerance for being unprepared and/or noncompliant
   - Compliance demonstration beyond *paper compliance*
   - Shifting PCA T/TA focus from program requirements to quality and performance
   - Unannounced OSVs? TJC/HRSA Pilot; 5 health centers

CURRENT OIG Work Plan – to what extent does HRSA continue to fund organizations failing to meet basic contract requirements (core 18)

HRSA Performance Expectations

2. BOD Engagement and Advanced Decision Making
   - Know how the HC is performing; knowledge of HC strategic plan; financial management and related performance (aged AR; cash flow management; revenue sources; no show rates; other)
   - PCMH accreditation and implementation process and impact; PHM
   - Oversight of organizational compliance program
   - CEO evaluation – process, results

HRSA Performance Expectations

3. Integrated approach to care delivery through “expanded access,” and “operational excellence,” (PCMH, HIT, HIE, PHM, APMs)

HRSA Performance Expectations

4. CMS Emergency Management (9/8/2016)
   - Establishes national emergency preparedness requirements for all Medicare and Medicaid participating providers and suppliers to plan adequately for both natural and man-made disasters, and coordinate with federal, state, tribal, regional, and local emergency preparedness systems
   - More comprehensive requirements to include:
     1. Risk assessment and planning
     2. Policies and Procedures
     3. Communication plan
     4. Training and testing program

Case Study: Cascading Security Risks

IT system and records management issues can immediately trigger additional areas of risks:

1. TJC standard violations
   - Information Management Chapter, i.e., backups (identified as direct impact to care risk); Emergency Management Chapter, Leadership Chapter (oversight, monitoring; response to system and process failures); Rights and Responsibilities (maintain security and system integrity, protect against loss, damage; health information available/retrievable; accuracy of information

Case Study: Cascading Security Risks

Performance Improvement Chapter (PCMH related coordination from patient data); Record of Care, Treatment and Services (likely entire/most of chapter)

Waived Testing Chapter (capacity to demonstrate competency in technicians; loss, destruction of records would negate ability to identify tech)

Medication Management Chapter (management of recalls, demonstrate timeliness of dispensing, orders, etc. if record disruption, loss, destruction)

Alabama Cases

First series of cases filed related to complete failure of computer server, loss of medical practice management database, failure to protect and preserve redundant systems and proper backups within Alabama health center

HC vs EHR vendor, technology consultants and vendors

SWOT Analysis of Performance Factors

Strength – **internal** factor that positions the organization well for high performance and to mitigate risks

Weakness – **internal** factor that creates risks or places the organization at a disadvantage

Opportunities – **external** factors that the organization is positioned to avail itself of

Threats – **external** factors that either create risks or place the organization in a position of weakness, disadvantage

- What you can do well?
- How you stand apart from your competitors?
- Do you possess strong research and development capabilities?
- What internal resources do you have?
- What kind of tangible assets (capital, credit, distribution channels or technology) you own?

S

STRENGTHS

- Which areas need improvement to compete with your strongest competitor?
- What does your business lack?
- Are there any limited resources?
- Is your business in a poor location?

W

WEAKNESSES

- What opportunities exist in your market?
- How can these benefit?
- Is the perception of your business positive?
- Had there been any changes the market recently?

O

OPPORTUNITIES

- Who are your potential competitors?
- Which factors you need to control to prevent the risks \ to your business?
- Is there anything, deteriorating your revenues or profits?
- What threatens your marketing efforts?

T

THREATS

SWOT:
Areas to Assess S/W

IT systems and infrastructure

Internal policies, procedures, workflow

Risks (information systems, workforce, procedures, compliance)

Status of continued readiness (TJC, HRSA, AMA, OCR)

Staff turnover- continued training of new staff

Provider turnover – continued training of new staff

Availability and integration of performance data in governance, management, clinical operations

SWOT:
Areas to Assess S/W

- Quality assurance
- Quality improvement
- Systems of monitoring quality and performance (operational, financial, clinical, other)
- Full HIT/HIE adoption and capacity
- Policy and procedural documentation
- Alignment of policy and procedure to actual practice

SWOT:
Areas to Assess S/W

Clarity in roles, responsibilities as evidenced by engagement and performance

“Effective” compliance program

Cybersecurity

Risk assessment and mitigation for record loss (DR, backups)

Level of understanding and consistent application of policy and procedure across all staff levels

EM readiness – natural, System failure

SWOT Breakout

Opportunities and Threats

OPPORTUNTIES

ACHNs

Care coordination

Telehealth

Behavioral/substance abuse health

Marketing capacity

ACHN performance goals

Schools

Prescriptions meds excluded in PMPM model

THREATS

ACHN/patient assignment/ACHN FQHC pick

AHCA/Medicaid funding cut

Rising private hospital referrals to internal primary care

Provider workforce

Urgent care centers

Measures not met/limiting network

mental/health dept. services shifted to HC

Next Steps

Establish Security Related Goals and Objectives

Integrate Security Specific Strategies into related Work Plan

Board Review and Adoption

Board and Staff Engagement, Monitoring, and Reporting

Questions!!!

Sharon Parker, RN,CVRN-BC, CHTS-CP, PCMH CCE
Chief Quality Officer
sparker@alphca.com
334.386.3985