Reducing Risk for Small Provider Practices

OCR/NIST

Safeguarding Health Information: Building Assurance through HIPAA Security

September 6, 2017

Robert M. Tennant
Director, Health Information Technology Policy
Medical Group Management Association
rtennant@mgma.org

About MGMA

- MGMA is the premier association for professional administrators and leaders of medical group practices
- Since 1926, the association has delivered networking, professional education and resources, political advocacy and certification for medical practice professionals
- Through its national membership and 50 state affiliates, MGMA represents more than 40,000 medical practice administrators and executives in practices of all sizes, types, structures and specialties

Reducing Risk by Changing the Culture in…

Small Practices…and

Government!

Current Practice Environment (*Change from paper to electronic*)

- Practices adopting EHRs (75%+)
- Focus of technology has been on meeting govt reporting requirements (Meaningful Use/QPP), not on security
- Wannacry/Petya ransomware attacks make front page news
- Patients increasingly worried that sensitive health information might leak because of weak security
- Small practices rely heavily on EHR vendors for security
- Providers in general and small providers in particular face unique security challenges and have limited abilities and resources

What are Typical Cybersecurity "Events"?

- Unauthorized access by employees
- Misuse of authorized access
- Physical disasters
- Server crashes
- Staff untrained on dealing with security issues
- Ineffective disposal of PHI
- External attacks

What are the Consequences?

- Temporary loss of medical records
- Loss of financial data
- Permanent loss of confidential information
- Unauthorized access to confidential information
- Loss of physical assets
- Damage to clinic reputation, patient confidence, business continuity
- Government enforcement

Culture Change for Small Practices

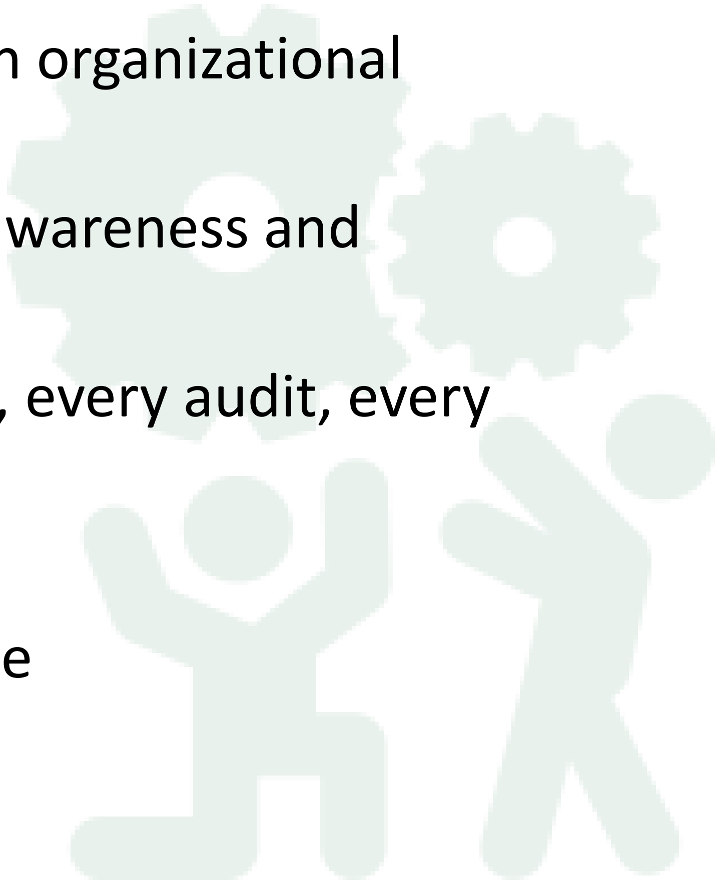
How Small Practices Can Reduce Risk

- ***Understand the critical nature of data security***
- Not to view security as solely a compliance issue, but more of a business continuity issue
- Practice leaders need to ask the key questions that begin with "what if"
    - ❑What if we experienced a system failure or disaster?
    - ❑What if we had a data breach?
    - ❑What is we lost patient data?
    - ❑What if we lost claims data?
    - ❑What if we lost patient and colleague confidence?
- And then ask…What would these mean to our business?

How Small Practices Can Reduce Risk

- ***Conduct a Comprehensive HIPAA Security Risk Assessment***
- Leading cause of failing a CMS Meaningful Use audit, now in QPP
- Leverage available resources or contract with a qualified consultant to conduct one
- The assessment should review:
  - Issues related to practice use of the Internet and the potential of an external cyberattack
  - Practice’s administrative, physical, and technical safeguards
  - Focus on the highly vulnerable areas:
    - Mobile technology
    - Email/texting
    - Remote access
    - Employee policies

How Small Practices Can Reduce Risk



- ***Creating a Healthy Cybersecurity "Culture"***
- A culture of security is enhanced through organizational communication
  - Create a practice culture of security awareness and seriousness
  - Encourage learning from every event, every audit, every person
- Create a culture of "trust but verify"
  - Anyone can be questioned at any time
  - Non-defensiveness when questioned
  - Modeled from the top down
- Generate pride in the security culture and protecting patient data

How Small Practices Can Reduce Risk: Specific Action Steps

1. Control Physical Access
2. Protect Mobile Devices
3. Deploy offsite data backup
4. Use a Firewall
5. Install and Maintain Anti-Virus Software
6. Limit Network Access
7. Control Access to PHI
8. Use Strong Passwords and Change Regularly
9. Plan for the Unexpected
10. Train and retrain all clinical and administrative staff

Culture Change for Government

What OCR and NIST (and ONC) can do

- Change focus from "compliance" to engagement and assistance
- Don't just highlight "bad actors" (OCR website, HHS Breach Portal) but celebrate the success stories (HHS awards?)
- Opportunities include:
  - Create a "National Physician Practice Security Week"
  - Full transparency of results from Figliozzi (CMS MU), OCR, OIG audits
  - Turn audit results into teaching modules
  - Leverage CMS "open door calls" to educate small practices
  - Expand current risk assessment tools
    - Go beyond simply asking questions based on 2005 rule
    - Provide sample policies/procedures for each requirement and allow for customization
    - Mirror OCR's excellent sample privacy notice
  - Encourage 3rd party security accreditation/certification
  - Recognize these 3rd parties in QPP program

Thank you.

MGMA®