Introduction to Building and Governing Your HIPAA Compliance Program

June 28, 2016

HealthInsight

This Webinar is Brought to You By….

HealthInsight

HIPAAOne
PROTECT YOUR ePHI

mountain-pacific quality health
HTS HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive, Helena MT 59602 | www.gotohts.org | 406.457.5897
transforming health care through innovative technology

PASS

About HealthInsight and Mountain-Pacific Quality Health

- HealthInsight and Mountain-Pacific Quality Health are private, non-profit, community-based Quality Innovation Networks Quality Improvement Organizations (QIN-QIOs) that have dedicated more than three decades to improving health and health care and are composed of locally governed organizations in: Alaska, Hawaii, Montana, Nevada, New Mexico, Oregon, Utah and Wyoming. As part of our efforts to assist hospitals and practices with HIPAA compliance, HealthInsight and Mountain-Pacific Quality Health teamed together to form **HIPAA Privacy and Security Solutions**, or ***HIPAA PASS***, to offer affordable, easy and comprehensive Risk Analysis and Risk Management services.

About HIPAA One®

- Following a thorough search for the best software to assist our practices and hospitals to achieve HIPAA compliance, HIPAA One® emerged as the clear solution.
- For more information about HIPAA One® please visit:

https://www.youtube.com/watch?v=9G_B7U_pnuo&feature=youtu.be

Mark Norby, CHP

- 15 Years of IT experience
- Eight Years as the CIO of the Community Health Center of Central Wyoming and University of Wyoming Family Medicine Residency Program
- Six Years as a HIPAA Compliance Officer
- Four Years as a HIPAA Compliance Consultant
- Provided help to more than 150 hospitals and clinics

Essential HIPAA Terms to Know

Covered Entities (CE)

- Includes health plans, health care clearinghouses and most health care providers
- Applies to most health care providers because they transmit health information electronically (e.g. billing)

Business Associates

- Individuals and organizations that perform services for or on behalf of your practice that involve routine access to Protected Health Information (PHI)

Protected Health Information (PHI)

Refers to individually identifiable health information that relates to the individual's past, present, or future physical or mental condition, including the provision of health care to the individual, that is

- Transmitted by electronic media
- Maintained in electronic media
- Transmitted or maintained in any other form or medium

Three Legs

- HIPAA Privacy Rule – April 2003
- HIPAA Security Rule – April 2005
- HIPAA Breach Notification Rule – Sept. 2009

HIPAA Privacy Rule

- Establishes standards for the use and disclosure of PHI
- Protects PHI whether electronic, oral or paper
- Establishes standards for providing patient rights
- Outlines civil and criminal penalties for failure to comply

Examples of Patient Rights

- The right to inspect, review and receive a copy of their health information
- The right to request amendments
- The right to an accounting of disclosures
- The right to confidential communications
- Access to Notice of Privacy Practice

HIPAA Security Rule

- Protects individuals' **electronic** PHI that is created, received, maintained or transmitted by CE
- Protects confidentiality, integrity and availability (CIA) of ePHI
- Consists of administrative, physical and technical safeguards

Breach Notification Rule

- Requires CE's to promptly notify individuals and the Secretary of HHS of the compromise of **unsecured** PHI

Privacy and Security Starts at the Top

- Designate a privacy and security officer
- Make sure that each has a job description
- Select a qualified professional to assist you with the Security Risk Analysis
- Promote a culture of protecting patient privacy

Document Your Process, Findings and Actions

- Records will be essential if you are audited
- Good faith effort can be the difference between a corrective action plan (CAP) and a fine
- Maintain records for six years

Examples of Documentation to Keep

- Completed checklists
- Security Risk Analysis report(s)
- Risk management action plan
- Business associate (BA) agreements
- Trainings for staff
- System monitoring results
- Policies and procedures
- Meeting minutes

Conduct a Security Risk Analysis

- An ongoing process to identify risks to CIA
- It's the first step towards Security Rule compliance
- NOT optional – regardless of size
- A checklist will not suffice
- HHS recommends a nine step process as outlined in NIST SP800-66
- Consistently review/update and keep documentation
- Soak up the education

Develop an Action Plan (Risk Management Plan)

- Use Security Risk Analysis to identify threats and vulnerabilities
- Focus on high priorities and low hanging fruit
- Identify what needs to be done
- Who is going to do it
- When will it be done
- The plan must include the following five components:

1) Physical Safeguards

- Facility security - Is the server room locked, who has keys to the building?
- Workstation and office security - Are passwords written on a sticky note, do workstations auto log-off?
- Protecting portable devices

2) Administrative Safeguards

- Designated security officer
- Workforce training and oversight
- Controlling information access
- Periodic security reassessment

3) Technical Safeguards

- Controls on access to electronic health record (EHR) and other software
- Use of audit logs to monitor activities
- Secure exchanges of electronic data

4) Policies and Procedures

- Establish protocols for administrative, physical and technical safeguards
- Specify individual patient rights
- Documented incident response plans
- Processes for breach notification and sanctions

4) Policies and Procedures (cont'd)

- Train staff on policies and procedures
- Consistently apply policies and procedures
- Periodically review and update policies and procedures
- Retain old policies and procedures for six years after they have been updated or replaced

5) Organizational Requirements

- Breach notification and associated policies, **are they in place and have staff been trained**?
- BA agreements, are they in place and is the BA aware of their responsibilities?

Business Associates

- Responsibilities are very similar to those of a CE
- CE is responsible for obtaining a BA agreement obligating the BA to safeguard PHI
- Breach notification requirements must be met
- CE must respond to non-compliance

Prevent with Education and Training

- Build your policies and procedures and train, train, train; including employees, volunteers, trainees and contractors
- Keep copies of your policies and procedures in an easy to find place
- Formally educate and train your workforce at least once a year or when changes happen
- https://www.healthit.gov/providers-professionals/privacy-security-training-games?ref=322915122&uid=919993707

Keep Up With the Changes

- Join the OCR Privacy and Security Listservs

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html

Governance Methods

- Use the job description as an evaluation form
- Comply with 45 CFR 164.308(a)(8) using the OCR Audit Protocol
- Use the Security Standards Matrix as a checklist
- Use the Omnibus Final Rule checklist
- Use the HIPAA Privacy Rule checklist

Governance Methods (cont'd)

- Use the Network Access Request Form
- Develop a termination checklist
- Define, by role, which polices and procedures are to be read and build a checklist

Periodic Tasks to Consider

- HIPAA refresher training - at least annually
- Review of access rights - annually
- Re-sign Confidentiality Agreements - annually
- IT inventory - annually
- Facility walkthrough inspection - annually

Periodic Tasks to Consider

- Assess firewall, router, anti-virus settings for optimum security
- Annual report to HHS

Join Us!

Our next free webinar

Essential Steps to HIPAA Compliance

Tuesday, July 26, 2016

1-2 p.m. MT

To register visit:

http://healthinsight.org/hipaapass#events

Save the Date!

One-Day HIPAA Privacy and Security Bootcamp

Tuesday, September 13, 2016
At HealthInsight Utah
756 E. Winchester Street Murray, Utah
8 a.m. - 5 p.m. MT

Watch your email for registration details in the coming weeks!

Questions?

Mark Norby, Certified HIPAA Professional
HIPAA Counselor
307.258.5322
mnorby@healthinsight.org

Visit our website:
healthinsight.org/hipaapass
for more information about our privacy and security solutions!

Thank you and have a wonderful day!!