HIPAA Myths

WEDI Regional Affiliates

Chris Apgar, CISSP
Apgar & Associates

Overview

- Missed Regulatory Requirements
- Common HIPAA Privacy Myths
- Common HIPAA Security Myths
- Other Related Myths
- Finding the Right Answer
- Q&A

Missed Regulatory Requirements

- Contingency planning – more than just “we’re cloud based so we can log in anywhere”
- Risk analysis – not just required for Meaningful Use
- It’s more than just technology
- Incident response – does that mean breach only?

Missed Regulatory Requirements

- Training is required and it can be costly if you don't pay attention it – just ask UCLA
- Policies and procedures – If it's not written down, it didn't happen
- Do I really need to look at those audit logs?
- Documents – why centralized storage and regular updates are so important

Missed Regulatory Requirements

- What I don't know can hurt me – "willful neglect, know or should have known"
- I only need to worry about HIPAA, right?
- Beware of state attorneys general
- OCR does investigate – complaints, breaches and what to expect when OCR calls
- If a government agency requests it, it doesn't always mean you can share

Missed Regulatory Requirements

- Why it's not a good idea to mitigate after receiving that OCR or CMS audit letter
- Auditors are not your friends
- Detailed Medicaid contractual requirements do have the force of law – Californians beware (among others)
- Fines from OCR and Texas – state laws and compliance enforcement

Common HIPAA Privacy Myths

- Patient rights often overlooked and do directly tie to quality of care
- Loss of confidentiality leads to lack of trust
- It's OK to adopt more stringent privacy practices – just don't blame it on HIPAA
- Those in health care are confused about when PHI can be shared and how much – what is minimum necessary anyway?

Common HIPAA Privacy Myths

- The much maligned Notice of Privacy Practices
  - Direct care – actually handing it to the patient required
  - Find a place on the wall that all can see and summaries are OK
  - Burying the Notice on your web site is not a good idea
  - The Notice should be readable

Common HIPAA Privacy Myths

- Patient privacy rights – some of the myths
  - "You can't view your record – it's electronic"
  - Paper or electronic – patients can ask for either
  - "I didn't create the record, I can't locate the entity who did so I can't amend it" – it's just not true
  - Abuse reporting and individual notification requirements

Common HIPAA Privacy Myths

- Meaningful use audits – is the auditor entitled to all PHI?
- OCR compliance audits – what can OCR's auditor really ask for
- Minimum necessary myths
  - "Everyone needs access to everything"
  - "Subpoenas entitle the presenter to everything and I don't need to inform the patient"
  - "Sharing PHI with other providers – you can't have it all"

Common HIPAA Privacy Myths

- Business associate myths
  - "No formal contract needed because the statute requires compliance"
  - "Business associates can assess risk in the event of a breach"
  - "Cloud vendors can't see the PHI so they're not business associates"
  - "Only covered entities are required to execute a business associate contract

Common HIPAA Privacy Myths

- Business associate myths (continued)
  - "It's not in the law so no indemnification clause needed"
  - "Business associates aren't required to honor patient rights – that's only for covered entities"
  - "Business associates are always agents of covered entities"

Common HIPAA Privacy Myths

- “Health information organizations (HIO) and health information exchanges (HIE) – compliance falls to covered entities”
- “It’s paper – why worry?”
- “If employees post it on Facebook® on their own time, it’s their liability”
- “Contracted employees aren’t workforce members”

Common HIPAA Privacy Myths

- Loud voices and waiting rooms
- “I can’t tell you because HIPAA says so”
- What to do about incidental disclosures
- Conversations after work that can get covered entities in trouble
- Who is responsible if the ex-employee talks about that patient?

Common HIPAA Privacy Myths

- Friends and family
  - "I can't tell you because HIPAA prohibits it"
  - Opportunity to object – what does it really mean?
  - The patient doesn't necessarily need to sign anything
  - "The parents need to know" – HIPAA and informed consent
  - What happened if the patient arrives in the ER – what can you say and to who

Common HIPAA Privacy Myths

- The real rights of a personal representative
  - Pay attention to state law
  - When you can deny information to the personal representative
  - “I’ve seen (him/her) with the patient before – it must be OK to share”
  - “I can’t disclose a patient’s PHI if the personal representative signs the authorization”

Common HIPAA Privacy Myths

- Ask Cignet what not to do – what you can and cannot keep from the patient
- Psychotherapy notes – what are they really?
- “Patients can’t look at their psychotherapy notes”
- “If some else’s name is in the record, I can’t share it”
- What isn’t included in the designate record set or medical/claims record

Common HIPAA Security Myths

- Security is not just about technology
- The most significant risk is not hackers – it's people and many from the inside
- It's not just a one-time event
- Yes, the HIPAA Security Rule only covers ePHI but the HIPAA Privacy Rule covers everything else
- You really can't separate privacy and security – without security, there is no privacy

Common HIPAA Security Myths

- Role based access control – why it's required
  - Minimum necessary
  - Keeping those records confidential
  - Employee promotion or transfer – why old access should go away
  - Granularity not defined but important to use common sense

Common HIPAA Security Myths

- The importance of audit logs
  - If it's tracked and you don't look at it, it can hurt you
  - What the HIPAA Security rule really requires
  - "If I don't turn it on, I'm still compliant"
  - Audit log retention – two schools of thought and HITECH
  - "If the doctor looked at it, it must be OK"

Common HIPAA Security Myths

- Data backup & recovery
  - Why backup recovery testing is critical
  - “If it’s data at rest, I don’t need to encrypt it” – ask BCBS of Tennessee…
  - Where to store backup media and places to avoid
  - What about that non-electronic data?

Common HIPAA Security Myths

- Encryption myths
  - "If I'm sending it to a colleague, of course it's secure"
  - "Secure email is too expensive and a pain"
  - "I'll never lose my tablet"
  - "If it's inside my network, it's safe"
  - "All encryption is the same"

Common HIPAA Security Myths

- Workforce training
  - "Once is enough"
  - "The Omnibus Rule didn't change much"
  - "Don't worry about those temporaries – they won't be here long"
  - "HIPAA training is HIPAA training"
  - "They can just read those policies and procedures"
  - "It's in the employee handbook"
  - "Those affiliates can find their own training"

Common HIPAA Security Myths

- If you don't run regular malware scans, it won't work
- If you don't update it, it won't find that new malware
- What about those mobile devices, especially BYOD (bring your own device)?
- "It's just a web link, right?" – Phishing and other clear and present dangers

Common HIPAA Security Myths

- Just standing up that firewall isn't enough
- Remote desktops and the risk to harm and hackers – RDP and "man-in-the-middle"
- Just like anti-malware, it needs to be updated regularly (and hopefully not in production)
- Pay attention to those firewall logs

Common HIPAA Security Myths

- Mobile and local device management – where's the PHI?
  - "I prohibit storage of PHI on workstations – isn't that enough?"
  - "No one stores PHI on their smartphone or tablet"
  - "If they quit, they'll delete it"
  - That pesky USB drive
  - "It's in the policy"

Common HIPAA Security Myths

- Passwords
  - "It's OK not to change a password because the (insert health care professional title here) said so"
  - "It's easy to remember if it's the name of my (insert person or animal descriptor here)"
  - "It's OK to share – he/she is my assistant"
  - "Strong passwords are too hard to remember"
  - How about password length?

Common HIPAA Security Myths

- Open the door – “When someone quits, why change the (key, swipe card application, key pad combination, etc.)?”
- Open bins, open doors and chart racks
- Does everything need to be locked all of the time?
- How strangers wandering the halls can impact your organization
- Social engineering – just because they’re nice doesn’t meant they’re not up to no good

Common HIPAA Security Myths

- Yes, you do need to enable auto-logoff
- Myths around use of generic user names
- Network engineers – “We just trust them”
- New hardware and what not to do – the State of Utah provided the case study
- “The only system authentication needed is a password”

Common HIPAA Security Myths

- Wireless networks – how secure is yours?
- Parking lot surfing
- Is your guest network really secure?
- Mobile hot spots – easier to hack than you know
- “I installed a VPN – it’s all secure”

Common HIPAA Security Myths

- That risk analysis
  - "It's only technology"
  - "It's something to do with Meaningful Use"
  - "So I haven't done one in a few years?"
  - "I'll just get one of those generic checklists"
  - "EHR incentive program measure only requires I conduct a risk analysis"
  - "So it looks bad, I did it"

Common HIPAA Security Myths

- Contingency planning
  - "It's in the cloud and that's all I need"
  - "I know what to do – why write it down?"
  - "I just need to protect my hardware, software and data"
  - "My EHR takes four hours to recover – is that a problem?"

Common HIPAA Security Myths

- Breaches
  - "Security incidents and breaches are the same thing"
  - Who pays the bill – better to define in advance
  - "To avoid breaches, I'll encrypt everything"

Common HIPAA Security Myths

- Breaches
  - What really happens after that breach of 500 individuals or more's PHI?
    - OCR will call
    - Extensive document requests will occur
    - If you don't answer their questions, OCR will not go away
    - "Can I hide substitute notice on page 36 of my local weekly?"
    - Who really has the burden of proof?

Common HIPAA Enforcement Myths

- “If you violate HIPAA, you could go to jail”
- “You’ll go to jail and we’ll have to pay a big penalty”
- OCR does look at headlines and does investigate those complaints
- “Willful neglect” is a good way to pay a lot of money
- “My organization is small – OCR won’t go after me” – a lesson from Phoenix and Idaho

Summary

- Pay attention to what is really required
- You can make it more stringent but don't blame it on HIPAA
- Training is a key to the dispelling of myths
- Your biggest risk – people
- Privacy and security are processes and not one-time events
- If you aren't sure, don't believe the first vendor who walks through the door

Q&A

Apgar & Associates, LLC

Chris Apgar, CISSP

CEO & President

Post Office Box 80278 | Portland, Oregon 97280

503-384-2538 | 503-384-2539 Fax | www.ApgarAndAssoc.com