cognosante
minds on health

Healthcare Security
The Business Side

Barbara Filkins (GSEC, GCIH)
barbara.filkins@cognosante.com
805/524-4282

Privacy & Security Workshop
Connecting California to Improve Patient Care in 2011
July 14, 2011

Historical Perspective (Mine)

- Background:
  - Problem solving in Aerospace/C4I environment
  - Mentored by a ‘system engineer’ who emphasized the ‘big picture’
  - Infrastructure → distributed applications → security
- Transitioned to healthcare IT ~’96
  - Military Health System – networks and infrastructure
  - Interoperability and strategic planning – understanding the environment
  - Policy and procedure development – making business decisions work
  - Deep dive into mental health around 2000 opened my eyes to interoperability
  - And always seemed to get pulled into that security space…..
- Established a set of rules to live by:
  - Technology is not the center of the universe to a provider
  - Technology is part of the business equation to a health system
  - Know the language of health, but don’t expect your client to know that of IT
  - Identify opportunities that can be easily missed to develop understanding
  - Take the time to educate (and train) if needed

- And always that security space…

Security… must align with the business

- Understand the business drivers for security
  - Privacy →the business rules for security
  - Legislation/regulation → audit/compliance/sanctions
  - Avoidance → lost revenue, licensure, censure
  - Enabler →EHR, HIE, PHR
- Must make business sense
  - Economics - a factor for both network and security design
  - Need – exposure, compliance
  - Limitations – impact on usability and quality of patient care
- Consider how to present the business for security:
  - Cost-benefit analysis
  - Risk assessment that addresses and supports both strategic and tactical plans/decisions by management

Security…. is not just about technology

- Touches all aspects of a business
  - Administrative
    - How many contract provider staff have access to your information systems or buildings?
    - How is the coordination between your HR and your IT when an employee gets terminated or transferred?
  - Physical
    - It's 10 pm – where are your backup tapes or disks?
    - It's partly cloudy – do you know where your data is?
  - Technical
    - How many of those functional requirements you used to select your system contained "authorized user"?
- Don't just automate -- security architecture can include:
    - Policy, workflows that use limited technology
    - Training, management oversight

Security…has an (even small) enterprise focus

- Security is not a product feature
  - How many vendors have you heard state “my EHR is HIPAA compliant” when referring to security?!
- True security is more holistic
  - The workplace
    - Is security built into normal operational procedures and training?
  - The technical infrastructure:
    - How is the network designed?
    - What and where are the applications containing ePHI?
    - Is there any biomed equipment attached to the network?
  - Assessment and attention to detail
    - Is evaluation of the security posture done routinely?
    - Does the organization act on the results?
- And what will/does HIE certification mean in terms of security requirements?

Security… must not negatively impact usability

- Known fact:
  - Users will bypass security feature if the security feature prevents them from doing their job
  - It's know as a "work-around"
- Other considerations:
  - Security design must not impact patient safety
    - Does security impede timely access to critical information?
    - Does security have a deleterious effect on ergonomics?
  - Security must allow transparent conformity with the business rules
    - Privacy of patient information
    - Release of information
    - Role-based access

Security…. means knowing the future

- And acting on it
- Society:
  - Social networking and more openness about conditions
  - More engaged patients
  - More open communication between patient/providers
- Healthcare initiatives at the federal and state levels:
  - ACO/Medical Home
  - HIE/HIX
- Technology
  - Increased automation of healthcare (HIE/HIT)
  - More porous boundaries around sensitive data (cloud computing)
  - Growing demand for bandwidth to support advanced mobile devices (iPhone and iPad)
  - Federated authentication/authorization

In summary….

- Healthcare security -- architecture & implementation -- will continue to have interesting technical problems… and even more non-technical challenges
- So….
  - Be open to the whole picture
    - Understand a little bit of the ‘other side’ -- business
    - Keep the functional and technical sides firmly in mind
  - Communicate and collaborate
  - Stay informed on overall trends in healthcare, not just privacy and security
- Above all, use informed common sense in your approach to planning for, implementing, and executing security in your organization