

What's New?

- Since December, 2013 we have experienced the most severe privacy and data security breaches and incidents in our nation's history
 - T.J. Maxx
 - Target
 - Home Depot
 - Neiman Marcus
 - Sony
 - Verizon "super cookie" fine by FCC
 - EU vs Germany the Germanwings health privacy debate



What's New?

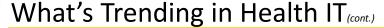
- But more than 90% of all breaches are not "public" breaches
 - Non-consumer based companies of all sorts
 - Hospitals, health systems, other "covered entities" and business associates
 - Disgruntled employees
 - IT vendors
 - Business process outsourcing providers (SaaS, IaaS, PaaS, "cloud")



What's Trending in Health IT

- Security
 - In 2014, 42% of all serious data breaches were in the healthcare sector
 - According to the FBI, in 2015, half of all healthcare organizations will have experienced between 1 and 5 cyber attacks in the prior 12 months, 1/3 of which will be successful





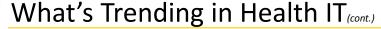
- A recent Harris poll of health technology decision makers revealed that healthcare organizations may be reassessing the role that compliance requirements play in protecting patient data
 - 54% said compliance requirements are the primary reason for protecting patient records
 - 68% said that compliance is an effective means of mitigating insider threats and data breaches
 - 63% are planning to increase breach prevention spending
 - BUT, 92% said that that are vulnerable to insider threats



What's Trending in Health IT (cont.)

- By 2020, it is expected that 80% of health data will pass through the cloud at some point in its lifecycle
- The datacenters that empower the cloud are becoming increasingly centralized and therefore subject to attack as business process outsourcing becomes an even more global enterprise and larger companies acquire smaller regional players





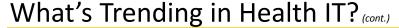
- The major national and international laaS players including Microsoft, Amazon, LexisNexis and others are accumulating market share
- The major regional players including Expedient and Bluebridge are working hard to compete by offering terms that are more protective



What's Trending in Health IT (cont.)

- Data analytics is ready for prime time
 - Driving operational and clinical decision-making and change
 - HIPAA administrative simplification modifications to the medical data code set for International Classification of Diseases (ICD)
 - ICD-10 effective date is October 15, 2015
- Telemedicine takes off?





- In the face of escalating risk, except in segments subject to regulation, corporate entities are not prepared from a policy or technical perspective to meet the challenge of privacy and security breaches
- Spending in this area is lagging clear evidence of necessity
- In-house IT departments are already overwhelmed and without the necessary depth



What's Trending in Health IT (cont.)

- In-house legal departments do not have the necessary expertise and are focused on breach response, rather than up-front preparation as a policy matter
- Breaches are becoming multi-billion dollar problems resulting from direct damages, penalties, lawsuits, loss of productivity, diversion of resources, and <u>reputational</u> harm
- Corporate boards are not responding quickly enough to meet the evolving threat



Federal Privacy and Information Security Law

- The United States does not have a comprehensive, well-defined body of privacy or information security law
- In the United States, federal privacy and information security law is made up of a patchwork of statutes, regulations and guidelines applicable to various industries and actors



What Laws Apply?

- For HIPAA "covered entities" and "business associates", we of course know that a well developed body of law exists <u>pertaining to</u> protected health information.
- But, a host of other state, federal and international laws, rules and regulations may also apply and every entity operating in the health information technology space must be aware of this body of law.



Federal Privacy Law (cont.)

- Healthcare Privacy
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Privacy Rule
 - Health Information Technology for Economic and Clinical Health Act (HITECH)
 - State privacy law
 - International privacy law (EU, Switzerland, EEA, AMEA, Australia, Canada, Mexico and Russia)



Information Security Law

- In the United States, there is even less welldefined federal law with respect to information security than with respect to privacy
- Well defined information security law does exist in certain areas such as:



Federal Information Security Law

- HIPAA
 - Security Rule
- Fedeal Health Information Security Breach Notification
 - HIPAA/HITECH
 - Interagency Guidance on Response Programs for Security Breaches
- State data security laws (47 states currently)
- International data security (EU, Switzerland, EEA, AMEA, Australia, Canada, Mexico and Russia)



Information Security Standards

- ISO 27001 series
- Statement on Auditing Standards (SSAE-16 /AT-101)
- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (NIST) Guidelines – HIPAA and HITECH



Where Should the Focus Be?

- Board level attention
- Effective risk assessment and analysis
- Data classification
- Comprehensive policies and procedures for privacy, security, data breach and incident response
- · Education and training
- · Global thinking
- Contracts IT, IP, Cloud, Vendor
- · Social media
- Protection of competitive intelligence and trade secrets
- Physical security



What Do Buyers Want?

CERTAINTY And CLOSURE



What Do Vendors Want?

CLOSURE AND CERTAINTY



Top 10 Ways to Get the Deal Done

Buyers and Vendors want the same things, <u>but in a</u> <u>different order of priority</u>



10. Understand that in a sophisticated health IT deal, a simple contract is not always a better contract because it is viewed by buyers and their counsel as unsophisticated and doesn't give them the necessary certainty



9. Understand that failing to offer reasonable market terms on data security and privacy can lengthen the sales cycle by months



8. Bring subcontractors to the table that are themselves fully compliant with applicable laws, rules and regulations, and stand behind them

Benesch

7. Realize that there is a professional (i.e., lawyer) who is going to need to opine on the deal before it gets signed and that professional is <u>not a risk taker</u>



6. If you are a vendor, realize that your customer knows that you are not likely to walk away from the deal and will use every strategic advantage to obtain the terms it wants and needs including pushing you to month, quarter and year end



5. If you are a vendor, realize that your customer knows that your threat to have to "redeploy the Ateam is usually not real



4. If you are a vendor, realize that your client wants the best terms you have and not the terms you give to lesser clients, and does not want to have to ask you for it

