



# Encryption: the Good, the Bad, the Ugly

*Stephen Treglia, JD, HCISPP  
Absolute Software Corporation  
Legal Counsel & HIPAA Compliance Officer,  
Investigations*

19<sup>th</sup> Annual Cyber Security Conference  
NYS Office of IT Services  
June 9, 2016

# First – Polling the Audience

- Helps me understand how to contour the presentation
- Lawyers?
- (Still just lawyers) Public. Private. Corporate.
- Public employees (whether or not lawyers)
- In health care (regardless of public/private, lawyers or not)
- In education (regardless of public/private, lawyers or not)
- Encounters “PII” (private identifiable info – regardless of position or public/private)
- Come in contact with credit card info (again, regardless)
- Law enforcement (at any level or category)
- Anyone not one of these?
- Probably not the last poll I’m asking today



# Speaker info:



**Stephen Treglia** – Esq., HCISPP, Legal Counsel & HIPAA Compliance Officer for Absolute’s Investigations Teams and co-leader of Absolute’s Health Care Investigations Team

- Completed 30-year career as a prosecutor in New York – last 25 years as an investigative prosecutor handling major organized crime, corruption and narcotic cases in NYC area for 10 years, and created and led one of world’s 1<sup>st</sup> computer crime units for his last 15 years
- Joined Absolute in 2010 – currently legal counsel to 40-member Absolute’s Investigations Team
- Beginning in 2013, requested to become more involved regulatory compliance & was appointed HIPAA Compliance Officer for Investigations
- In March, 2015, acquired HealthCare Information Security and Privacy Practitioner (HCISPP) Certification from the International Information Systems Security Certification Consortium (ISC)<sup>2</sup>
- Now co-leads Absolute’s **Health Care Investigations Team** – comprising 7 Absolute Investigators, all ex-law enforcement, all with privacy certifications

# Typical lawyer disclaimer

*Nothing said during this presentation should be considered legal advice. This is intended to be nothing more than a general analysis of broad legal principles in a scholastic setting. Legal advice is properly provided only when it is more finely attuned to specific facts and specific issues in a specific, real-life situation, which will not be provided at this presentation. When seeking legal advice in this area of law, look to counsel who is both knowledgeable in this area of law and fully understands how your business or enterprise operates.*



# Are you asking, “I’m no techie. Why do I need to know this?”

- I’m no techie, either, but ignorance is rapidly becoming no longer a valid option
- What kind of sensitive data do you deal with?  
(Especially you lawyers and law enforcement officers)
- But really, in all walks of business, commercial, service fields workers are constantly coming across personally sensitive data
- We’ll see there are serious legal consequences to using or not using encryption



# Accurate use of terms is CRITICAL



- Helps in understanding Encryption if you understand certain terms
- Cryptography is the all-encompassing term for secretive writing in its several forms
- Greek for the “practice and study of techniques for secure communications”
- Steganography is not Encryption
- Coding is not Encryption
- Encryption is not the same as Password-protected Data

# What is Steganography?

- Literally means, “hiding in plain sight”
- The info is there and unaltered
- You just don’t know where to find it
- Once uncovered, readily readable
- Earliest known form used by Greeks around 500 BC
- Info written on tablets covered by wax
- Or a tattoo on a soldier’s head hidden by outgrowing hair

## Past use :

- Hidden messages within wax tablets — in ancient Greece, people wrote messages on the wood, then covered it with wax .



Figure 1: Wax tablet with stylus from Demaratus' time.

# Another form of non-digital Steganography

- Hiding the message
- Invisible ink – one method
- Microdots – another method
- Shrinking a message to microscopic proportion
- Bury it within another message
- Popular practice during WW II

## Technical Steganography



- Uses scientific methods to hide a message, such as the use of invisible ink or microdots
- In 1941 the FBI discovered a Micro Dot carried on a letter from a suspected agent
  - Micro Dot production
    - Create a postage stamp sized secret message
    - Reduce this in size using a reverse microscope producing an image .05 inches in diameter
  - The dot was pressed onto a piece of paper using a hypodermic needle in place of a period



Mark IV microdot camera

# Modern forms of Steganography

- 2 different examples employing the same concept – a coded message interwoven within parts of another visible message (NOT encryption)
- Remember, “hiding in plain sight”
- Example 1 removes pre-determined letters from another **visible** message to provide the coded message
- Can do the same with “1s” and “0s” of computer code – Example 2
- Pre-determined binary characters, “visible” to the computer (1s and 0s that make up the individual pixels), are accumulated to provide the coded message

## Examples of steganography

### Example 1: Coded message

Apparently neutral's protest is thoroughly discounted and ignored.  
Isman hard hit. Blockade issue affects pretext for embargo on byproducts,  
ejecting suets and vegetable oils.

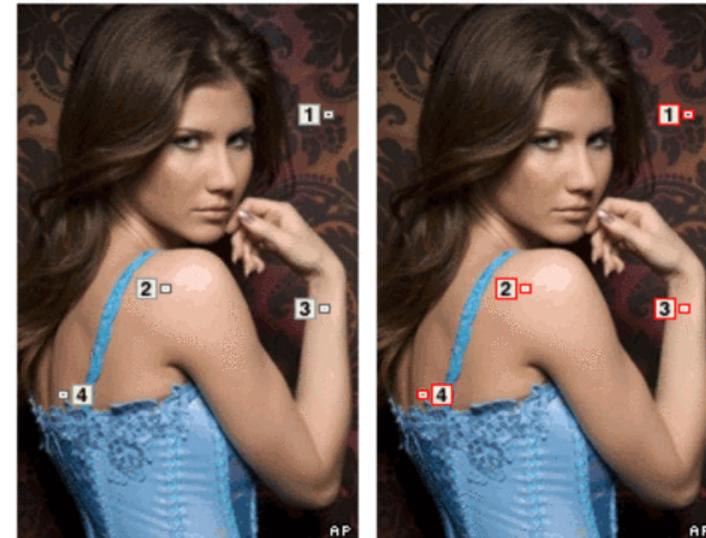
Take second letter of each word to get message:

**Pershing sails from NY June 1**

### Example 2: Coded images: Least Significant Bits (LSB) insertion

Original image

Altered image



Areas where binary code of pixel has been altered

Binary code from original image pixel 1

10000000 10100100 10110101 10110101 11110011 10110111 11100111 10110011 00110000

Changes made on altered image pixel 1

10000001 10100100 10110100 10110100 11110010 10110110 11100110 10110011 00110011

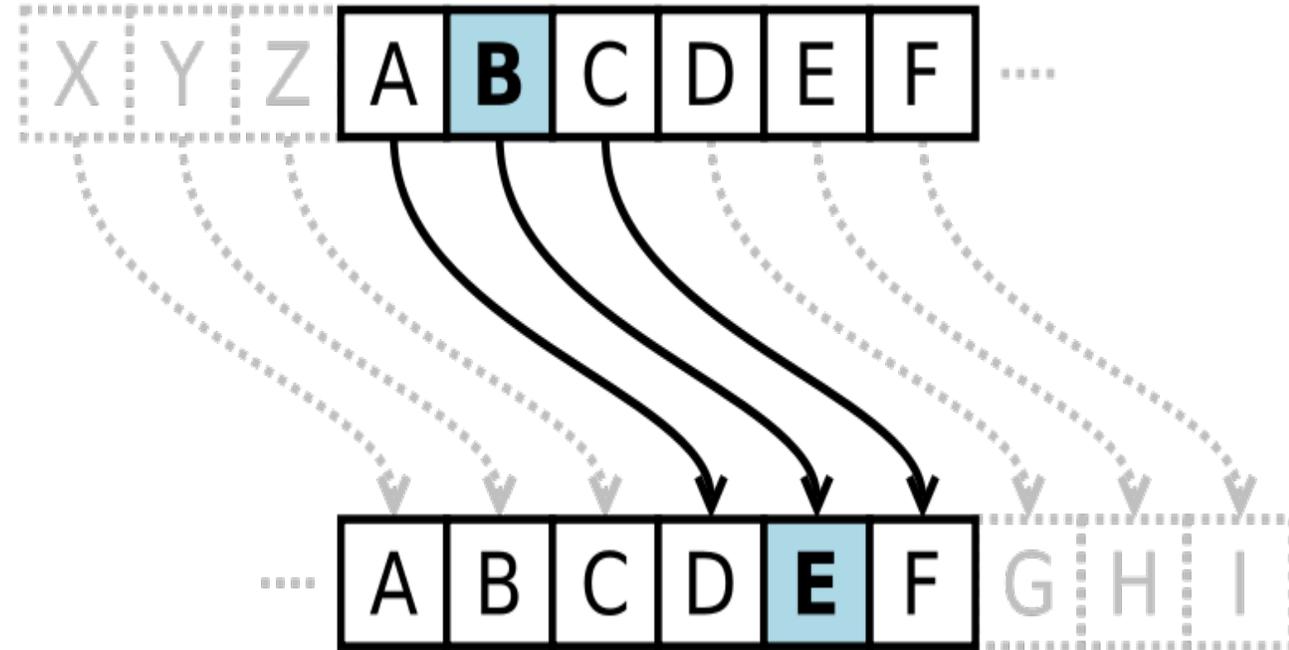
Read last digit:

1000001 which is ASCII binary code for A

1 2 3 4

# Using coded messages

- Switching message letters with other letters
- Again, technically not encryption
- Earliest known form called “Caesar’s Code”
- Originated at the time of Julius Caesar
- An alphabet off-set or “shift” of the alphabet
- If you know the number of the off-set (i.e., 1 letter, 3 letters, 10 letters, etc.), you can decode the message



# Variation of Caesar's code

- Original version only has 25 code possibilities
- Doesn't take a lot of time to crack
- If the letter exchange is random, however, and not just off-set, there are now millions of possibilities
- As demonstrated in the recent hit movie, "The Imitation Game," if you change the code everyday, the ability to crack the code becomes much tougher
- Forced Alan Turing and his team to create the forerunner of the modern computer to crack the new code each day



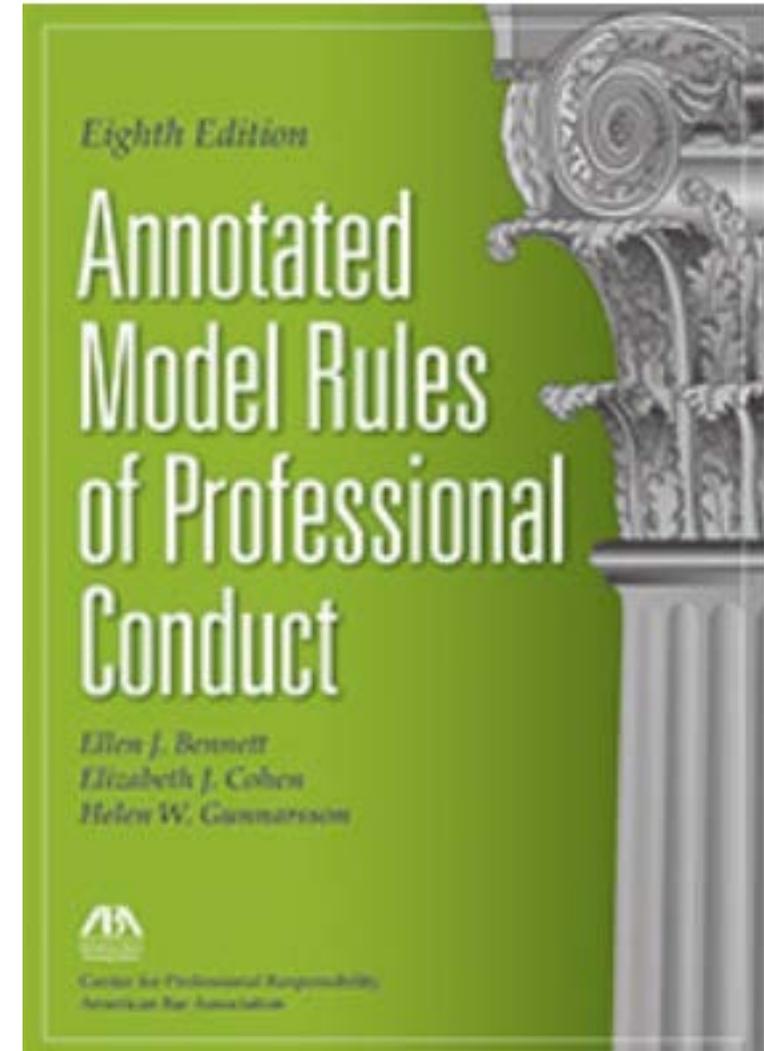
# Passwords are not encryption

- Passwords do not alter the text or depiction sought to be protected from discovery
- Passwords merely prevent access to data
- Encryption, rather, alters the very appearance of the of the data being protected
- Turns it completely unintelligible to a human reader
- Unless you know the decryption key
- Which “translates” the encrypted text/picture into words or images that can be understood by humans



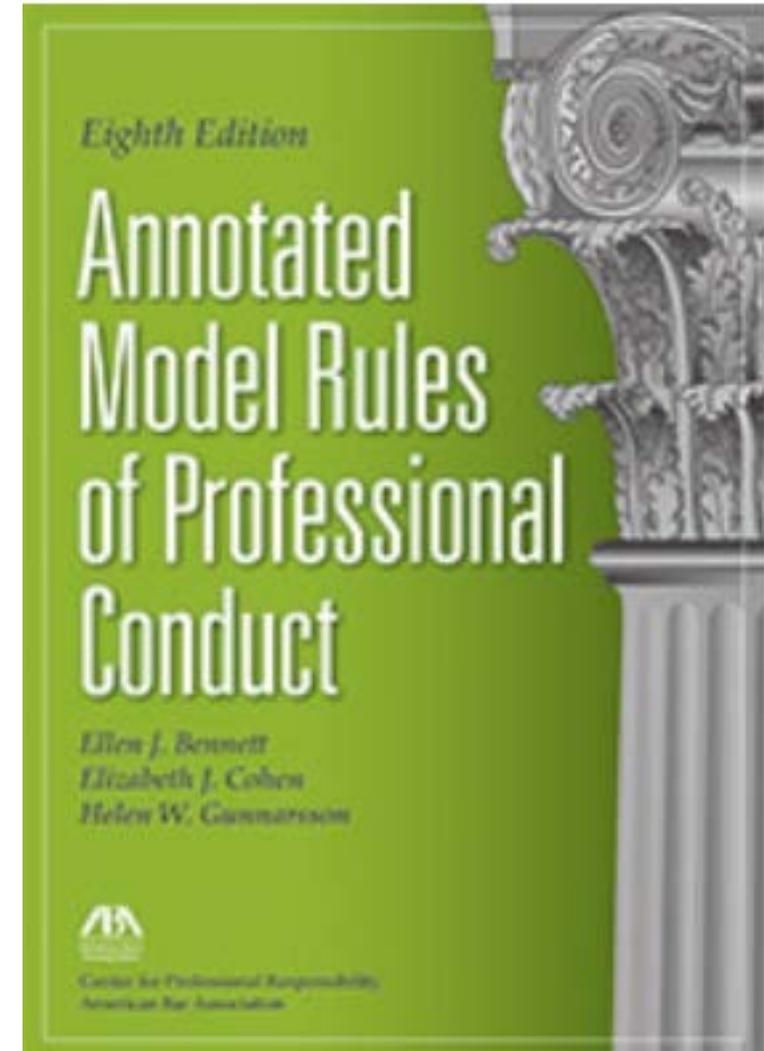
# Requirement for lawyers using technology

- Model Rules of Professional Conduct
- Rule 1.1 – "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
- Comment 6 to this Rule recently added that lawyers should keep up with changes in the law and its practice, "including the benefits and risks associated with relevant technology."
- Rule 1.4 – Pertains to the confidentiality of lawyer-client communications
- Comment 4 to this Rule expands this confidentiality rule to all forms of communications, even beyond phone calls



# Explicit requirements to respect data privacy rules

- Rule 1.6 – Section (c) requires lawyers to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."
- Comment 18 to this Rule warns lawyers that other laws, such as state and federal laws governing data privacy or breach notification requirements, may also impose other requirements.
- Some “other laws” are imposing breach notification and encryption requirements
- And these data privacy requirements are only beginning to evolve



# HIPAA-HITECH most prominent encryption requirement

- Section 164.312 – “A covered entity or business associate must...”
- Sub-paragraph (a)(2)(iv) – “Implement a mechanism to encrypt and decrypt electronic protected health information.”
- A law firm helping a health care practice is, by law, a “Business Associate”
- Important to note that encryption is only an “addressable” duty, as opposed to “required”
- In this case, however, a distinction with no substantive effect



# “Addressable” vs. “Required”



- Section 164.306 (a) – “*General requirements*. Covered entities and business associates must do the following:”
- (3) When a standard includes addressable implementation specifications, a covered entity or business associate must
  - (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment;... and
    - (A) Implement the implementation specification if reasonable and appropriate; or
    - (B) If implementing the implementation specification is not reasonable and appropriate—
      - (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and
      - (2) Implement an equivalent alternative measure if reasonable and appropriate.

# So must you encrypt under HIPAA-HITECH?



- Addressable means it's not required – so, technically, no, it's not absolutely required
- BUT addressable DOESN'T simply mean you can get away with doing NOTHING!
- You must first analyze and document why encryption's not appropriate
- Then implement “an alternative equivalent measure if reasonable and appropriate”
- What's an alternative equivalent to encryption?
- If you agree there's none, why is it reasonable and appropriate not to encrypt?
- Bottom line – you have to encrypt

# Encryption is NOT a Get-Out-of-Jail-Free Card

- No court or regulatory agency has yet to so rule
- Need to look at statutory/regulatory language
- 79 Federal Register 74, at page 19009, issued 2 months after HITECH Act went into effect

**PHI considered encrypted as long as “such confidential process or key that might enable decryption has not been breached.”**

*B. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies:

(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key”<sup>15</sup> and such confidential process or key that might enable decryption has not been breached.



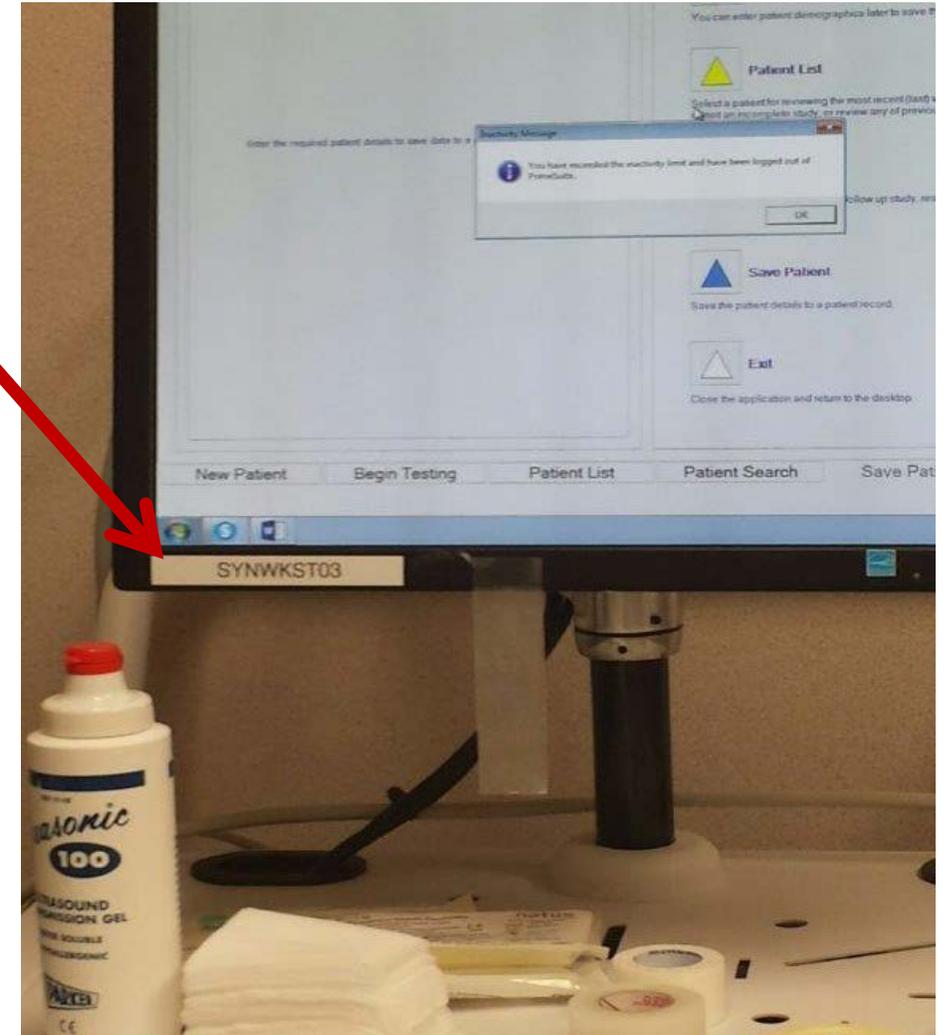
# Ways encryption can be defeated



- Brute force attack, successful with cracking passwords, next to impossible to crack encryption
- Sticky note on device – much more common
- Mistakenly granted administrative rights – disturbingly way too common
- Closing upper half of laptop without turning off device
- Device stolen by someone who knows the decryption key – also quite common
- Ran Federal Register issue & these example past representatives of FTC, FCC, SEC, NY Attorney General at Cybersecurity Conference last summer
- All agreed use of encryption under these circumstances is NOT a safe harbor

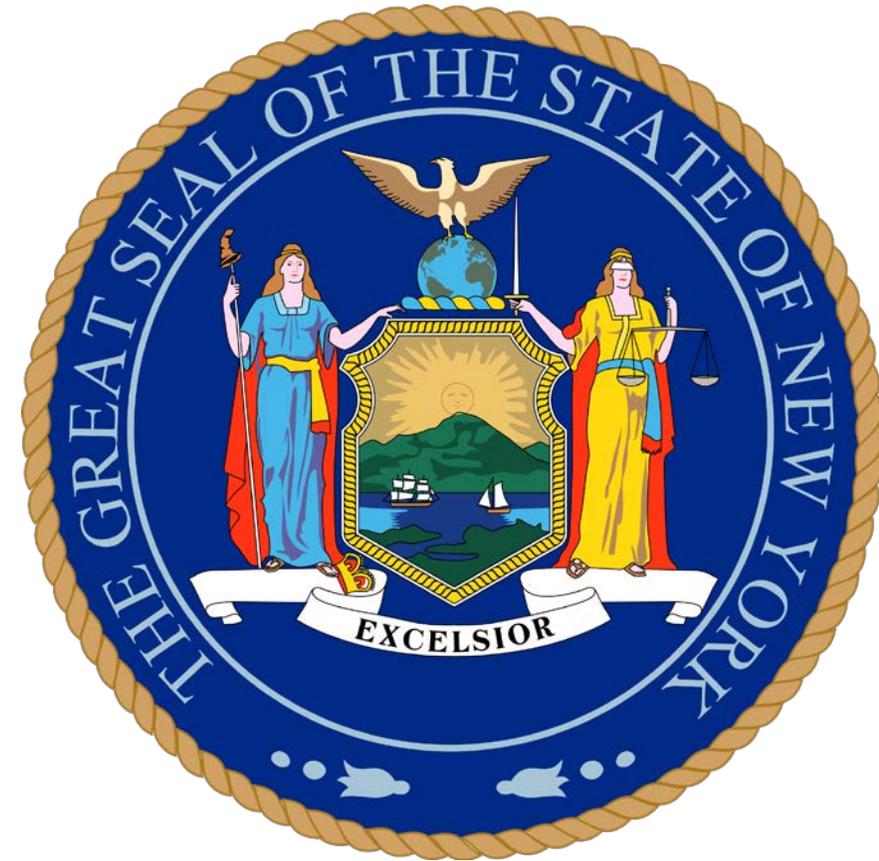
# A true-life story of encryption is not enough

- Major U.S. neurological clinic
- Every witnessed device had the device registration number on the front of the monitor
- And the device's decryption key on the back
- Multi-floor buildings
- Every type of access device, desktop or portable, literally thousands of machines
- When clinicians confronted, response was, "Too many devices used by multiple people. HIPAA requires encryption, but there's no other way to manage this"

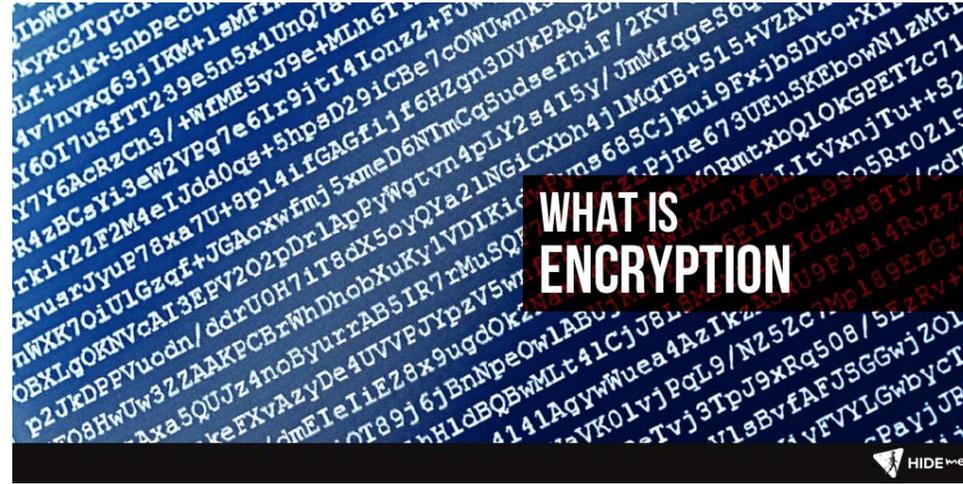


# HIPAA-HITECH not alone in encryption safe harbor

- New York's breach notification laws a prime example
- Encryption NOT a requirement in NY
- But it can protect you from a breach notification
- NY's General Business Law §899-aa, subd. 1(b); and Technology Law §208, subd. 1(a)
- Both have the same safe harbor provision
- A breach occurs if an unauthorized person accesses personal information "when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired"



# So what exactly is encryption?



- Not my purpose here to go into it at any great length & definitely not to go over the different brands
- This is predominantly a legal presentation which only touches on detailed technical issues, so we're only looking at the "bigger picture"
- Want the details, talk to an IT person
- Encryption alters the original message (often called "plaintext")
- In a manner unreadable to humans (often called "ciphertext"), but decipherable by a computer
- Unlike coded messages, figuring out what one character might represent does NOT necessarily carry over to other appearances of the same character

# How is data encrypted?



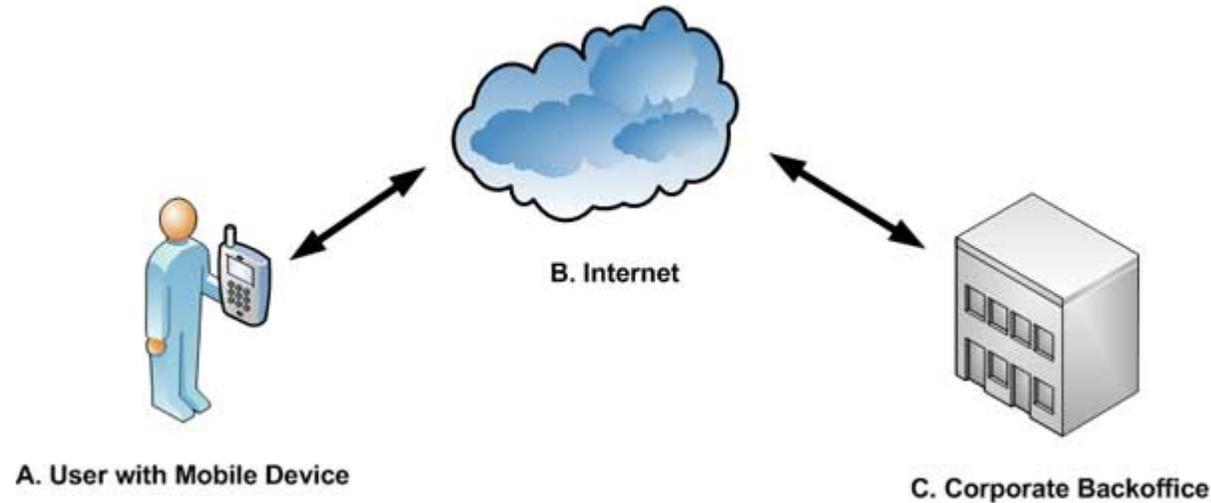
- Every version of encryption deploys an algorithm to encrypt the plaintext data
- An algorithm is a complex mathematical formula
- For example, the encrypted data in the following bulletpoint reads, when decrypted, “Come on over for hot dogs and soda.”
- Here is how it looks in encrypted format:
- wUwDPglyJu9LOnkBAf4vxSpQgQZlitz7LWwEquhdm5kSQIkQlZtfxTSTsmawq6gVH8SimlC3W6TDOh  
hL2FdgvdIC7sDv7G1Z7pCNzFLp0lgB9ACm8r5RZOBiN5ske9cBVjlVfgmQ9VpFzSwzLLODhCU7/2T  
Hg2iDrW3NGQZfz3SSWviwCe7GmNlvp5jEkGPCGcla4Fgdp/xuyewPk6NDIBewftLtHJVf=PAb3

# What types of data gets encrypted?



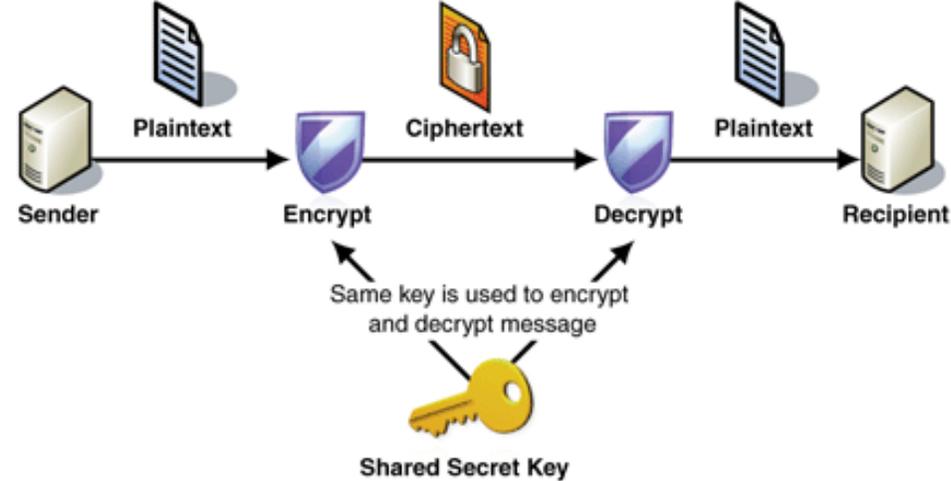
- Obviously, you should encrypt anything that “sensitive”
- E.g., personal identifiable information (PII), protected health information (PHI), credit card transactions as required by the Payment Card Industry (PCI), privileged communications, intellectual property, etc.
- Sensitive data is often described as “at rest” or “in motion” (also called “in transit”)
- Data “at rest” means data “in storage”
- Such as saved on a hard drive

# Data in transit



- Data that leaves user's control and is sent to another computer is "in motion" or "in transit"
- Far greater risk this data might wind up in the possession of unauthorized persons
- Certain "at rest" data is also highly vulnerable – a hybrid of "at rest" and "in transit"
- Data stored on a mobile device is technically "at rest"
- But the device itself is mobile, so, in a sense, the data is still "in motion"
- Also easily accessible by unauthorized persons
- Hence, also very necessary to encrypt "at rest" data on mobile devices

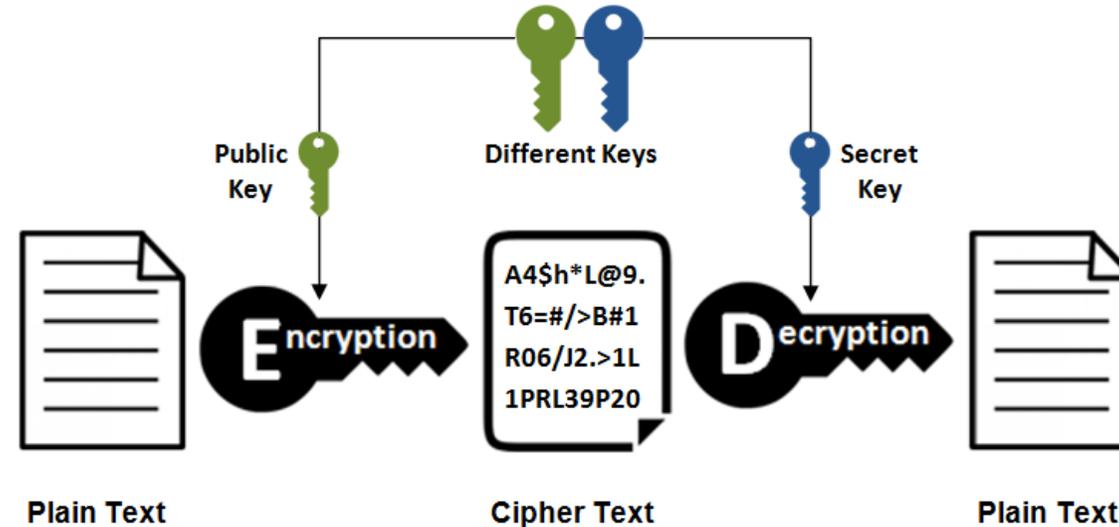
# How to encrypt data “in transit”



- “Symmetric” vs. “Asymmetric” methods
- Symmetric method easier to use
- The algorithmic formula used to create the encryption key to change the plaintext to encrypted “ciphertext” is the same key in the possession of the recipient to decipher the message back into plaintext
- Very risky form of encrypting “in transit” data
- It’s like giving your neighbor the key to your house when you’re away on vacation, and not bothering to get the key back after you return home

# “Asymmetric encryption”

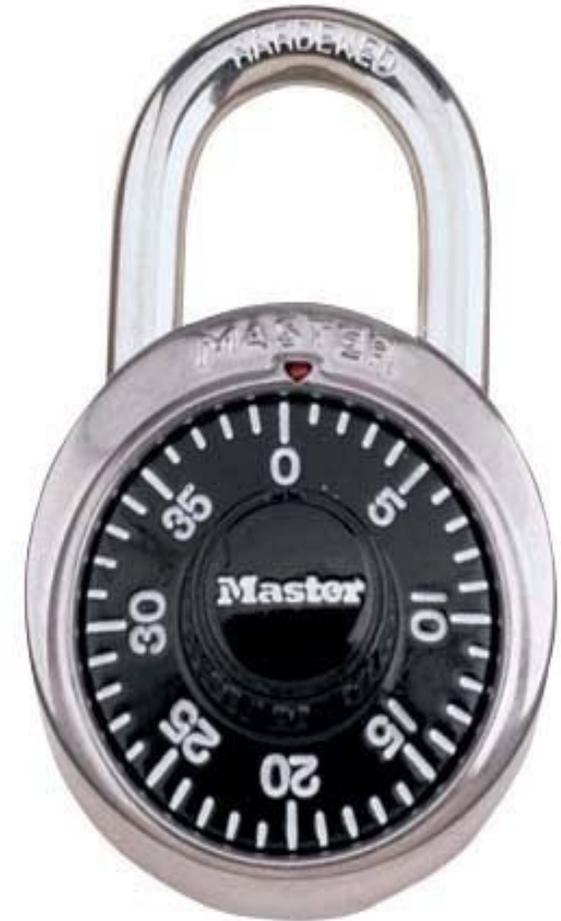
## Asymmetric Encryption



- Often called “Public Key” – “Private Key” method
- Intended recipient gives anyone sending text to him/her the same “public encryption key” that can be used by any person encrypting and then sending text to the recipient
- However, this ciphertext message can only be deciphered by the recipient’s use of his/her “private key” which no one else possesses
- Much safer means of encrypting data “in transit”

# How difficult is it to “crack” an encryption cipher?

- It is reported as being extremely difficult to “brute force decrypt,” if not virtually impossible
- The possible combinations of the encryption keys’ components are too numerous
- Takes the biggest computers dozens of years working non-stop to find the right combination
- For a more understandable analogy...
- A Master combination lock has 64,000 possible unlocking combinations (40 x 40 x 40)
- Equivalent of about “16-bit encryption”
- Best encryption today is “256-bit encryption”
- Soon to be “512-bit encryption”



# Dire consequences for not encrypting – \$100+ million hit for loss of a single laptop (and climbing)



7/2011  
 Employee laptop containing  
 information on 23,000 patients  
 stolen.

7/2012  
 \$2.5M HIPAA Settlement  
 pursued by MN AG.

6/2013  
 Class action  
 lawsuit.

9/2013  
 \$14M Class  
 Settlement

12/2013  
 FTC  
 Settlement.

- Federal HIPAA action pursued by Minnesota AG
- \$2.5M HIPAA penalty settlement
- Company cannot operate in Minnesota for 2-6 years
- \$23-25M/year estimated loss of revenue
- \$14M Class action shareholder suit settlement

# Other failings by Accretive – important practices beyond merely health care data safety



- Failure to have policies and procedures regarding encryption
- Failure to have policies and procedures regarding how to protect laptops containing PHI
- Failure to conduct a risk assessment that might have caught the lack of these policies & procedures
- Failure to train employees on the proper use of laptops containing PHI
- Failure of supervision to spot any of these failings (including failure to audit employees' activity)

# Accretive's breach extends to others

## \$1.55 million settlement underscores the importance of executing HIPAA business associate agreements

- From HHS website, this March, 2016 press release announced North Memorial Health Care of Minnesota (NMHC) settles \$1.55 million with HHS
- Accretive was a Business Associate (BA) of the hospital
- NMHC lacked BA agreement with Accretive and failed to do an organization-wide risk analysis of its BA
- Moral of story – every Covered Entity (CE) is responsible for its PHI data possessed by every BA in its downstream
- Moral #2 – even though NMHC lost no PHI data, it still committed HIPAA violations for not following all requirements made of CE with its downstream

# HITECH Act – harbinger of data privacy rules coming to other industries in possession of personal data?



## Burden of proof has changed

- Breach of protected data resumed if such data leaves the hands of authorized users
- Unless it can be established, there is a LOW PROBABILITY that, based on a risk assessment, no protected health information was acquired by or transmitted to unauthorized persons
- Forensic analysis is one of the authorized means
- State AGs can bring HIPAA actions
- Fines/penalties GREATLY enhanced
- A Covered Entities' Business Associates (which, by definition, can include a law firm) must also comply
- Remember, encryption alone is not enough
- But helps greatly if you can show it was never deactivated



If there is no breach, there is **NO REQUIREMENT OF NOTIFICATION**

**WARNING – Failure to do pre-breach preparation may even be a security violation**

# Perfect demonstration of evolving nature of data regulation

- Last 9 months has shown dramatic changes in the EU
- October, 2015, *Schrems v. Data Protection Commissioner*, abolished the 15-year Safe Harbor Agreement between the EU & US and was replaced in February, 2016
- Somewhat unrelated that same month, has been the superseding of the 1995 EU Data Protection Directive with the new General Data Protection Regulation
- Directive only recommended rules, Regulation will require
- Adopts breach notification for the first time
- Institutes a statutory “Right to be Forgotten”
- 4% global gross revenue penalty for violations



# Recent court battles over forcing Apple to decrypt iPhones

- Courts have gone both ways
- On 2/16/16, a federal judge (Central District of California) granted law enforcement's request to compel Apple to bypass its encryption to give them access to a cell phone believed to be in the possession of one of the terrorists in the San Bernardino attack
- On 2/29/16, a federal judge (Eastern District of NY) denied such a request in a drug case
- In the San Bernardino case, the court's order became moot as law enforcement found a way to overcome the encryption
- A subsequent reapplication before another EDNY judge in the drug case was again denied on 4/15/16

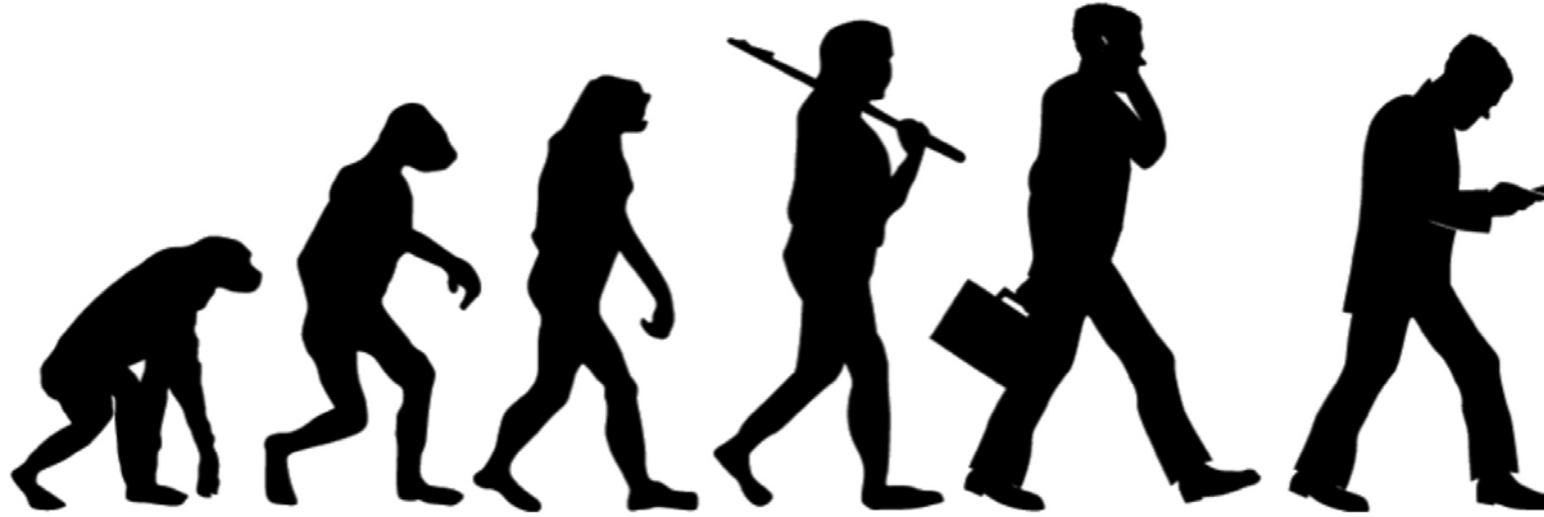


# Reasons for the denial in the NY case?

- Law enforcement had not exhausted all other remedies
- No evidence it contacted other law enforcement agencies to see if anyone had a solution
- Specifically mentioned was the San Bernardino case
- Why were they able to decrypt, and the New York authorities had not contacted them to find out how?
- A bit more disconcerting is the finding by both New York federal judges is that the “All Writs Act,” used to request the order compelling Apple to assist, does not grant the authority law enforcement sought
- Congress is considering enacting amendments to the All Writs Act to compel compliance in future cases



# Conclusion – What does this all mean?



- We're still in an evolutionary stage of technology
- Although we've hit something of a relative plateau the last couple of years
- But the law and regulatory fields are growing rapidly
- And enforcement actions based on these laws and regulations have only just begun
- The time to simply just stand by and watch how this will play out is over

# Solutions for those who have to deal with this responsibility?



- If you're not tech savvy, GET so NOW
- DON'T wait until a security/privacy response is imminent
- Talk to your IT people until YOU understand what's going on – don't let them snow you
- Talk to all relevant stakeholders – managers, C-suite, IT supervisors
- Realize from the start that one size does NOT fit all
- Multiple capabilities often requires alternative solutions (e.g., mobile vs. stationary)

# Any questions?

