PLAN
PROFESSIONAL LIABILITY
ATTORNEY NETWORK

HIPAA/HITECH Compliance:

Best Practices in Data Privacy and Security

Webinar Overview

- Why healthcare matters
- HIPAA Basics
  - Privacy Rule
  - Security Rule
  - Enforcement Rules
- Responding to healthcare data breaches
- Developing issues in healthcare privacy
- Best practices for compliance

Healthcare Data Security By the Numbers . . .

- **804** breaches of protected health information (PHI) between 2009 and 2013
- **29,276,385** health records affected by breach between 2009 and 2013
- **7,095,145** breached health records in 2013
- **137.7%** increase in records breached 2012-2013

. . . In Perspective

- The healthcare industry represents **43.5%** of all data breaches

- **90%** of health care organizations have lost patient information

Where Do Records Come From?

- Treatment: medical history, lifestyle details, lab test results, medications, research participation
- Insurance: payment records, applications for disability, life, or accident insurance
- Employment: medical exams and inquiries
- Individuals: online searches, support groups, mobile apps monitor their health and fitness

Why Healthcare Records?

- Medical info is "worth 10 times more than . . . credit card number[s] on the black market"[1]
  - Medical Records: approx. $50 each
  - Credit cards: approx. $1 each
- Potential black market use:
  - Fraudulently bill insurance or Medicare
  - Use information for free consultations
  - Obtain prescription medications

[1] www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals

Where and How Is Healthcare Data Breached?

© Mike Baldwin / Cornered

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

	# INCIDENTS (2013)	%	# RECORDS	%
Laptops and other portable devices	69	34.7%	1,876,349	26.4%
Desktops and servers	49	24.6%	4,343,440	61.2%
Paper	38	19.1%	390,144	5.5%
Other	17	8.5%	406,190	5.7%
Email	16	8%	51,419	0.7%
Electronic Medical Records	10	5%	28,563	0.4%
Total	**199**	**100%**	**7,096,105**	**100%**

Redspin, “Breach Report 2013: Protected Health Information (PHI)” (February 2014), available at: www.redspin.com

	# BREACHES (2013)	% OF TOTAL	# RECORDS	% OF TOTAL
Theft	90	45.2%	5,905,595	83.2%
Other	26	13.1%	320,314	4.5%
Unauthorized Access	44	22.1%	313,353	4.4%
Improper Disposal	8	4.0%	288,167	4.1%
Loss	19	9.5%	150,282	2.1%
Hacking IT Incident	12	6.0%	118,394	1.7%
Total	**199**	**100%**	**7,906,105**	**100%**

Redspin, “Breach Report 2013: Protected Health Information (PHI)” (February 2014), available at: www.redspin.com

HIPAA Overview

- 1996 – Congress passed HIPAA
- 2003 – HHS issued and adopted the Privacy Rule, Security Rule, and Enforcement Rule
- 2009 – HITECH Act signed into law to address electronic medical records
- 2013 – HHS issued HIPAA Omnibus Rule

Who Is Covered?

- Health plans
- Health care clearinghouses
- Health care providers who electronically transmit health information with covered transactions (e.g. billing, claims, eligibility)
- Business associates: functions on behalf of a covered entity that involve use or disclosure of identifiable health information

Business Associates

- Creates, receives, maintains, or transmits PHI on behalf of a covered entity
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a covered entity that involves disclosure of PHI
- Business associate now directly responsible (and liable) for complying with HIPAA

Who Is Not Covered?

- Life and long-term insurance companies
- Workers compensation insurers
- Employers
- Search engines and websites that provide health information
- Gyms and fitness clubs
- Many health and fitness apps
- And the list goes on . . .

Protected Health Information

- Information that relates to:
  - Past, present, or future physical or mental health or condition;
  - Treatment provided to a person; or
  - Past, present, or future payment for healthcare and individual receives; and
- Identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual

Privacy Rule

- Defines and limits circumstances in which an individual’s PHI may be used or disclosed
- Basic principle: may not use or disclose PHI, except: (1) as Privacy Rule permits or requires; or (2) as authorized in writing by the individual or his representative
- Applies to PHI that that is transmitted or maintained *in any format or medium*

Minimum Necessary Rule

- Must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose
- Does not apply to internal use for treatment or disclosures to other health care providers for treatment
- Covered entities and business associates must have policies and procedures designed to ensure compliance

Effect of *U.S. v. Windsor*

- In September, OCR provided guidance concerning *Windsor's* application to the Privacy Rule
- "Spouse" includes individuals who are in a legally valid same-sex marriage
- "Marriage" includes same-sex marriages, and "family member" includes dependents of those marriages where permitted by law

Current Issue: Records “Snooping”

- Nebraska Medical Center fired two workers in September for inappropriately accessing medical records of Ebola patient
- Similar incidents occur with celebrity or other high profile cases
- Good opportunity to review policies with workforce and emphasize zero tolerance

Security Rule

- Protects PHI that is created, received, maintained or transmitted in electronic form (e-PHI)
- Requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI

HIPAA-Required Administrative Safeguards

- Perform risk analysis to identify and analyze potential risks to e-PHI
- Designate security official responsible for developing and implementing policies
- Limit access to e-PHI only when appropriate based on user’s role
- Regular workforce training and management
- Periodic evaluation of effectiveness

Other Best Practices

- Confidentiality policies and agreements
- Data security and mobile device policies
  - Data Security Policy
  - BYOD Policy
  - Data Breach Response Plan
- Regular training of personnel
  - Create strong security culture
  - Study by Financial Times found that 93% of workers admit knowingly violating policies
- Enforce the policies consistently and equally

Factors Affecting Cost

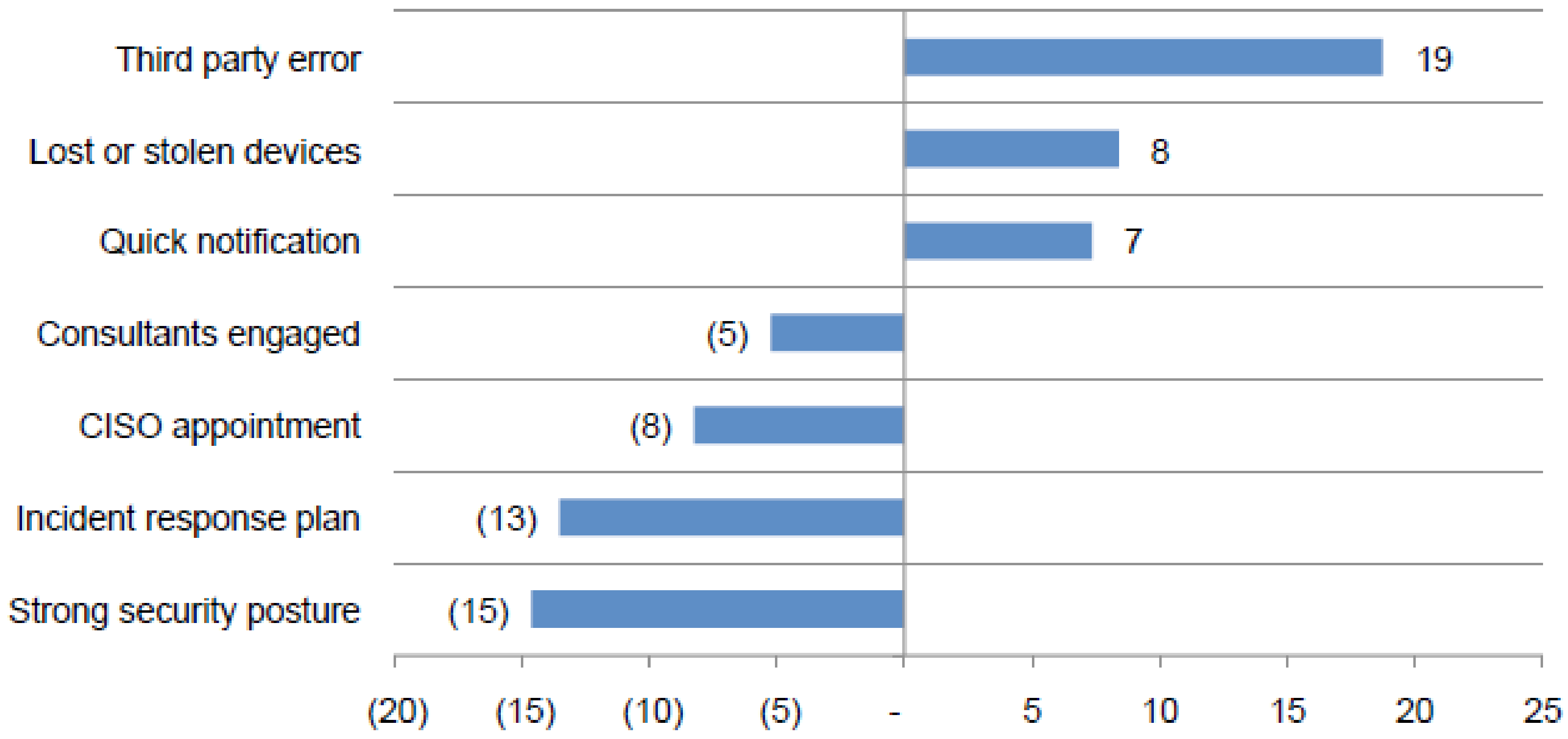


Figure 9. Impact of seven factors on the per capita cost of data breach
Consolidated view (n=277). Measured in US$

Source: Ponemon Research Institute, 2013 Cost of a Data Breach Study, www.ponemon.org

Business Associate Agreements

- Transition period for operating under old agreements expired on September 14, 2014
- Follow samples provisions posted by OCR
- Other issues to address: data breach coordination and response, indemnity, and agency status
- State laws (e.g., California, Massachusetts, Maryland) require businesses to have contracts with third-party service providers to safeguard personal information, which likely will include information in addition to protected health information under HIPAA

HIPAA-Required Physical Safeguards

- Limit physical access to its facilities while ensuring that authorized access is allowed
- Implement policies and procedures to specify proper use of and access to workstations and electronic media
- Implement policies and procedures for transfer, removal, disposal, and re-use of electronic media to protect e-PHI

Other Best Practices

- Limit access to only authorized individuals
- Limit device transfer and storage
- Workstation security: login required, strong passwords, logoff when not at desk
- Locked doors, warnings of restricted access, surveillance cameras, alarms, ID badges
- Secure IT equipment to immovable fixtures and store sensitive data in separate, secure area

HIPAA-Required
Technical Safeguards

- <u>Access controls</u> – polices should allow only authorized people to access e-PHI
- <u>Audit controls</u> – hardware, software, and/or procedural mechanisms to record and examine system access and other activity
- <u>Integrity controls</u> – ensure that e-PHI is not improperly altered or destroyed
- <u>Transmission security</u> – security measures that guard against unauthorized access to e-PHI being transferred over network

Other Best Practices

- **Encrypt all hard disks and portable devices!**
- Secure hosts and network (firewalls, anti-virus, anti-malware)
- Password protect all computers and devices
- Keep all software up to date
  - Upgrade from Windows XP
  - Patch browsers
- Install intrusion detection software

HIPAA Data Breach

- The unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information
- Three exceptions :
  - Member of workforce, acquires, accesses, or uses PHI in good faith without further violation of HIPAA
  - Inadvertent disclosure between two authorized individuals
  - When there is a good faith belief that unauthorized person would not be able to retain the information

Notification Rule

- Only applies if PHI was “unsecured”
- Presumed to be a breach unless covered entity or BA demonstrates there is a low probability that PHI has been compromised
  - Nature and extent of PHI involved
  - Person who gained unauthorized access
  - Whether PHI was actually acquired or viewed
  - Extent to which risk to PHI has been mitigated

Notification Requirements

- Individual notice – without unreasonable delay within 60 days by mail or e-mail if authorized by individual in advance
- Media notice – if more than 500 affected
- Notice to HHS – in all cases via website
- Business associates – must notify covered entity within 60 days (or as BAA specifies)

Federal Trade Commission

- Breach notification rule applicable to providers of web-based consumer personal health records (PHR) that are not subject to HIPAA
- E.g., online weight-tracking program that sends information to a PHR or pulls information from it
- E.g., HIPAA-covered entity such as a hospital that offers its employees a PHR

HIPAA Enforcement

- Individual may file complaint with OCR
- OCR Audit Program
- State attorney generals may file civil actions
- Some state courts recently have held that negligence claims for breach of patient privacy are not preempted by HIPAA
- A company called SLC Security recently said it will begin notifying individuals if it believes it has identified a security breach and it has not received a satisfactory response from the company

OCR Audit

- OCR has announced it will be resuming its audit program– which applies to both covered entities and business associates
- OCR wants to be able to see that the organization has taken steps to address the standards under the privacy and security rules.
- A documented risk assessment, written policies and procedures, and sign-off sheets showing workforce members went through HIPAA training are all examples

HIPAA Penalty Matrix

Violation	Penalty (per violation)	Total penalties for violating identical provision within a calendar year
Unknowing	$100 - $50,000	$1,500,000
Reasonable cause	$1,000 - $50,000	$1,500,000
Willful neglect – corrected	$10,000 - $50,000	$1,500,000
Willful neglect – not corrected	At least $50,000	$1,500,000

New Challenges and Threats

- Mobile devices
- Healthcare and fitness apps
- Social media privacy violations
- Implantable medical devices
- Third-party vendors and the cloud

Mobile Devices

- While laptops currently account for the majority of healthcare breaches, smartphones and tablets are on the rise
- Physicians increasingly using smartphones to exchange PHI. Survey showed:

- Over 80% of physicians acknowledge using smartphones to exchange PHI

- 107 responding pediatric hospitals used text messaging to communicate work-related information

Mobile Devices

- Smartphones introduce new avenues for hackers to access medical information
  - Messages containing e-PHI are often not encrypted and thus can be accessed by anyone with access to the device
  - Apps can read data stored on a handset, such as emails, text messages, attachments, and log-ins and passwords
  - Mobile data that leaves a device wirelessly to connect to a Wi-Fi network can be easily hijacked
  - Data automatically syncs with the cloud, which itself can be hacked

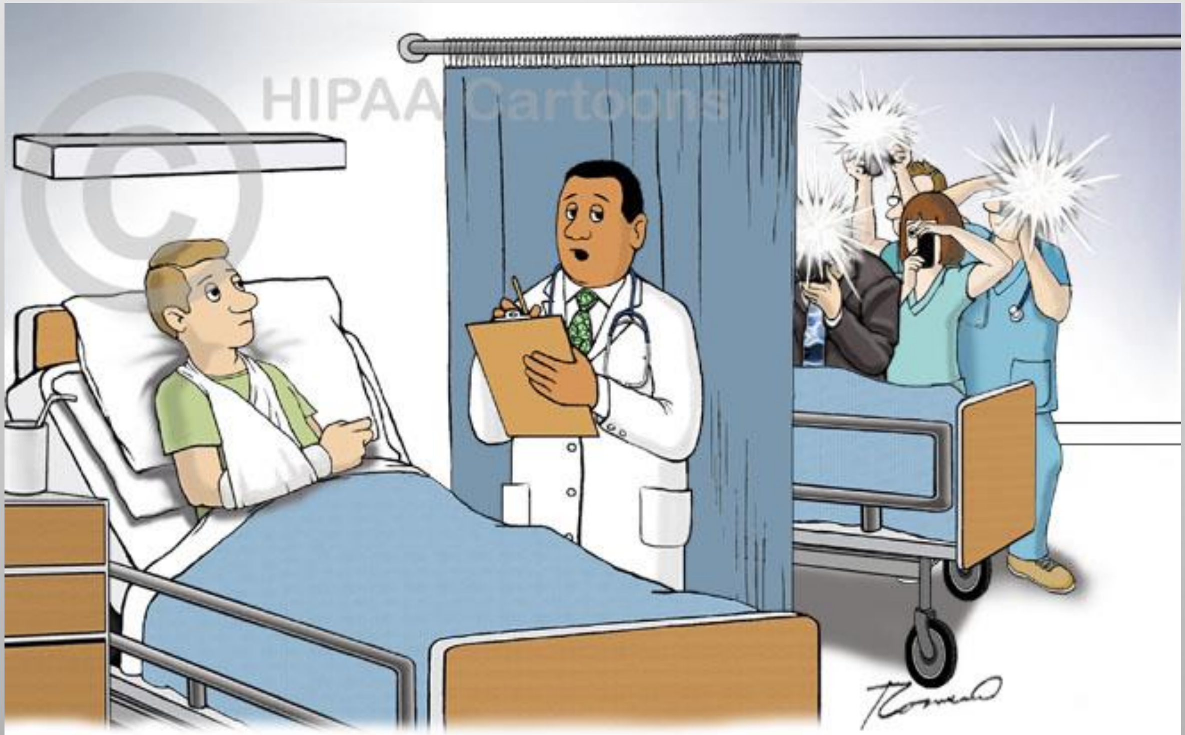
Other Risks of Mobile Devices

- Exchanging PHI on wireless devices exposes health workers to liability for HIPAA retention violations and spoliation of evidence
  - Since any message containing PHI must be retained for the legally required period of time , simply deleting a text message containing PHI may result in a HIPAA violation
  - Since any message containing PHI is part of the patient's medical record , deletion of text messages may expose the hospital to spoliation charges in subsequent litigation

Healthcare and Fitness Apps

- Mobile devices are great tracking tools that can offer many benefits, but amount of data also presents privacy risks
  - Name, age, gender, email address
  - Weight, height, photo, lifestyle information
  - Collected data (exercise, food, medicine, etc.)
- The ecosystem is largely unregulated – only have whatever protections developer provides

Social Media



"A celebrity? Oh, they aren't Paparazzi. Our staff likes to take interesting photos for their blogs and Facebook."

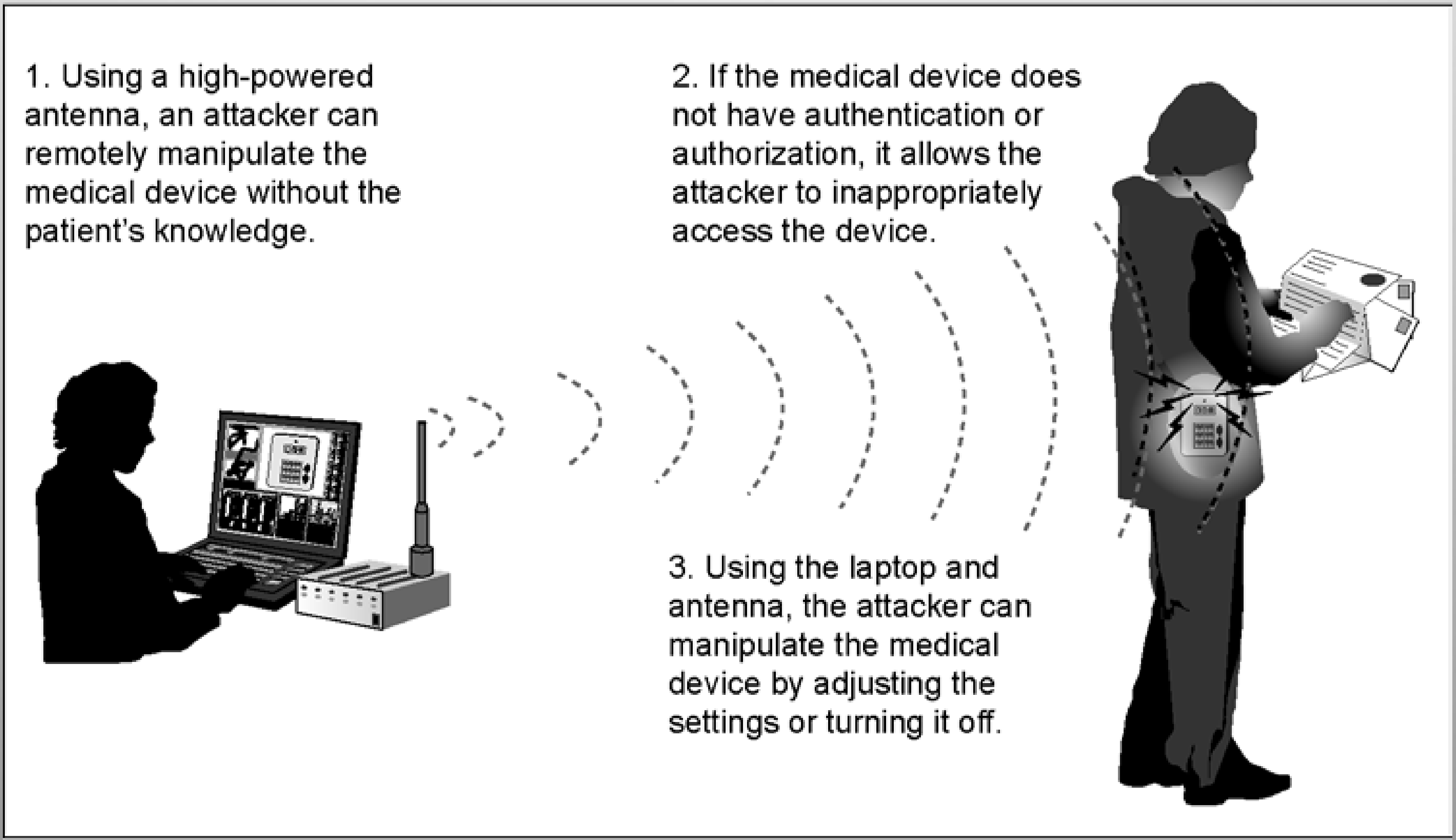
Privacy Breaches in Social Media

- Paramedic posted information about his patient’s sexual assault on his MySpace page.
- Nurses snapped photos of a man who had been stabbed more than a dozen times and posted them on Facebook
- Nurses discussed patients on Facebook
- Doctor conducting surgery on Joan Rivers allegedly snapped a selfie with Rivers before she died

Potential Cyber Attacks on Medical Devices

- Unintentional:
  - Interference from energy generated by other devices or from the surrounding environment
  - Defective software or firmware
- Intentional:
  - **Malicious actor** - person intercepting and altering signals sent wirelessly to the medical device
  - **Malware** – a malicious software program designed to carry out annoying or harmful actions.
  - **Denial-of-Service Attack** – launched using computer worms or viruses that overwhelm a device by excessive communication attempts, making the device unusable by either slowing or blocking functionality or draining the device’s battery

Example of Intentional Attack



1. Using a high-powered antenna, an attacker can remotely manipulate the medical device without the patient's knowledge.

2. If the medical device does not have authentication or authorization, it allows the attacker to inappropriately access the device.

3. Using the laptop and antenna, the attacker can manipulate the medical device by adjusting the settings or turning it off.

Source: GAO.

FDA Guidance on Medical Devices

- So far, no known malevolent software breaches have led to patient harm, but FDA is taking increasingly tough position
- In recent guidance, FDA recommends device manufacturers to send the following with their premarket submissions:
  - Hazard analysis
  - Traceability matrix
  - Summary of controls
  - Device instructions

FDA Guidance on Medical Devices

- More generally, FDA recommends focusing on 5 core functions to address and manage cyber threats on medical devices:
  - **Identify** risks posed by devices intended use
  - **Protect** the device against threats
  - **Detect** intrusions and notify user
  - **Respond** by showing user what to do
  - **Recover** by providing user means to authenticate

EHR Vendors and the Cloud

- Owner of data will always be responsible – cannot shift responsibility to vendor by storing data in the cloud
- Another interesting issue deals with access to cloud data:
  - In a current dispute, a third-party EHR vendor blocked a medical provider from accessing medical histories on its patients after the provider did not pay its monthly service fee for 10 months
  - Security Rule requires a business associate to “ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits”
  - Whether this requires making PHI available to the covered entity in this situation is an open question, but could be addressed in BAA