MAYER·BROWN

Medical Devices and Data:
PROTECTING PATIENTS AND THEIR PHI

Marcus Christian
Partner
mchristian@mayerbrown.com

Laura Hammargren
Partner
lhammargren@mayerbrown.com

Christopher Mikson, MD
Partner
cmikson@mayerbrown.com

Emily Strunk
Associate
estrunk@mayerbrown.com

Today's Presenters

Marcus Christian
Washington DC

Laura Hammargren
Chicago

Christopher Mikson
Washington DC

Emily Strunk
Washington DC

Topics to be Covered Today

- The FDA & Medical Devices
- HIPAA & PHI – Key Issues
- Trends & Best Practices for Enforcement and Investigations

FDA & MEDICAL DEVICES

FDA & Medical Devices: Introduction

- Cybersecurity concerns are rapidly growing across all sectors
  - World is increasingly dependent on information technology and networked operations. By 2020, some experts predict 200 billion connected “things” (personal devices, homes, cars, animals, hospitals, entire cities)
  - Examples of “things” that have been hacked:
    - *Infrastructure: power grid, dam, and traffic lights*
    - *Transportation: Cars and airplanes*
    - *Domain Name Service (DNS): Dyn attack in October 2016*
    - *Healthcare: Pacemakers, insulin pumps, and infusion pumps*
    - *Federal Agencies: compromise of information or functionality*

FDA & Medical Devices: Introduction

- Cybersecurity is the protection of information from unauthorized access and use (data breaches)
  - Cybersecurity protects all systems (not just information systems) from:
    - (1) *threats* (who is attacking) that exploit
    - (2) *vulnerabilities* (how they are attacking) and
    - (3) the resulting *impacts* (what the attack does)

Cybersecurity → Health Care → Medical Devices

- Health care is no exception!
- In the health care sector, medical devices are particularly vulnerable
  - Medical devices global market > $300 billion = many, many medical devices and opportunities
  - Medical devices used to be stand-alone equipment, but now have operating systems connected to networks and other devices, with far more potential for cyber attacks

Example – Ransomware Attack on a Medical Device

- Ransomware is one of the biggest cybersecurity threats
- An Example of just how easy a ransomware attack can be –
  - Company X manufactures a medical device that reads test data from lab samples. These machines are purchased by hospitals and medical centers, and results are used for diagnosing patients or for research.
  - The machine is networked so that it can upload data to doctors' and researchers' computers. The machine's manufacturer installs a standard password to access data on the machine. Users have an option to change the password but are not required to do so.
  - Hackers use the standard password to access a dozen of Company X's machines across the world and install ransomware on the machine, which encrypts all data until a ransom fee is paid to unencrypt the data.

Why Do We Need to Address Cybersecurity Threats to Medical Devices?

- Wide range of cyber attacks possible on medical devices
  - Unsecured communication ports
    - Allow downloading unauthorized firmware onto a device
  - Network vulnerabilities
    - Allow a hacker to alter medical records or actual treatment
  - Software vulnerabilities
    - Cause a device malfunction
  - Patients have been caught hacking their own morphine pumps!

Consequences of Cyber-Insecurity

- If cybersecurity threats are not properly addressed:
  - Potential for serious injury or death for patients
  - Increased time and cost burdens on the healthcare system (repairs, replacements, ensuring medical records accuracy)
  - Potential liability for those involved in the medical device industry (manufacturers, doctors, researchers, hospitals, academic research institutions)
  - Patients may lose confidence in advanced therapies which, in turn, could compromise patient care

How Does Government Regulation Address Cybersecurity Threats in Medical Devices?

- In addition to business reasons to protect against cyber threats, FDA has begun to develop a framework that incorporates cybersecurity considerations into premarket submission and Quality Systems Regulations (QSR) requirements

How Does Government Regulation Address Cybersecurity Threats in Medical Devices?

- FDA regulates approximately 30 percent of the gross domestic product (GDP) including
  - **Medical Devices** and Radiological Equipment
  - Pharmaceuticals and Biologics
  - Food and Dietary Supplements
  - Cosmetics
  - Tobacco

How Does Government Regulation Address Cybersecurity Threats in Medical Devices?

- Cybersecurity is an issue with all systems that are connected to a network across product areas
  - Many medical devices are networked and can thus be hacked to change treatment plans, medical records, dosages, etc.
- FDA has jurisdiction if the product meets the statutory definition of "**medical device**"
- FDA regulates from two principal standpoints
  - Safety
  - Effectiveness

Statutory Definition of “Medical Device"

- The Food Drug and Cosmetic Act (FDCA), 21 USC §§ 301 et seq., defines a medical device as
  - ***an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is***
    - Recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them;
    - ***Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals***; or
    - Intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.”

Statutory Definition of "Medical Device"

- Short Version
  - A medical device is a device that is intended to diagnose, cure, mitigate, treat or prevent a disease in man or other animals.
- Medical Device Software
  - Software is a medical device if it is intended to diagnose, cure, mitigate, treat or prevent a disease in man or other animals; OR that is the component of, or accessory to, any medical device.

Background and Timeline Highlights of Government Regulation of Cybersecurity

- February 2013–The White House issued Executive Order 13636 and Presidential Policy Directive 21 to formally recognize and bring attention to cybersecurity issues and strengthen critical cybersecurity infrastructure.
- FDA has also established formal partnerships with **Department of Homeland Security's** (DHS) Industrial Control Systems Cyber Emergency Response Team and entered into an MOU for collaboration with the **National Health Information Sharing and Analysis Center** (NH-ISAC) and the **Medical Device Innovation, Safety and Security Consortium** (MDISS)

Background and Timeline Highlights of Government Regulation of Cybersecurity

- June 2013–FDA issues safety communication to medical devices and hospital network advising them to take appropriate safeguards against cyber attacks and draft of guidance addressing cybersecurity in premarket submissions.
- October 2014–FDA finalized its guidance documents containing recommendations for incorporating premarket management of cybersecurity during the design stage of device development and held a public workshop for stakeholders.

Background and Timeline Highlights of Government Regulation of Cybersecurity

- May 2015–FDA issued its first product-specific safety communication for cybersecurity vulnerabilities in a medical device for an infusion pump product; two more have been issued since: one for a different infusion pump and one for an implantable cardiac device (no injuries or deaths were associated with any of these devices)
- December 2016–FDA finalized its guidance containing recommendations for addressing cybersecurity measures in postmarket compliance and held a public workshop for stakeholders.

Government Regulation of Cybersecurity

- Both FDA and FTC have taken a significant interest in cybersecurity.
- FTC–Concerned with consumer protection side. Does a data breach pose an economic harm to consumers? (i.e., someone obtains your information through a cybersecurity breach and then uses it to commit fraud of some sort (e.g., raid your bank accounts, submit fraudulent Medicare claims, etc).)
- FDA–Concerned with public health side. Generally concerned with keeping medical devices secure and maintaining functionality, but its focus is on cybersecurity vulnerabilities and exploits that present a reasonable probability of serious adverse health consequences or death.
- *Quick note: cybersecurity breaches may also implicate HIPAA when "protected health information" (as defined by HIPAA) is involved.*

Regulation of Devices by FDA and Other Agencies

Threshold Issue: Is the Device a Medical Device?

- Yes → regulated by FDA
- No → regulated by CPSC
- Either way → FTC will also have jurisdiction over consumer protection aspects of claims, cybersecurity

FDA Regulation of Cybersecurity Issues

- FDA’s role is to ensure the safety and effectiveness of medical devices at all stages of a device’s lifecycle and policy is evolving to address cyber threats
- Medical device manufacturers to consider cyber risks as part of it quality system regulation (QSR) obligations, and addresses specifics in guidance:
  - **Premarket Considerations**–Is Medical Device Software proactively designed to prevent cybersecurity vulnerabilities and exploits?
  - **Postmarket Considerations**–Does the manufacturer’s postmarket compliance program adequately address cybersecurity issues that may lead to safety or effectiveness concerns?

Premarket Considerations for Cybersecurity in Medical Devices

- FDA finalized guidance on *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (“Premarket Guidance”) in October 2014
  - Manufacturers should consider cybersecurity risks when designing and developing their medical devices–including design inputs, software validation and risk analysis–to better mitigate patient risks.
  - Supplements (1)*Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices* and (2)*Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*

Premarket Considerations for Cybersecurity in Medical Devices

- The approach should address the following elements:
  - Identify assets, threats, vulnerabilities
  - Assess the impact of threats/vulnerabilities on device functionality and patients (end users)
  - Assess likelihood of a threat and of a vulnerability being exploited
  - Determine risk levels and suitable mitigation strategies
  - Assess residual risk and risk acceptance criteria

Premarket Considerations for Cybersecurity in Medical Devices

- Additionally, the guidance:
  - Enumerates cybersecurity functions that are consistent with the NIST Framework (described below)
  - Lists required cybersecurity-related documentation and recognized standards

Postmarket Considerations for Cybersecurity in Medical Devices

- FDA finalized guidance on *Postmarket Management of Cybersecurity in Medical Devices* ("Postmarket Guidance") in December 2016
  - Cybersecurity risks are continually evolving and impossible to mitigate through premarket controls alone
  - Manufacturers should implement a comprehensive cybersecurity risk management program to monitor, identify and address cybersecurity exploits, consistent with the Quality Systems Regulation (QSR), as a part of their postmarket management of medical devices

Postmarket Considerations for Cybersecurity in Medical Devices

- The comprehensive cybersecurity risk management program should:
  - Apply NIST Framework;
  - Monitor cybersecurity information sources to identify and detect cybersecurity vulnerabilities and risks;
  - Maintain robust software lifecylce processes that incorporate monitoring third-party software, and verifying and validating software updates and patches;
  - Understand, assess, and detect the presence and impact of vulnerabilities;
  - Establish and educate on processes for vulnerability intake and handling;

Postmarket Considerations for Cybersecurity in Medical Devices

- The comprehensive cybersecurity risk management program should:
  - Use threat modeling to clearly define how to maintain safety and essential performance;
  - Establish a process to assess the severity of patient harm and residual risk;
  - Develop mitigations that protect, respond and recover from cyber risks;
  - Adopt a coordinated vulnerability disclosure policy and practice; and
  - Deploy mitigations that address cybersecurity risks early and prior to exploitation.

NIST Framework for Improving Critical Infrastructure Cybersecurity

- Although not required, FDA encourages the use and adoption of this Framework, which was developed by the National Institute of Standards and Technology (NIST).

ISAO–Information Sharing and Analysis Organization

- Although not required, FDA stresses the importance of information sharing via participation in an Information Sharing Analysis Organization (ISAO), a collaborative group in which public and private sector members share cybersecurity information.
  - FDA incentivizes participation with enforcement leniency; postmarket guidance defines “active participation.”
  - Information shared through ISAOs is protected from release under the Freedom of Information Act (FOIA).
  - FDA signed MOU with NH-SAC and MDISS the to help create an environment conducive to industry participation.

ISAO–Information Sharing and Analysis Organization

- For companies that voluntarily participate in an ISAO and follow recommendations in Postmarket Management Guidance, FDA will not enforce certain reporting requirements in cases where there are no serious adverse events or deaths associated with the vulnerability.
- Guidance defines “participation” in an ISAO. Manufacturer must:
  - Be a member of an ISAO with documented policies;
  - Share vulnerability information with that ISAO; and
  - Have documented policies for assessing and responding to vulnerability and threat intelligence from the ISAO.

NIST Framework of Identify/Protect/Detect/ Respond/Recover

- Identify
  - Maintaining safety and essential performance
  - Identify cybersecurity signals
- Protect/Detect
  - Characterize and assess identified vulnerabilities
  - Conduct and periodically update cybersecurity risk analyses that include threat modeling

NIST Framework of Identify/Protect/Detect/ Respond/Recover

- Protect/Detect
  - Analyze possible threat sources
  - Incorporate design features that establish or enhance the capability of the device to detect and produce forensically sound postmarket evidence to capture in the event of an attack
  - Develop process to assess the impact of a cybersecurity signal horizontally (across all devices) and vertically (within all elements of the devices)

NIST Framework of Identify/Protect/Detect/ Respond/Recover

- Protect/Respond/Recover
  - Implement device-based features as a primary mechanism to mitigate the impact of the vulnerability on essential performance
  - Determine if residual risk levels are acceptable

Cybersecurity Risk Management

- Define Safety and Essential Performance for each device
- Identify vulnerabilities that could compromise safety or essential performance
- Use threat modeling to determine exploitability and severity of patient harm if vulnerability were exploited
- Guidance suggests a matrix, tailored to each product, with combinations that consider likelihood of exploitability and severity of patient harm to determine whether risk of patient harm is controlled or uncontrolled
- Ultimate question: Is there an unacceptable residual risk of patient harm, considering risk mitigations and compensating controls?

Remediating and Reporting Cybersecurity Vulnerabilities

- Reporting *is not* generally required for vulnerabilities of controlled (acceptable) risks, which are generally remediated by routine updates or security patches and considered device enhancements
- Reporting *is* generally required for uncontrolled (unacceptable) risks to safety and essential performance, which require remediation beyond routine updates and patches
- Reporting *is always* required if the device would be likely to cause or contribute to a serious injury or death if malfunction were to occur
- Guidance document provides examples of scenarios

Good "Cyber Hygiene"

- FDA additionally stresses employing general principles of good cyber hygiene to further mitigate emerging risks and reduce impacts to patients. This includes:
  - Routine device cyber maintenance
  - Assessing postmarket information
  - Employing a risk-based approach to characterizing vulnerabilities
  - Timely implementation of necessary actions

How Is All of This Playing Out in the Real World?

- Lots of opportunity–if devices are not secure, significant vulnerabilities
- Thus far, the majority of these vulnerabilities are not being exploited–perhaps a lack of motivation to meddle with medical equipment (lack of benefit to the hacker)
- Potential Upside: Small study revealed that many medical devices targeted for cyber attacks appeared to be targeted just because their systems were open, not because hackers were looking for medical equipment, but this may be changing
- Now is an opportune time to fix the system before there are significant adverse events due to cybersecurity lapses

Summary of FDA Cybersecurity Actions

- Issued premarket and postmarket cybersecurity guidance documents
- Held public workshops to explain cybersecurity guidance documents
- Collaborated with NIST to develop cybersecurity framework for all medical devices
- Established formal partnership with the ISAO NH-ISAC and MDISS for enhanced information sharing (MOU)

Summary of FDA Cybersecurity Actions

- Established a formal partnership with the Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team
- Issued first cybersecurity alert in August 2015 in conjunction with DHS
- Interpreting current regulations (QSR) and enforcement mechanisms in the context of cybersecurity measures
- Offering enforcement discretion incentives to industry who follow guidance, including using the NIST Framework and participating in NH-ISAC

Conclusion

- FDA's cybersecurity program is still fairly new, but they are moving guidance documents quickly relative to other areas of regulation and the proactive approach appears to be a good start.
- At this time, most cyber attacks on medical devices have been benign. It remains to be seen if FDA and the industry can implement an effective program before there are attacks with serious consequences.

UNDERSTANDING THE EVOLUTION OF THREATS

YOU HAVE
BEEN HACKED

Cybercrime is Where the Money Is . . .

Then

When asked why he robbed banks, Willie Sutton supposedly answered, "I rob banks because that's where the money is."

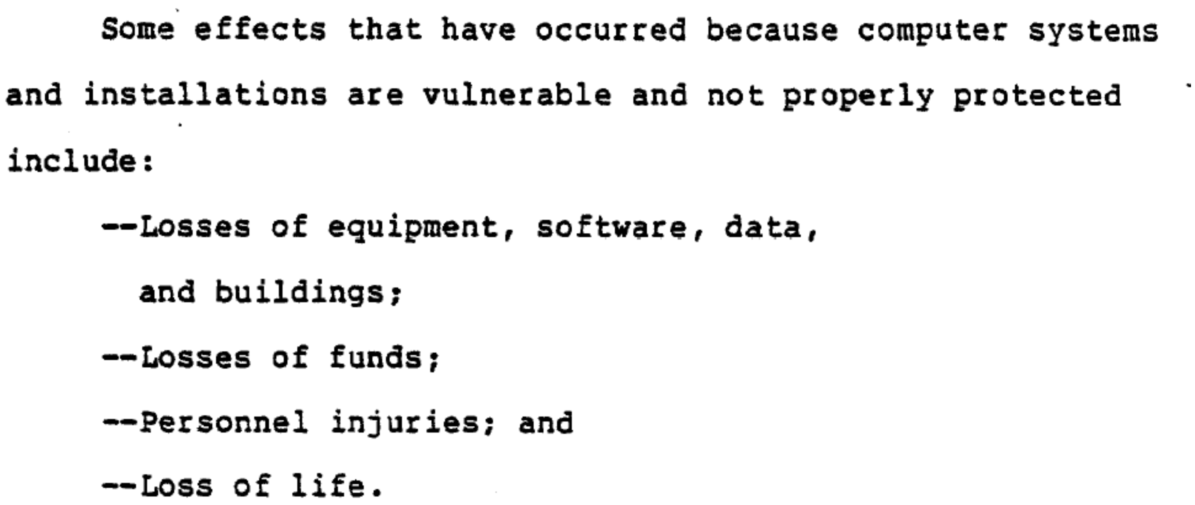
Now

Organized cybercriminals around the world monetize crimes compromising the confidentiality, integrity, or availability of information and systems.

Destructive Attacks

Inputs and Outputs

Healthcare Cybersecurity Goes Beyond Data and System Security and Integrity



Some effects that have occurred because computer systems and installations are vulnerable and not properly protected include:

--Losses of equipment, software, data, and buildings;

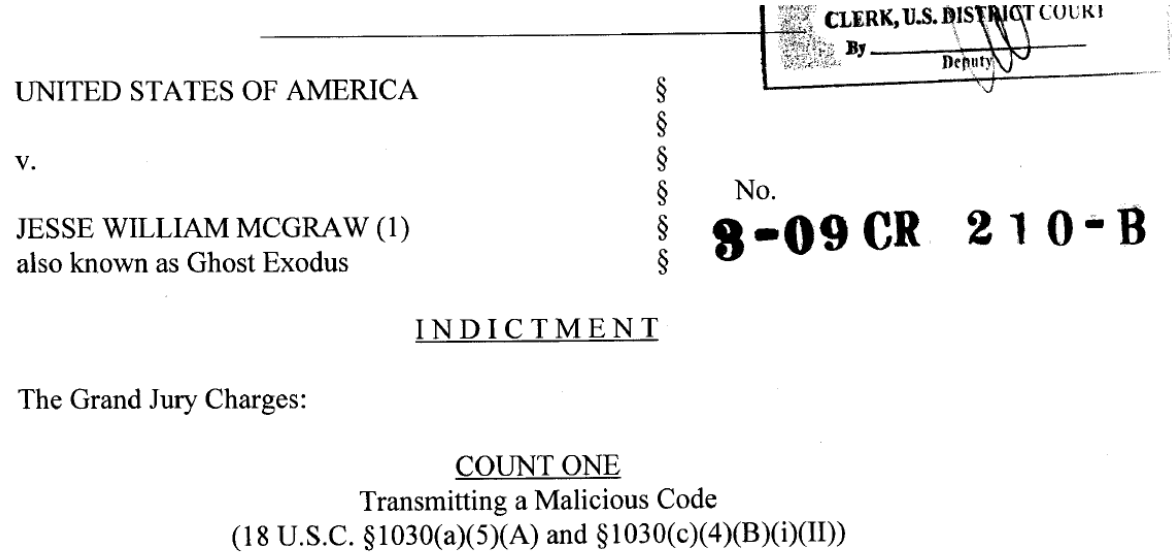
--Losses of funds;

--Personnel injuries; and

--Loss of life.

-DONALD L. SCANTLEBURY

Cyber Incidents Can Impact Patient Wellbeing



CLERK, U.S. DISTRICT COURT
By ____________ Deputy

UNITED STATES OF AMERICA §
§
v. §
§ No.
JESSE WILLIAM MCGRAW (1) § 3-09 CR 210-B
also known as Ghost Exodus §

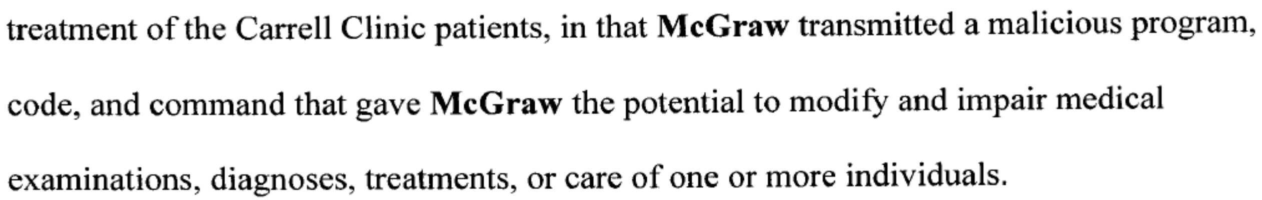
INDICTMENT

The Grand Jury Charges:

COUNT ONE
Transmitting a Malicious Code
(18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(i)(II))

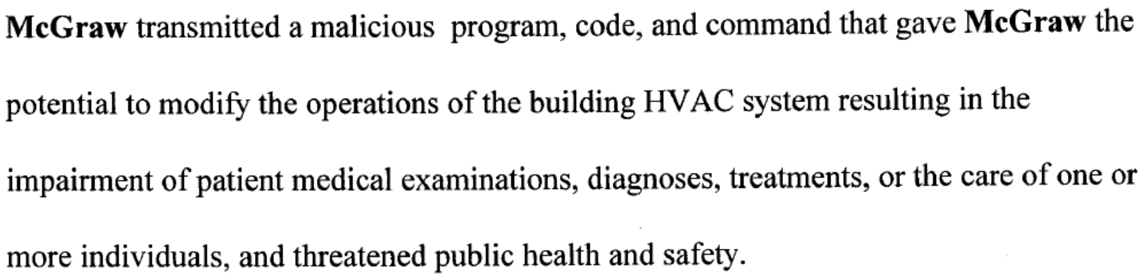
Cyber Incidents Can Impact Patient Wellbeing

COUNT ONE



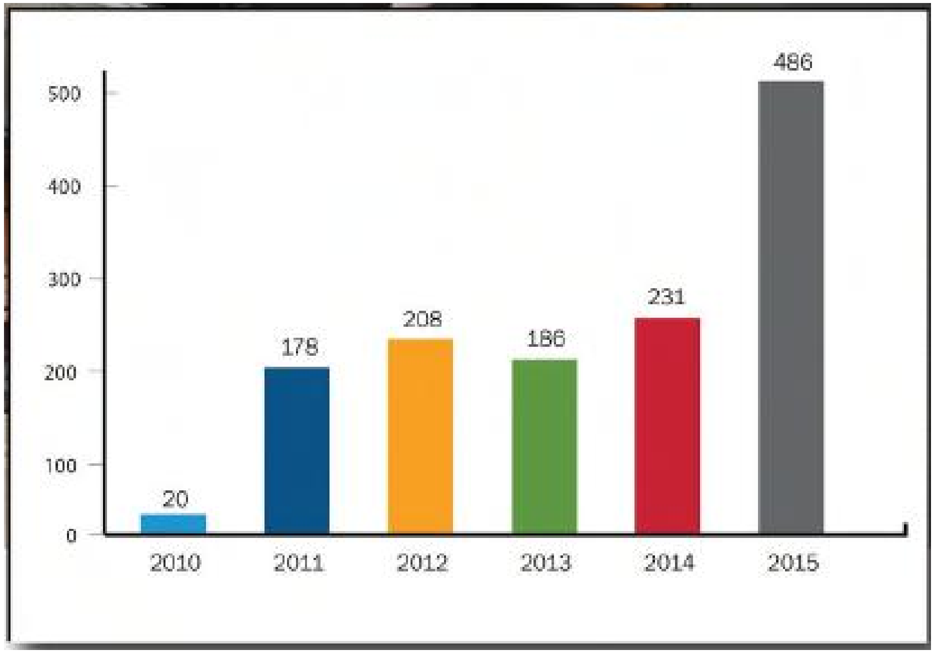
treatment of the Carrell Clinic patients, in that **McGraw** transmitted a malicious program, code, and command that gave **McGraw** the potential to modify and impair medical examinations, diagnoses, treatments, or care of one or more individuals.

COUNT TWO



McGraw transmitted a malicious program, code, and command that gave **McGraw** the potential to modify the operations of the building HVAC system resulting in the impairment of patient medical examinations, diagnoses, treatments, or the care of one or more individuals, and threatened public health and safety.

ICS-CERT Vulnerability Reporting FY 2010 to FY 2015



CRITICAL ISSUES IN THE CYBERSECURITY OF HEALTHCARE DATA

Why Digital?

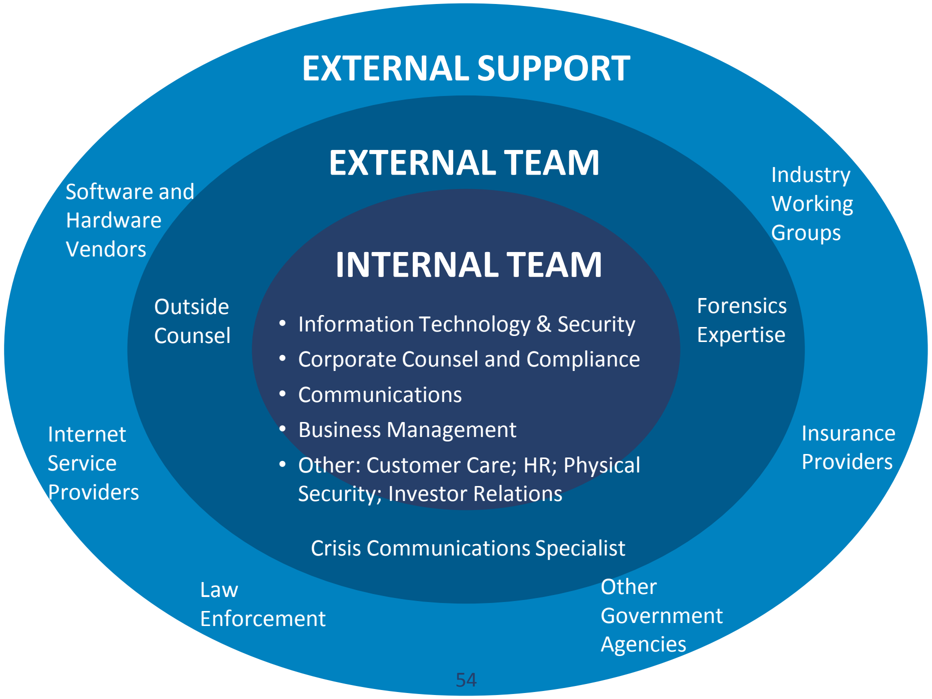
- If policy makers and businesses get it right, linking the physical and digital worlds could generate up to $11.1 trillion a year in economic value by 2025.
  - McKinsey & Company

How Much "Compliance" Is Sufficient?

- Privacy Rule
- Security Rule
  - Administrative Safeguards
  - Technical Safeguards
  - Physical Safeguards
- Breach Notification Rule

Insiders, Third Parties, and Unknowns are Critical

Incident Response Capacity: Readiness for the Inevitable



EXTERNAL SUPPORT

EXTERNAL TEAM

INTERNAL TEAM

- Information Technology & Security
- Corporate Counsel and Compliance
- Communications
- Business Management
- Other: Customer Care; HR; Physical Security; Investor Relations

Outside Counsel

Forensics Expertise

Crisis Communications Specialist

Software and Hardware Vendors

Industry Working Groups

Internet Service Providers

Insurance Providers

Law Enforcement

Other Government Agencies

Liability and Costs Come from Countless Sources

Reputational Harm

HHS OCR Enforcement Actions

Shareholder Actions

Spiking Operational Expenses

FTC Enforcement Actions

Class Actions

Contractual Damages

State AG Investigations and Enforcement Actions

TRENDS LEARNED FROM 2016 HIPAA ENFORCEMENT

Trends Learned from 2016 HIPAA Enforcement

- Settlements in 2016 totaled more than any other year prior: over $20 million
  - *Healthcare Network (Illinois)*: $5.5 million
  - *Research Institute (New York)*: $3.9 million
  - *Insurance Company (Puerto Rico)*: $3.5 million
  - *Primary Care (Minnesota)*: $1.5 million
  - *Orthopedic Clinic (North Carolina)*: $750,000

Trends Learned from 2016 HIPAA Enforcement

- Non-monetary penalties:
  - Prison Sentences
  - Revoked Medical Licenses
  - Fines levied by states
- Also demonstrated that would take cases to litigation
  - *Director of Office for Civil Rights v. Lincare Inc.* (No. CR 4505, Jan. 13, 2016)

Trends Learned from 2016 HIPAA Enforcement

Key Issues

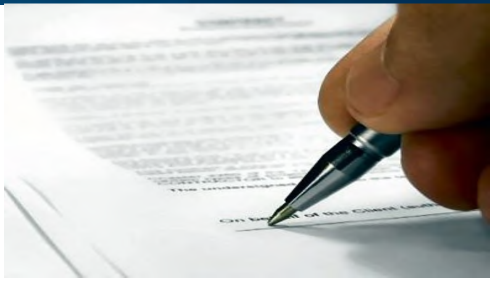
- Failed to implement policies and procedures

Trends Learned from 2016 HIPAA Enforcement

Key Issues

- Failed to implement policies and procedures
- Policies and procedures not followed

Trends Learned from 2016 HIPAA Enforcement



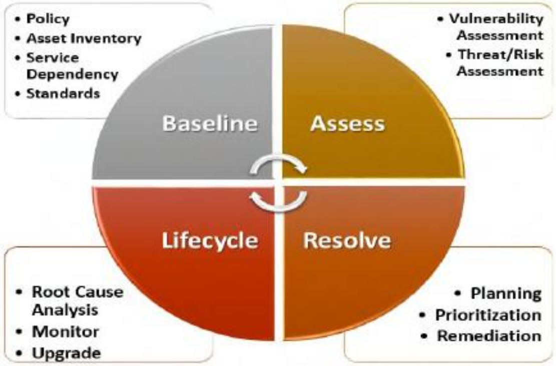
Key Issues

- Policies and procedures not followed
- Failed to implement policies and procedures
- Failure to obtain a business associate agreement or go through proper protocols in executing that agreement

Trends Learned from 2016 HIPAA Enforcement

Key Issues

- Policies and procedures not followed
- Failed to implement policies and procedures
- Failure to obtain a business associate agreement or go through proper protocols in executing that agreement
- Failed to conduct risk analyses



Baseline
- Policy
- Asset Inventory
- Service Dependency
- Standards

Assess
- Vulnerability Assessment
- Threat/Risk Assessment

Resolve
- Planning
- Prioritization
- Remediation

Lifecycle
- Root Cause Analysis
- Monitor
- Upgrade

Trends Learned from 2016 HIPAA Enforcement

Key Issues

- Policies and procedures not followed
- Failed to implement policies and procedures
- Failure to obtain a business associate agreement or go through proper protocols in executing that agreement
- Failed to conduct risk analyses
- Conducted risk analyses but failed to address vulnerabilities

HIPAA Enforcement under the New Administration

- Impact on agencies
  - Office for Civil Rights
    - New director: Roger Severino
  - Office of the National Coordinator for Health IT
  - Federal Trade Commission
- Scaled-back examination of mergers may increase transmittal of data with less focus on security
- Potential for increased risk related to IoT
- Overall: Privacy and security are popular issues and enforcement brings money into the government

Individual Lawsuits for HIPAA Violations

- No private right of action under HIPAA
- Small emergence of a trend of individuals finding other ways to file claims based on HIPAA violations:
  - Negligence for violating HIPAA
  - Negligence for inappropriate disclosure that led to harm (loss of custody, privacy concern, severe embarrassment or distress)
  - Breach of fiduciary duty

Best Practices for Companies Under Investigation

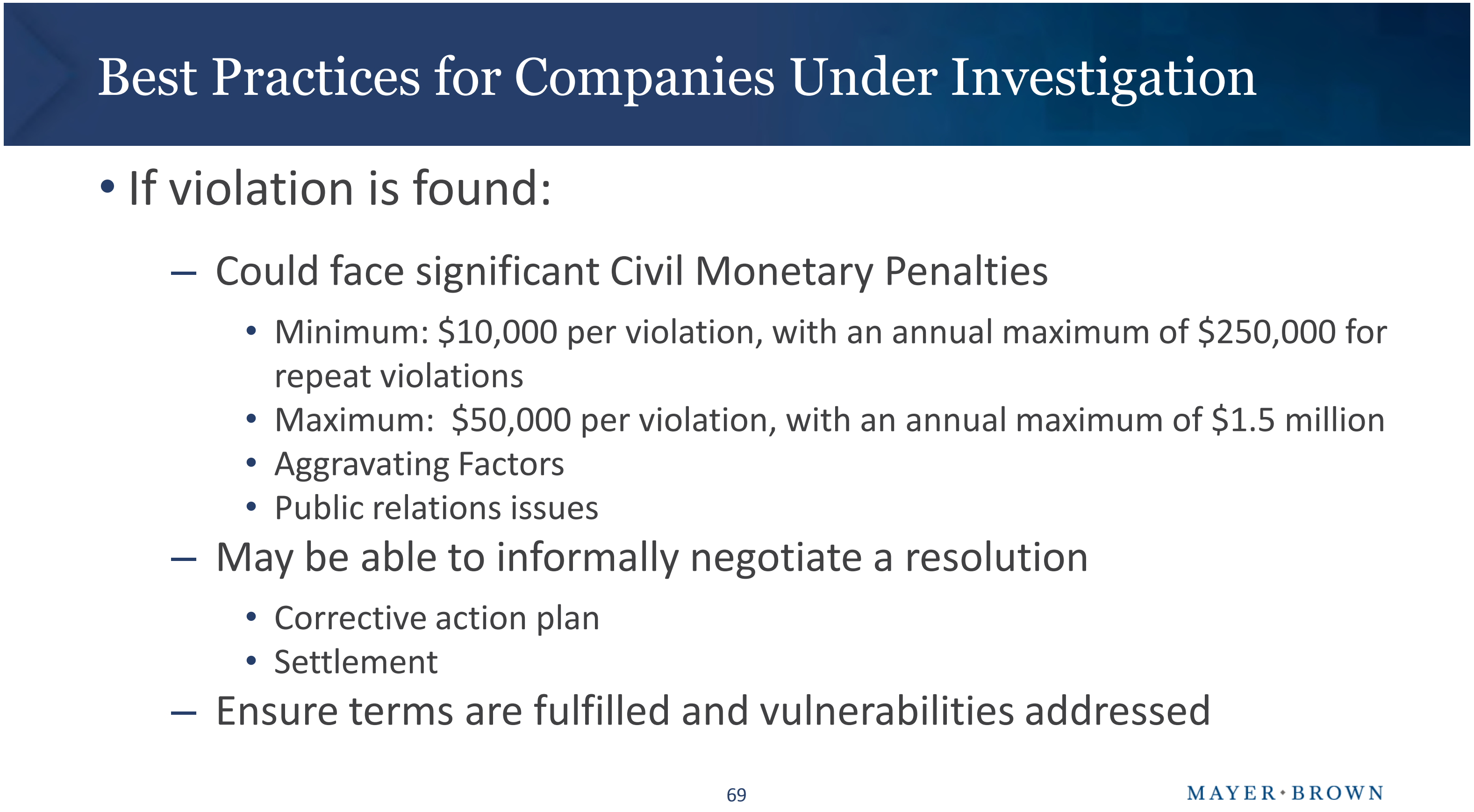
- Pre-enforcement Best Practices
  - Indemnity clauses in business associate agreements
  - Cyber insurance protection
  - Reasonable steps to protect information (encryption)
  - Create policies and monitor their enforcement
  - Set rules about any information that can leave the premises
  - Conduct risk assessments
  - Employee training and sanction policy
  - Have a protocol set for handling complaints or government enforcement actions

Best Practices for Companies Under Investigation

- Protocol when complaints or enforcement actions arise
  - Determine investigation players (company employees and in-house counsel, outside counsel, outside consultants and experts) and scope of investigation and work product
  - If a third-party complaint:
    - Establish response team and begin an investigation
    - Assure complainant the issue is being investigated, explain process and timing
    - Carry out investigation with sufficient documentation
    - If violation, implement corrective action plan
    - Determine if notification to customers or any regulators is necessary
    - Notify complainant about outcome of investigation

Best Practices for Companies Under Investigation

- Protocol when complaints or enforcement actions arise
  - If government enforcement action:
    - Establish appropriate response team (privacy officer, in-house counsel, outside counsel)
    - Ascertain nature of the investigation and the alleged violations
    - Update organization to the extent necessary and any necessary outside parties
    - In response to government requests, begin balancing act of complete cooperation yet limiting disclosure to what is requested
    - Provide employees and documents as necessary
    - Conduct parallel internal investigation
    - Seek opportunity to sit down with regulators about potential violations and Company's findings



Best Practices for Companies Under Investigation

- If violation is found:
  - Could face significant Civil Monetary Penalties
    - Minimum: $10,000 per violation, with an annual maximum of $250,000 for repeat violations
    - Maximum: $50,000 per violation, with an annual maximum of $1.5 million
    - Aggravating Factors
    - Public relations issues
  - May be able to informally negotiate a resolution
    - Corrective action plan
    - Settlement
  - Ensure terms are fulfilled and vulnerabilities addressed

MAYER ◆ BROWN

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.