



Clean the house: Cyber-hygiene to safeguard patient information and ensure patient safety

October 31, 2017



Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
CEO



Sheetal Sood, CHC, CIPP, CISA, CRISC, CISSP, GIAC, GSEC
Senior Executive Corporate Compliance Officer

© Clearwater Compliance | All Rights Reserved

Discussion Flow

1. Connecting the Dots
2. Beyond Traditional IT Assets
3. Bona Fide Risk Analysis and Risk Management



2

© Clearwater Compliance | All Rights Reserved

First Healthcare Risk Manager

"First, Do No Harm."

- Hippocrates, 4th Century, B.C.E.
- OR

- Auguste François Chomel (1788–1858) Parisian
pathologist and clinician
- OR

- ???



**Digitization in Healthcare is Great AND We Can
Now Create Harm from New Threat Sources**



3

© Clearwater Compliance | All Rights Reserved

Very Real Need - Increasingly More Significant Business Risk

Damage to Brand Compliance Financial Competition

Talent Acquisition **Cyber** Patient Safety *Cyber and Compliance Risk Management is Not "an IT Problem"*

Business Interruption Third Party Liability Property Damage

© Clearwater Compliance - All Rights Reserved

CLEARWATER COMPLIANCE

4

Cyber criminals' next deadly target: Grandpa's pacemaker

Tim Johnson, McClintock Washington Bureau on Aug 7, 2017
Published in Health & Fitness

SUBSCRIBE Email Address

An MRI machine at a hospital in Germany displays its work at the University Medical Systems MRI Research Center in Bonn, Calif. (AP Photo/Chris Wedel)

"We're going to have our digital D-Day, our cyber D-Day, if you will, in medical, and there's going to be patients that die. It's going to be a big deal," said Dr. Christian Dameff, an emergency room physician and expert on cyber vulnerabilities.

WASHINGTON -- Cyberattacks are accelerating worldwide and the U.S. health care system is dangerously unprepared to defend itself, or its patients.

In the past two months, thousands of computers of the nation's No. 3 pharmaceutical company, Merck, seized up amid a global cyberattack, cutting into production of

<https://www.arcamax.com/healthandspirit/health/healthhttps-198547176>

© Clearwater Compliance - All Rights Reserved

CLEARWATER COMPLIANCE

5

Fears of hackers targeting hospitals, medical devices
| ABC News | June 29, 2017

0:00 / 1:07

https://www.youtube.com/watch?v=pU3NQ3GKC_0

© Clearwater Compliance - All Rights Reserved

CLEARWATER COMPLIANCE

6

The Risk Problem We're All Trying to Solve

What if my Sensitive Information is shared?

What if my Sensitive Information, Systems, or Devices are not complete, up-to-date and accurate?

What if my Sensitive Information, Systems, or Devices are not there when it is needed?

Don't Compromise CIA!

Don't Forget: PII, PCI Data, MNPI, Trade Secrets, Business Plans, Software Code, Etc.

© Clearwater Compliance. All Rights Reserved.

CLEARWATER COMPLIANCE

7

Discussion Flow

1. Connecting the Dots
2. Beyond Traditional IT Assets
3. Bona Fide Risk Analysis and Risk Management

© Clearwater Compliance. All Rights Reserved.

CLEARWATER COMPLIANCE

8

Must Include Every Information Asset in Every Location/LOB

 Clinics	 Hospitals	 LTC Facility	 ASC	 CHC
 Hospice	 Insurance	 Home Health	 EMS	 Rehab Clinic
 Imaging Center	 Rural Clinic	 Dialysis Clinic	 Behavioral Health	 Research

© Clearwater Compliance. All Rights Reserved.

CLEARWATER COMPLIANCE

9

Traditional Assets – IT Systems and Applications



- Electronic Health Record Applications
- Clinical Information Applications
- Lab And / Or Medical Specialty Applications
- Medical Billing/Claims Processing Applications
- Email Applications
- Company Intranet Websites
- HR Management Applications
- Network File Sharing Applications
- EDI Applications
- Fax Applications
- Payment Processing Applications
- Financial Management/Reporting Applications
- Any Other Software Used To Manage Sensitive Electronic Information



10

Biomedical Assets – Pumps, PACS, etc.



- Patient monitoring devices, monitors and smart rooms
 - Smart medical devices, infusion pumps, ventilators, incubators, telemetry, smart stethoscopes and medical imaging
- Electrocardiogram (ECG), heart rate, pulse oximetry, ventilators, capnography monitors, depth of consciousness monitors, regional oximetry, biopatch technology and respiratory rate
- Smart beds, hand hygiene and fall detection
- Remote ICU telemetry, Tele-ology (any medical science done remotely — for example, tele-neurology or tele-dermatology)
- Remote wellness and chronic disease management
 - Pacemakers, defibrillators and neuro-stimulators
 - Wearable wristbands, bio-patches, smartwatches and ear buds
 - Remote clinical monitor spirometer, pulse oximeter, ECG, glucometer and fall detection



11

IoT Assets – Facilities, Infrastructure, etc.



- Facilities Security, Building Management
 - Video surveillance, door locks and entry systems, and fire alarms
- Power monitoring, power distribution, energy consumption and management, and elevators
- HVAC, lighting, room control, water quality, humidity monitoring, and tissue and blood refrigerators
- Real-time location services (RTLS) for Assets, Employees, Patients and Visitors
 - Wheelchairs, infusion pumps, smart cabinets, medication carts, par-level management and rental management
 - Physicians, nursing staff and ancillary staff
 - Infant abduction and wandering systems
 - Wayfinding and digital signage
- Networking Hardware, Software, Security, Services
 - Routers, Switches, LAN cards, Wireless routers
 - Operating systems, Network Security and Services




12

[illegible][illegible]

Discussion Flow

1. Connecting the Dots
2. Beyond Traditional IT Assets
3. Bona Fide Risk Analysis and Risk Management



© Clearwater Compliance. All Rights Reserved.

CLEARWATER COMPLIANCE

16

NIST Risk Management Process¹

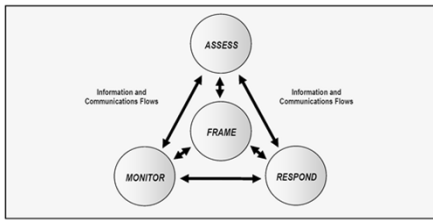


FIGURE 1: RISK MANAGEMENT PROCESS

¹<http://clearwatercompliance.com/wp-content/uploads/SP800-39-final.pdf>



© Clearwater Compliance. All Rights Reserved.

CLEARWATER COMPLIANCE

17

NIST Risk Assessment Process

- 01 Finalize Information Asset Inventory
- 02 Identify Threats & Vulnerabilities
- 03 Determine Likelihood & Impact
- 04 Determine Risk Level

What Are All the Possible Ways in Which We May Compromise Sensitive Information?

© Clearwater Compliance. All Rights Reserved.

CLEARWATER COMPLIANCE

18

Risk Assessment Example

Asset	Threat Source / Action	Vulnerability	Likelihood	Impact	Risk Level
Server	Hacker exfiltrates data	No DB encryption	Med (3)	High (5)	15
Server	Hacker exfiltrates data	Weak passwords	High (5)	High (5)	25
Server	Malware encrypts data	Unpatched OpSys	Med (3)	Med (3)	9
Server	Careless IT changes data	Integrity checks	Low (1)	Medium (3)	3
Server	Hardware head crash	No data backup	Med (3)	High (5)	15
Server	Hacker DDOS	Insufficient capacity	Low (1)	High (5)	5
etc					

© Clearwater Compliance. All Rights Reserved.



19

Risk Assessment Fundamentals

- Must be possible to have loss or harm
- Must have asset-threat-vulnerability to have risk
- Risk is a likelihood issue
- Risk is an impact issue
- Risk is a derived value (*like speed is a derived value = distance / time*)
- Fundamental nature of Risk is universal
- Risk assessment informs all other steps
- Not "once and done"
- Critical Output: *Risk Register*

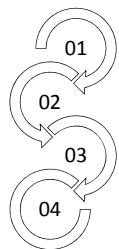


© Clearwater Compliance. All Rights Reserved.



20

NIST Risk Response Process



Identify Risk Responses

Evaluate Alternatives

Make Risk Response Decision

Implement Risk Response



What decisions do we need we need to make to treat or manage risks?

© Clearwater Compliance. All Rights Reserved.



21

Decide on Response or Treatment

© Clearwater Compliance | All Rights Reserved

CLEARWATER COMPLIANCE 22

Thinking Like a Risk Manager

Risks of all types & sizes exist

Risk Response

Risk Response is making informed decisions on how to treat risks.

© Clearwater Compliance | All Rights Reserved

CLEARWATER COMPLIANCE 23

Risk Response Fundamentals

- *Real* Risk Response Requires *Real* Risk Analysis
- All Risks Need a Response
- Not All Risks Must Be Mitigated
- Risk Response Requires Setting Your Risk Appetite
- Risk Response Requires Real Risk Framing
- Risk Management is Informed Decision Making – What's New?
- Risk Response Informs All Other Steps
- Critical Output: *Risk Management Plan*

© Clearwater Compliance | All Rights Reserved

CLEARWATER COMPLIANCE 24

Key Elements of Risk Action Plan

- Control Gap
- Recommendation
- What is Affected? (assets, ePHI, etc.)
- Responsibility for Implementation
- Priority
- Due Date
- Actual Completion Date
- Current Status
- Documentation



Risk Assessment In Practice: Bio-medical equipment

- Scenario: A mid-size hospital system with one ambulatory care unit and a small long-term care unit wants to start an audit of their bio-medical devices. Such an audit has never been performed before.

Challenge: Where to begin? How do I assess risk?

Risk Assessment In Practice: Bio-medical equipment

Issues

Resultant Risks

- | | | |
|-----------------------------------|---|--|
| 1. Inaccurate Inventory | → | 1. Scope and Universe of assets not known, No baseline information, no view of what assets need protection |
| 2. Improper Data Management | → | 2. Unauthorized access, use or disclosure |
| 3. Inadequate Security controls | → | 3. Unauthorized access, use or disclosure |
| 4. Insufficient Physical controls | → | 4. Unauthorized access, use or disclosure |
| 5. Lack of System Hardening | → | 5. Unauthorized access, use or disclosure |
| 6. Insecure transmission | → | 6. Unauthorized access, use or disclosure |

Risk Assessment In Practice: Bio-medical equipment

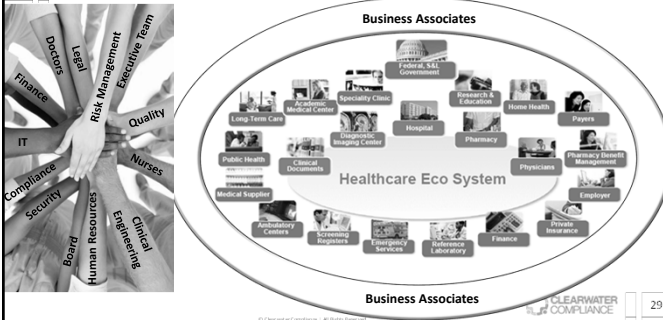
Audit methodology

- **Inventory:** Accurate, Current, Prioritized assets list
- **Data:** Nature, Quantity, Storage State
- **Security Capabilities of Device:** Access control, Logs, role-based access
- **Physical controls:** Locks, Secure spaces
- **System Controls:** Patches, updates, system hardening
- **Insecure Transmission:** Removable drive or solid-state drive, peripheral, printing, network connection

Final Outcome:

- * Risk Chart with Assets Prioritized by Risk
- * Short-term and Long-term Mitigation Plans

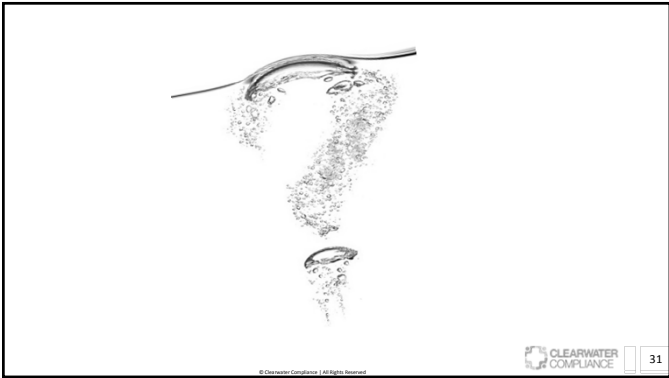
Information Risk Management Must Become a Team Sport

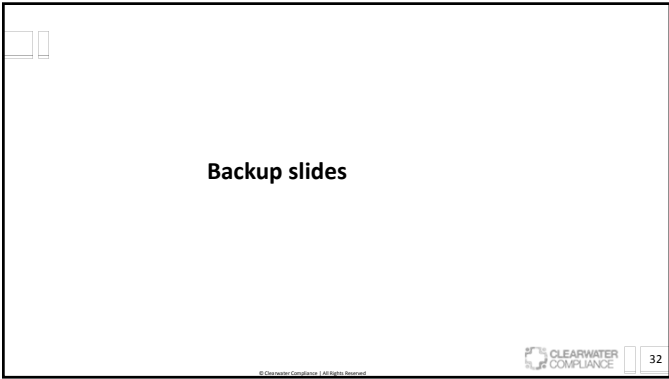


Four Critical Points

1. eHealth brings opportunities *and new risks*
2. It's about safeguarding ePHI AND assuring Patient Safety
3. *Information Risk Management* Language is Business Risk Management Language
4. *Information Risk Management* Must Become a Team Sport








Compromise of Confidentiality on Patient Satisfaction	
How Does It Happen?	Ramifications
Careless User <ul style="list-style-type: none">• Discussing treatment in an open environment• Calling the wrong family about a patient's status• Emailing or faxing patient information to an unauthorized person• Improperly disposing of paper records	<ul style="list-style-type: none">• Identity Theft• Reputational Damage• Relationship Damage• Employment Damage• Financial Damage• Anxiety• Depression
Snooping <ul style="list-style-type: none">• Accessing records of a friend on behalf of a colleague• Accessing records of an ex-spouse new partner• Accessing records of a neighbor out of curiosity• Accessing records of famous people	
Malicious <ul style="list-style-type: none">• Selling medical records of famous people for personal gain• Using medical information for medical fraud• Posting medical information on social media as revenge• Using medical records to provide insurance to friends or family	


Compromise of Integrity on Patient Safety & Quality of Care	
How Does It Happen?	Ramifications
Errors or Omissions <ul style="list-style-type: none">• Patient identification errors• Use of temporary names• Input errors• Inadequate reporting of test results	<ul style="list-style-type: none">• Incorrect Diagnosis• Incorrect Treatment• Incorrect Prescriptions• Incorrect Billing Charges• Contaminated Clinical Trial• Identity Theft• Reputational Damage• Death
Inadequate Information "Hand Off" <ul style="list-style-type: none">• Poor coordination of care between primary and specialist care• Poor care coordination with next level of care if not automated	
Inadequate Administrative Controls <ul style="list-style-type: none">• Inadequate role-based security on EMR system• Unsecured maintenance networks linked to the infrastructure network	
Inadequate Technology Controls <ul style="list-style-type: none">• Vulnerable networked medical devices• Use of robotics supporting telemedicine/telehealth	

 34

© Clearwater Compliance | All Rights Reserved

Compromise of Availability on Patient Safety & Quality of Care

How Does It Happen?	Ramifications
Incomplete or untested remediation plans <ul style="list-style-type: none"> Disaster Recovery Plans Business Interruption Plans Business Continuity Plans 	<ul style="list-style-type: none"> Delayed Admittance Delayed Diagnosis Delayed Surgery Delayed Prescriptions Delayed Discharge Diagnosis Errors Treatment Errors Death
Inadequate Processes <ul style="list-style-type: none"> Untimely or incomplete back-up procedures Disconnected Systems Unpatched applications 	
Inadequate Security Controls <ul style="list-style-type: none"> Back-up connected to infrastructure network Untrained workforce members on social engineering tactics 	



35

© Clearwater Compliance, L.L.C. All Rights Reserved
