Achieving Trustworthy Cyber Systems: Challenges & Strategies

Healthcare Systems

M. Jamal Deen FRSC FIEEE . . .

IEEE - ISPA / IUCC / SpaCCS – 2017; Thursday 14 Dec 2017

Guangzhou, China

Electrical and Computer Engineering Department

McMaster University Hamilton, ON L8S 4K1

(E-mail: jamal@mcmaster.ca)

Cybersecurity – Recent China News

CHINADAILY.COM.CN 中国日报网

By Cao Yin (China Daily)
Updated: 2017-12-06 08:27

Projection of cyber code on hooded man

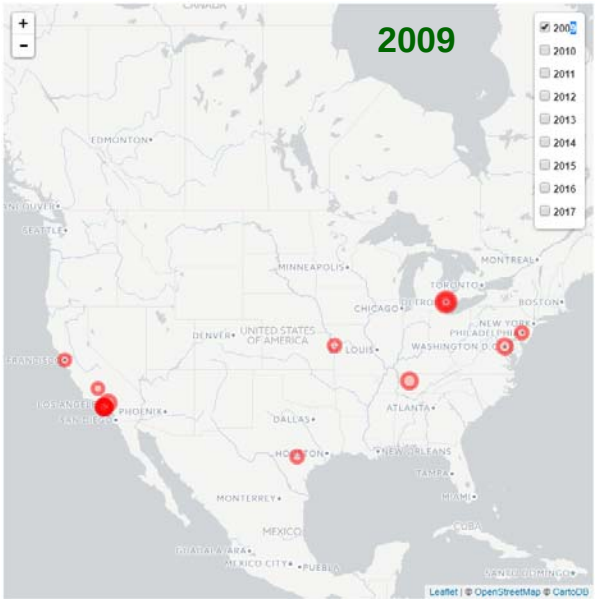
Cybersecurity threat could cause damage "beyond imagination"

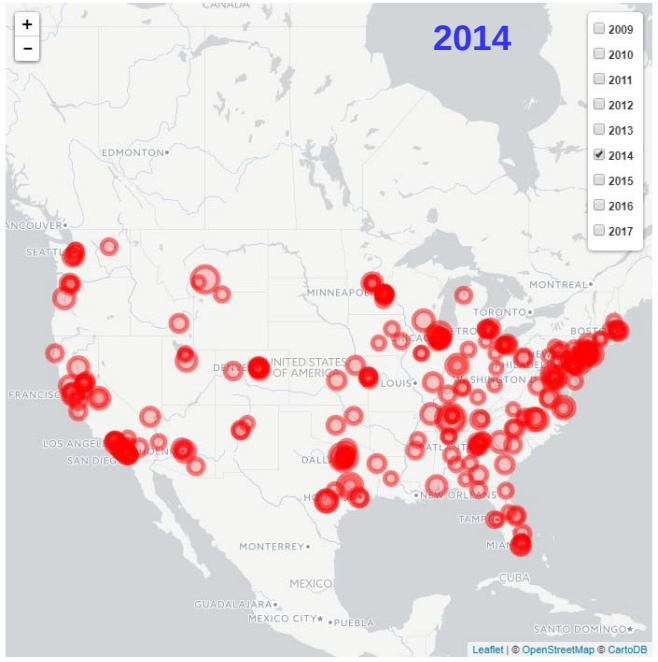
- **Cybersecurity - major problem for China**
  - Electronic attacks - frequent worldwide, no end in sight - Leading specialist on internet security

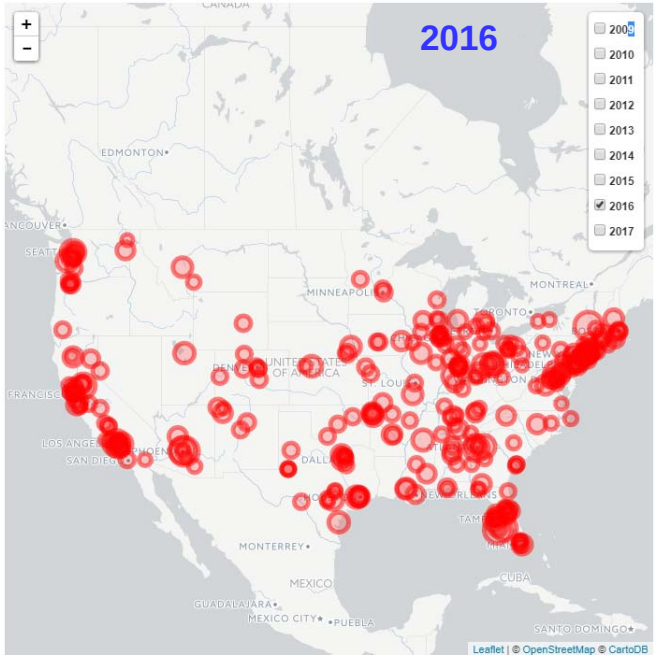
- **Jan - Oct, China hit by ~17.5M cyberattacks – Most from overseas - National Computer Network Emergency Response Technical Team and Coordination Center, China's top security risk-monitoring authority**
  - Most online attacks - Trojan viruses and bots, >17.23M attacks
  - Most from United States (Authority stated)
  - Targets include intelligent devices in peoples' homes, including internet routers and smart televisions

http://iosnews.chinadaily.com.cn/newsdata/news/201712/06/481505/article.html?from=singlemessage

Healthcare Breaches - USA







https://choisung.shinyapps.io/healthdatabreach/

Created by Sung Choi

Data source: U.S. Department of Health and Human Services Office for Civil Rights Breach Portal

Updated: Mar 1, 2017

The interactive map shows the reported health data breaches from 2009 to 2017. Each circle represents a breach. Click the circle to see more details. The radius of the circle represents the log of individuals records breached, hence a larger circle indicates a more severe breach.

Healthcare Cybersecurity Concerns

DATA PROTECTION

- Data protection compliance assessments (preparing for the EU General Data Protection Regulation)
- Privacy governance
- Privacy impact assessments
- Notifications (registrations) to the Data Protection Authorities
- Data Loss Prevention

CYBERSECURITY

- Cyber Strategy and Governance
- Infrastructure and software security
- Identity and access management
- Cyber threat and vulnerability management,
- Cyber incident detection and threat intelligence
- Cyber Incident Response & Business Continuity

Cybersecurity concerns come to medical technology

Medical devices are increasingly connected to the Internet. But connectivity comes with some constraints that underpins our organization. Vulnerability to hackers and criminals. As security breaches become more common and costly, medical device cybersecurity will emerge as a major issue in the coming years, requiring device companies and healthcare providers to take preemptive action to maintain trust in medical equipment and to prevent breaches that could cripple the industry.

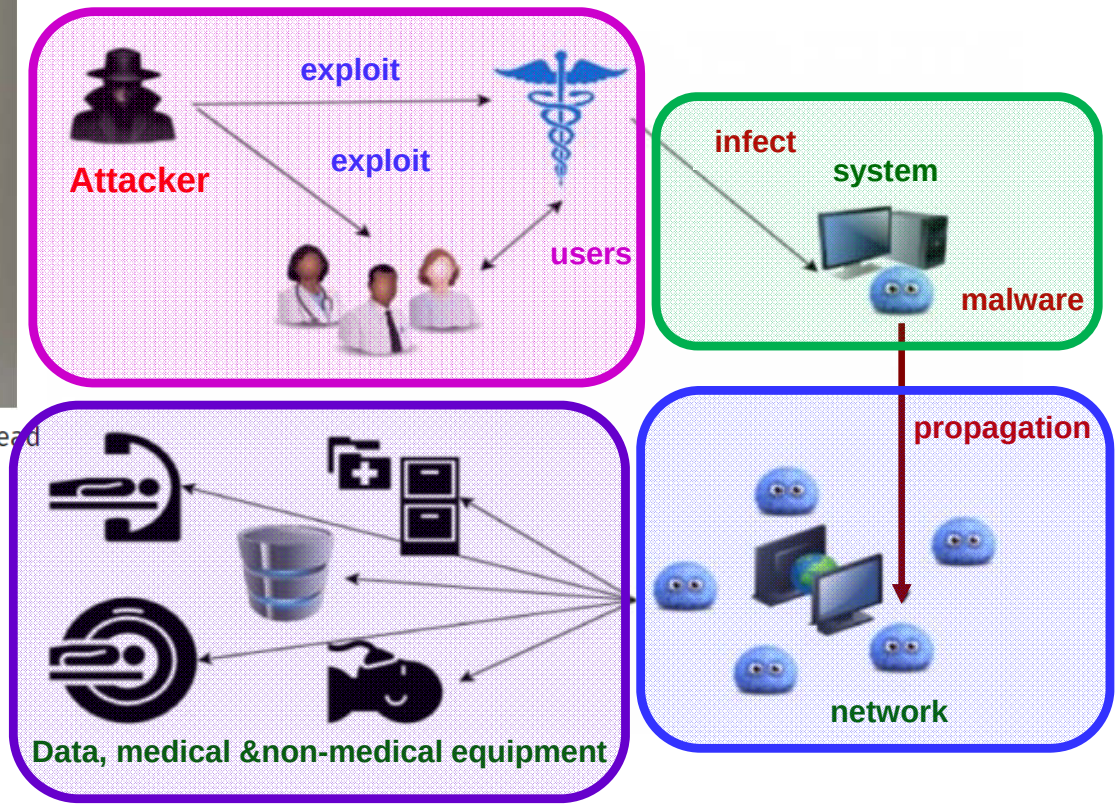
Privacy and security of personal data. Devices could allow improper access to networks of hospitals and other healthcare providers. Commercially valuable research data could be stolen from devices.

Deloitte's "The New Healthcare Economy is rising up", February 2017.

Healthcare Cyber-attacks

Confidential data and even human lives are at risk thanks to the huge spread connected technology in healthcare

MYRSINI ATHINAIOU
Monday 24 July 2017 23:00 BST



- More than 16M patient records were stolen from healthcare organizations in the US and related parties in 2016
- Healthcare was 5th most targeted industry to cyber attacks

http://www.independent.co.uk/life-style/health-and-families/why-has-healthcare-become-such-a-target-for-cyber-attackers-a7846311.html

Healthcare Cyber-security & CPS

McMaster University

Cyber security in the NHS...time to pull the plug on obsolete operating systems and legacy applications

Feature 1 MARCH 2017

Healthcare is facing the most cyber attacks since records began, with the sector accounting for the largest number of data security incidents, according to recent ICO figures

- **CPS - many medical healthcare apps.**
  - More powerful communication, computation and security capabilities
  - Various sensors collect information from patients at home - communicate with 3rd party
  - Cloud server - powerful computation capability
  - Doctors remotely monitor patient's physical condition – provide suggestions/ prescriptions

LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

THIERRY DOSOGNE/GETTY IMAGES

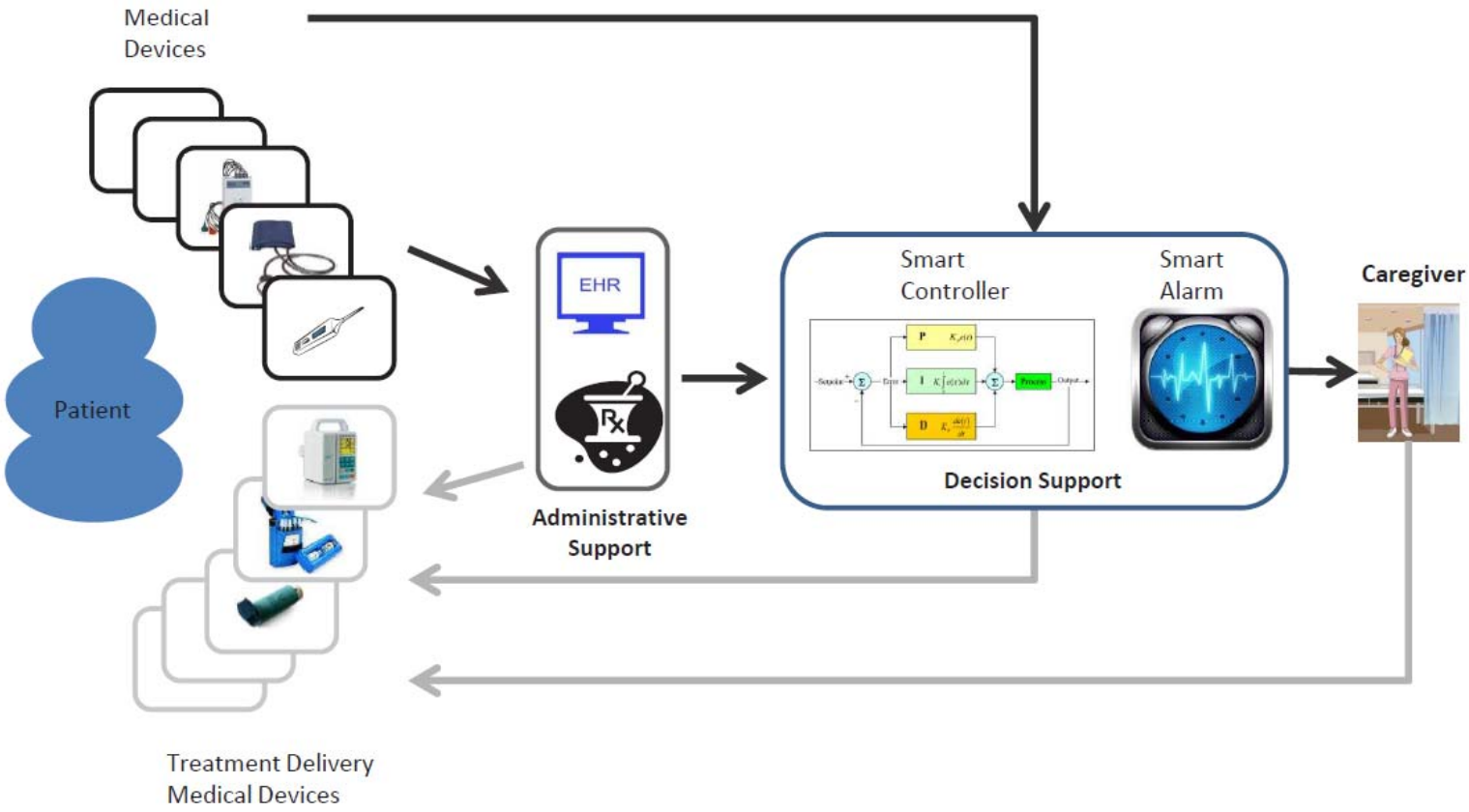
HACKED MEDICAL DEVICES make for scary headlines.

http://www.information-age.com/cyber-security-nhs-123464777/
https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

Medical Cyber-Physical Systems

- **Medical cyber-physical systems (MCPS) are life-critical context-aware, networked systems of medical devices**

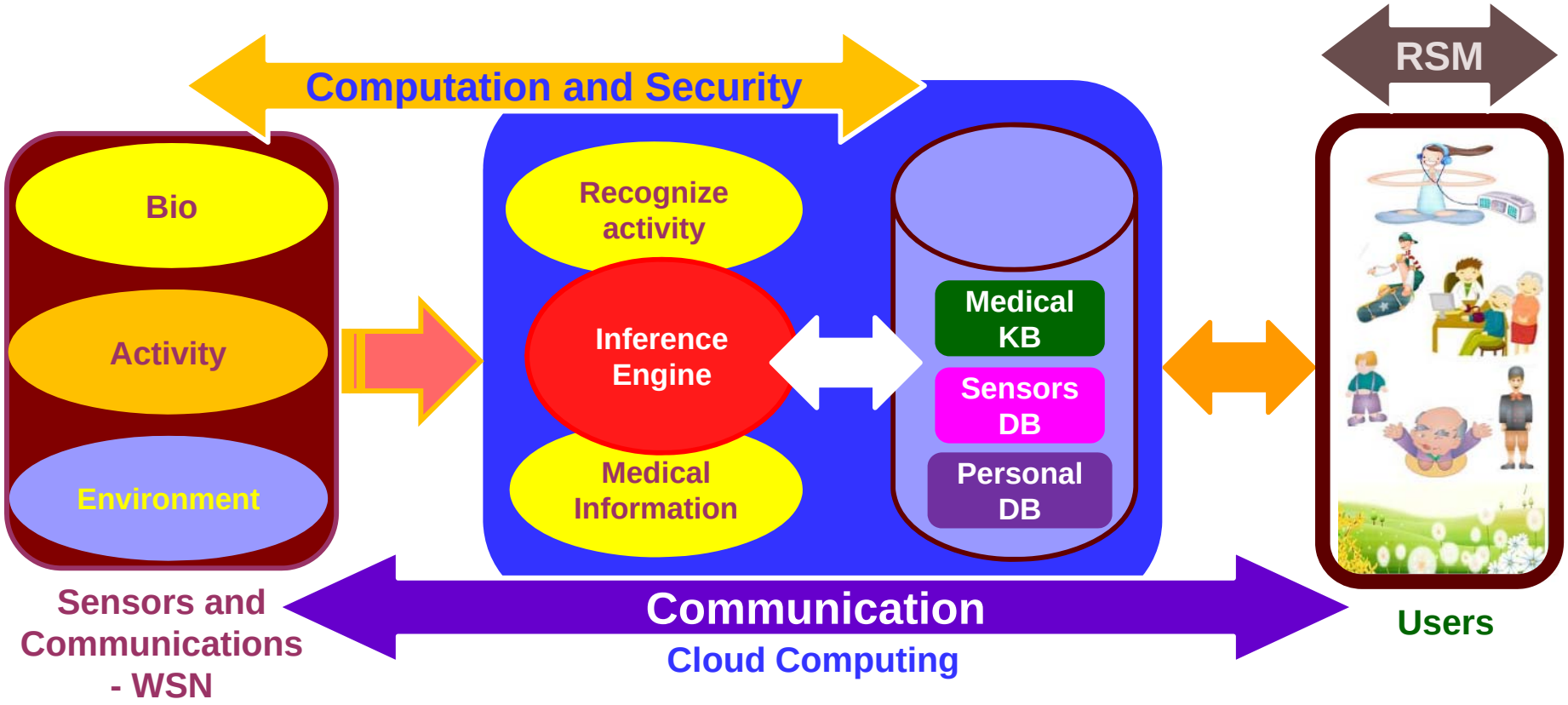
Proc IEEE, vol. 100(1), pp. 75-90, 2012



- **Security & Privacy - MCPS open door to host of security & privacy concerns**
  - Attacker penetrating MCPS network can harm/kill patients by reprogramming devices
  - Patient's health (infusion pump); Data (discrimination & abuse)
  - Device (denial-of-service, loss in privacy); Institution (access data, operational information)

CPS – Healthcare and Security

- Communication and sensing
- Computation and security
- Real-time resource scheduling & management (RSM)



Wearables - Security

- Wearables - Rapidly gaining popularity with smartwatches: Apple Watch and Samsung Gear; Exercise wearables from FitBit, Jawbone ….
- According to ABI Research, ~780M wearable devices in circulation, 2019
- Power, privacy & security concerns, technical difficulties – Some major hindrance in wearable sensors market

- Wearables - Tracking many personal information
  - GPS location, blood pressure, heart rate, and anything else - weight or diet; Personally identifiable information - target you for spear-phishing, identity theft
- Real opportunity - devices linked to smartphone
  - Phone numbers, personally identifiable information, emails, web logins … could be compromised

Cyber-Privacy/Security - Health Data

McMaster University

Key Framework Elements

Cyberprivacy	Cybersecurity
Minimize Data: Only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).	**Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Limit Use: Use PII solely for the purpose(s) specified in the notice to the identified person by the collecting organization. Sharing PII with an outside organization should be for a purpose compatible with the purpose for which the PII was collected.	**Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Data Quality and Integrity: Ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.	**Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

CGI

Experience the commitment®

Cyberprivacy and Cybersecurity for Health Data

Building confidence in health systems

PII - Personally Identifiable Information
PHI - Patient Health Information

Cyber-Privacy/Security - Health Data

McMaster University

Key Framework Elements

Cyberprivacy	Cybersecurity
Secure: Protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure	**Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Audit and Accountability: Audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.	**Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

CGI

Experience the commitment®

Cyberprivacy and Cybersecurity for Health Data

Building confidence in health systems

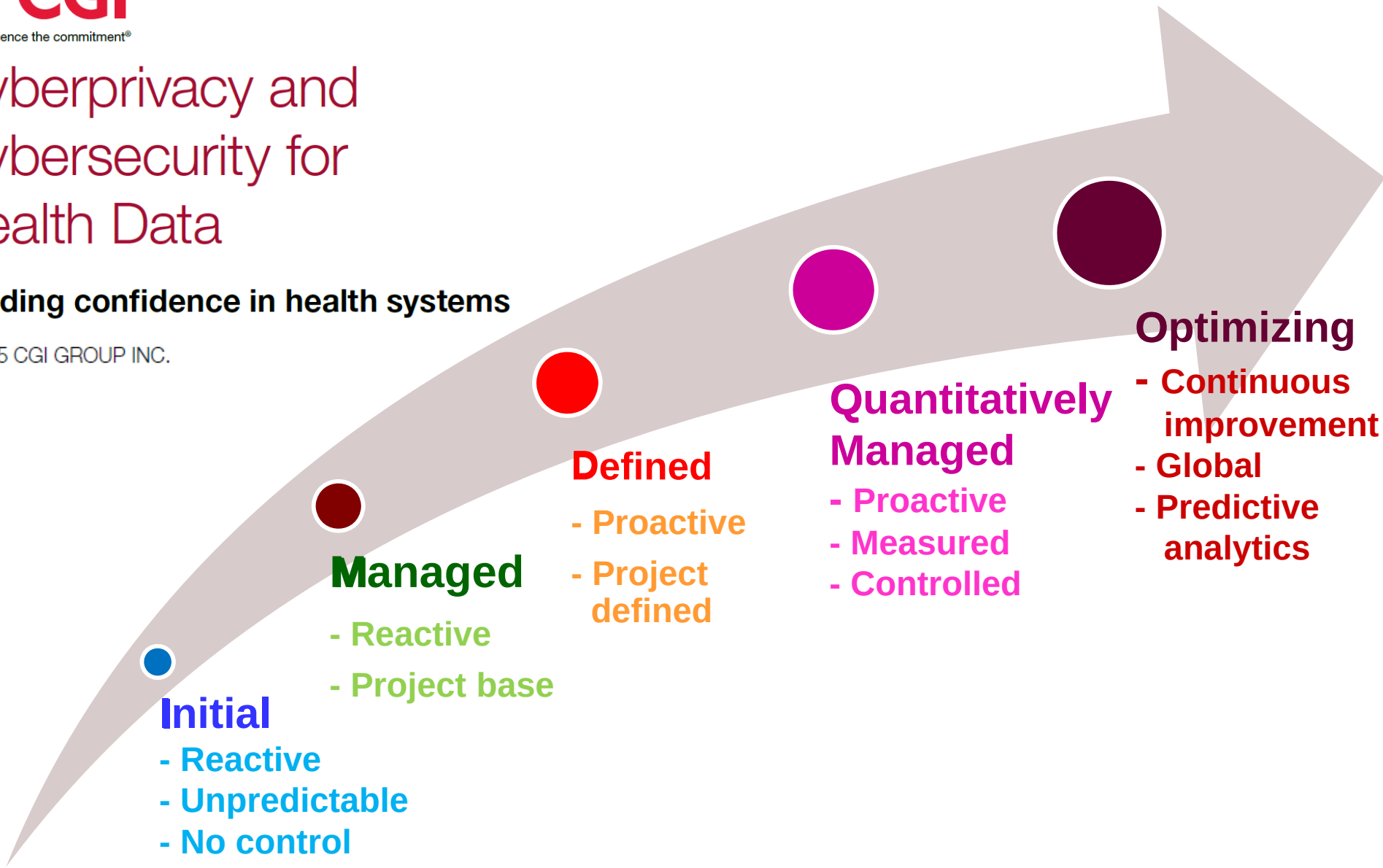
PII - Personally Identifiable Information
PHI - Patient Health Information

CGI

Experience the commitment®

Cyberprivacy and Cybersecurity for Health Data

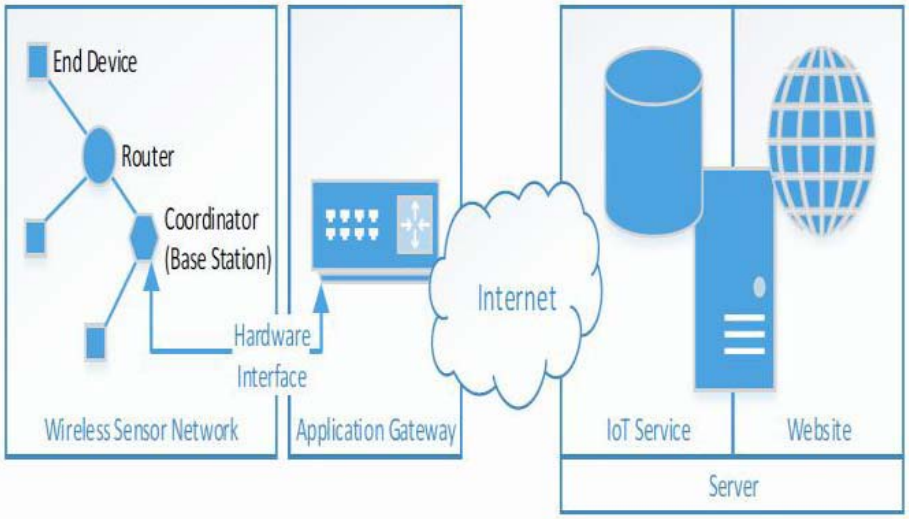
Building confidence in health systems



Privacy and Data Security Issues

- Can your data be shared / sold to third parties?
  - Contributing health information to centralized database of wearable maker; Not covered - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- How secure – Is it Padlocks or Fort Knox?
  - Information encrypted? Periodically review access ? What about monitoring?
- HIPAA cannot help
  - Heartbeats, steps, sleep history - Not considered PHI unless shared with doctor, hospital, 3rd party vendors
- Your Data may be Public-by-default
  - Triple-check default privacy settings & turn off anything not to be shared publicly
- Ownership of your data?
  - Personal data from wearable device - you or business compiling your vitals

WIRELESS COMMUNICATIONS
make physical eavesdropping almost undetectable.



Thank you !!!!!