American Hospital Association®

jriggi@aha.org

(O) +1 202-626-2272
(M) +1 202-640-9159
800 10th Street N.W.
Washington, DC 20001

JOHN RIGGI
Senior Advisor for Cybersecurity and Risk

Experience Summary

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the Senior Advisor for Cybersecurity and Risk for the American Hospital Association (AHA) and their 5000+ member hospitals. In this role John serves as a resource nationally to assist members identify and combat cyber and other sources of risk to their organizations. Additionally, John will support the AHA's policy efforts and Federal agency relations on cyber and other risk related issues. Previously, John led BDO Advisory's Cybersecurity and Financial Crimes Practice. While at the FBI, John served as a representative to the White House Cyber Response Group. He also led the FBI Cyber national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors for the investigation and exchange of information related to national security and criminal-related cyber threats.

John held a national strategic role in the FBI investigation of the largest cyber-attacks targeting healthcare, energy, entertainment, technology, financial services, government and other sectors. John led BDO's exclusive engagement with the AHA to provide cybersecurity training for their 5000+ member hospital CEOs. John is also a governing chair on the Health Information Trust Alliance (HITRUST) initiative to develop the healthcare sector's first cyber threat catalog.

In addition, he serves as an official private sector validator for the White House's Presidential Policy Directive (PPD)-41 on U.S. Cyber Incident Coordination. The PPD is designed to foster an improved working relationship between the public and private sector.

Previously in his career, John served in leadership positions in the FBI's Washington Office Intelligence Division, New York Office Joint Terrorist Task Force, High Intensity Financial Crimes Area Task Force and was the National Operations Manager for the FBI's Terrorist Financing Operations Section. He also served as a senior FBI representative to the CIA's Counterterrorism Center. John is the recipient of the FBI Director's Award for leading a highly successful classified terrorism financing interdiction program and the recipient of the CIA George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest counterterrorism award. John presents extensively on cybersecurity topics and is frequently interviewed by the media on cybersecurity issues.

PROFESSIONAL AFFILIATIONS
Association of Certified Anti-Money Laundering Specialists (ACAMS)
Global Information Assurance Certification (GIAC)
Society of Former Special Agents of the FBI
EDUCATION
B.S, magna cum laude, Criminal Justice, Northeastern University

American Hospital Association

Hospital and Health Systems Government Relations Officers Network Meeting

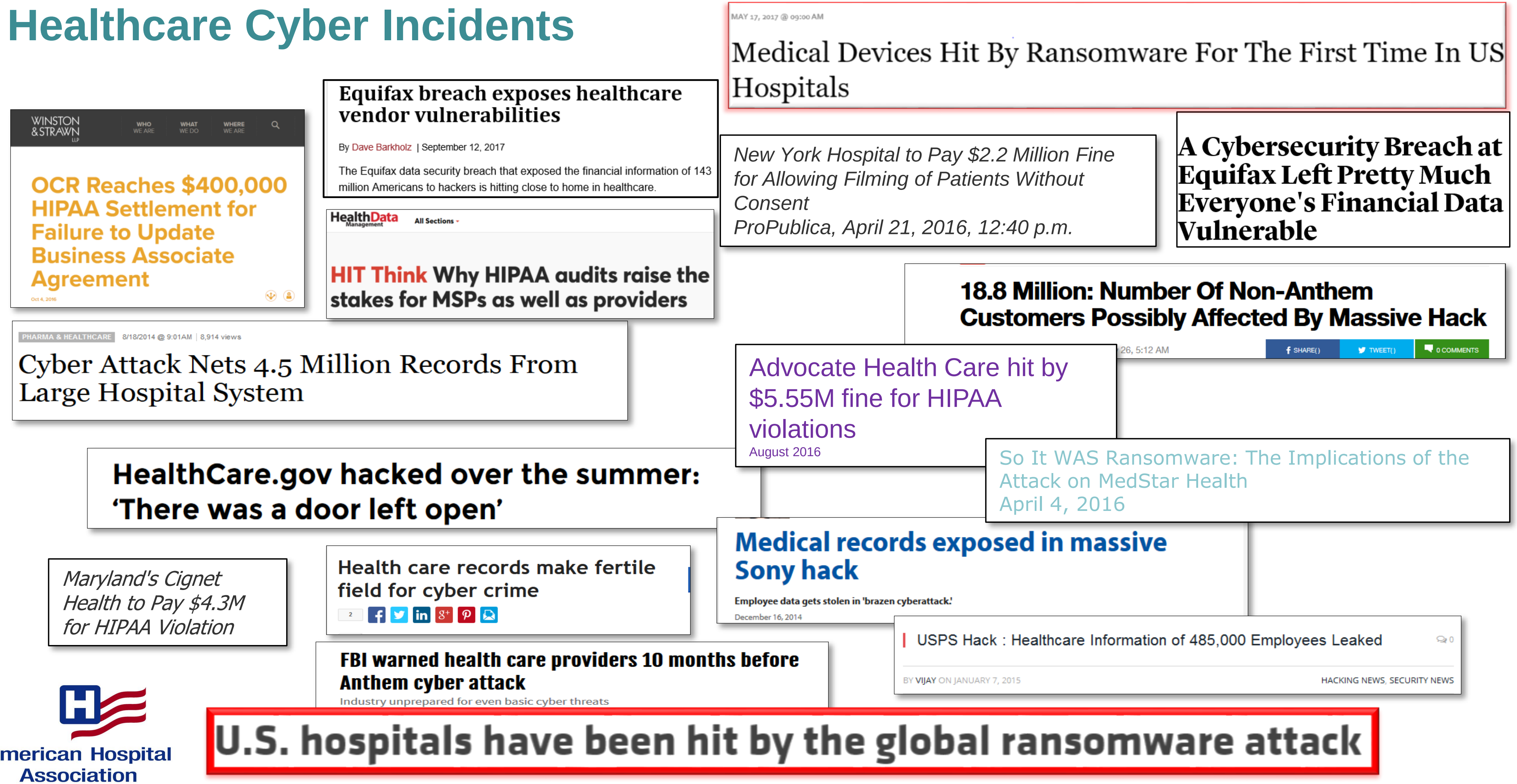
Cyber Threat Landscape in Healthcare

PRESENTED BY:
JOHN RIGGI
SENIOR ADVISOR FOR CYBERSECURITY AND RISK
THE AMERICAN HOSPITAL ASSOCIATION

MARCH 20, 2018

TODAY’S HEALTHCARE CYBER THREAT LANDSCAPE

Healthcare Cyber Incidents



MAY 17, 2017 @ 09:00 AM

Medical Devices Hit By Ransomware For The First Time In US Hospitals

WINSTON & STRAWN LLP WHO WE ARE WHAT WE DO WHERE WE ARE

OCR Reaches $400,000 HIPAA Settlement for Failure to Update Business Associate Agreement

Oct 4, 2016

Equifax breach exposes healthcare vendor vulnerabilities

By Dave Barkholz | September 12, 2017

The Equifax data security breach that exposed the financial information of 143 million Americans to hackers is hitting close to home in healthcare.

New York Hospital to Pay $2.2 Million Fine for Allowing Filming of Patients Without Consent
ProPublica, April 21, 2016, 12:40 p.m.

A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

HealthData Management All Sections

HIT Think Why HIPAA audits raise the stakes for MSPs as well as providers

18.8 Million: Number Of Non-Anthem Customers Possibly Affected By Massive Hack

26, 5:12 AM SHARE() TWEET() 0 COMMENTS

PHARMA & HEALTHCARE 8/18/2014 @ 9:01AM | 8,914 views

Cyber Attack Nets 4.5 Million Records From Large Hospital System

Advocate Health Care hit by $5.55M fine for HIPAA violations

August 2016

HealthCare.gov hacked over the summer: ‘There was a door left open’

So It WAS Ransomware: The Implications of the Attack on MedStar Health
April 4, 2016

Medical records exposed in massive Sony hack

Employee data gets stolen in 'brazen cyberattack.'

December 16, 2014

Maryland's Cignet Health to Pay $4.3M for HIPAA Violation

Health care records make fertile field for cyber crime

2

USPS Hack : Healthcare Information of 485,000 Employees Leaked 0

BY VIJAY ON JANUARY 7, 2015 HACKING NEWS, SECURITY NEWS

FBI warned health care providers 10 months before Anthem cyber attack

Industry unprepared for even basic cyber threats

American Hospital Association

U.S. hospitals have been hit by the global ransomware attack

TODAY'S HEALTHCARE CYBER THREAT LANDSCAPE

INTERNAL THREAT

Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.

COMPUTER INTRUSIONS

This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

RESOURCE HIJACKING

Emerging threat in 2018. Cyber criminals infiltrate and takeover high computing power resources for bitcoin mining.

RANSOMWARE

Nearly 80% of organizations [surveyed in the U.S.] have been victim of a cyber attack during the past 12 months and nearly 50% have been victim of a ransomware attack.

BUSINESS E-MAIL COMPROMISE

Between January 2015 and June 2016, there has been a 1,300% increase in identified exposed losses, a combined exposed dollar loss of more than $3 billion. In the last half of 2016, the FBI received reports of 3,044 U.S. victims reporting losses of $346 million.

DATA EXTORTION

A rising crime. Cyber criminals steal proprietary, sensitive or compromising data from an organization and threaten to publicly release it or provide it to competitors unless a ransom is paid

American Hospital Association

- Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection
- 2016 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2016
- FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA
- Understanding the Depth of the Global Ransomware Problem, Osterman Research Survey Report, Published August 2016, Sponsored by Malwarebytes

TODAY’S CYBER THREAT LANDSCAPE

Data Breaches By the Numbers

47%

caused by malicious or criminal attacks

$3.6 million

average cost of a data breach

31%

increase in total cost of data breach since 2013

$141

average cost per lost or stolen record

$369

average cost per lost or stolen record in healthcare organizations

American Hospital Association

2017 Data Breach Study: Global Analysis, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2017

TODAY'S CYBER THREAT LANDSCAPE

Motivations and Incentives of Cyber-Adversaries

Political-Ideological

HACKTIVISM
Hacktivists might use computer network exploitation to advance their political or social causes.

TERRORISM
Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.

Criminal

CRIME
Individual and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

INSIDER
Insider threat actors typically steal proprietary information for personal, financial or ideological reasons.

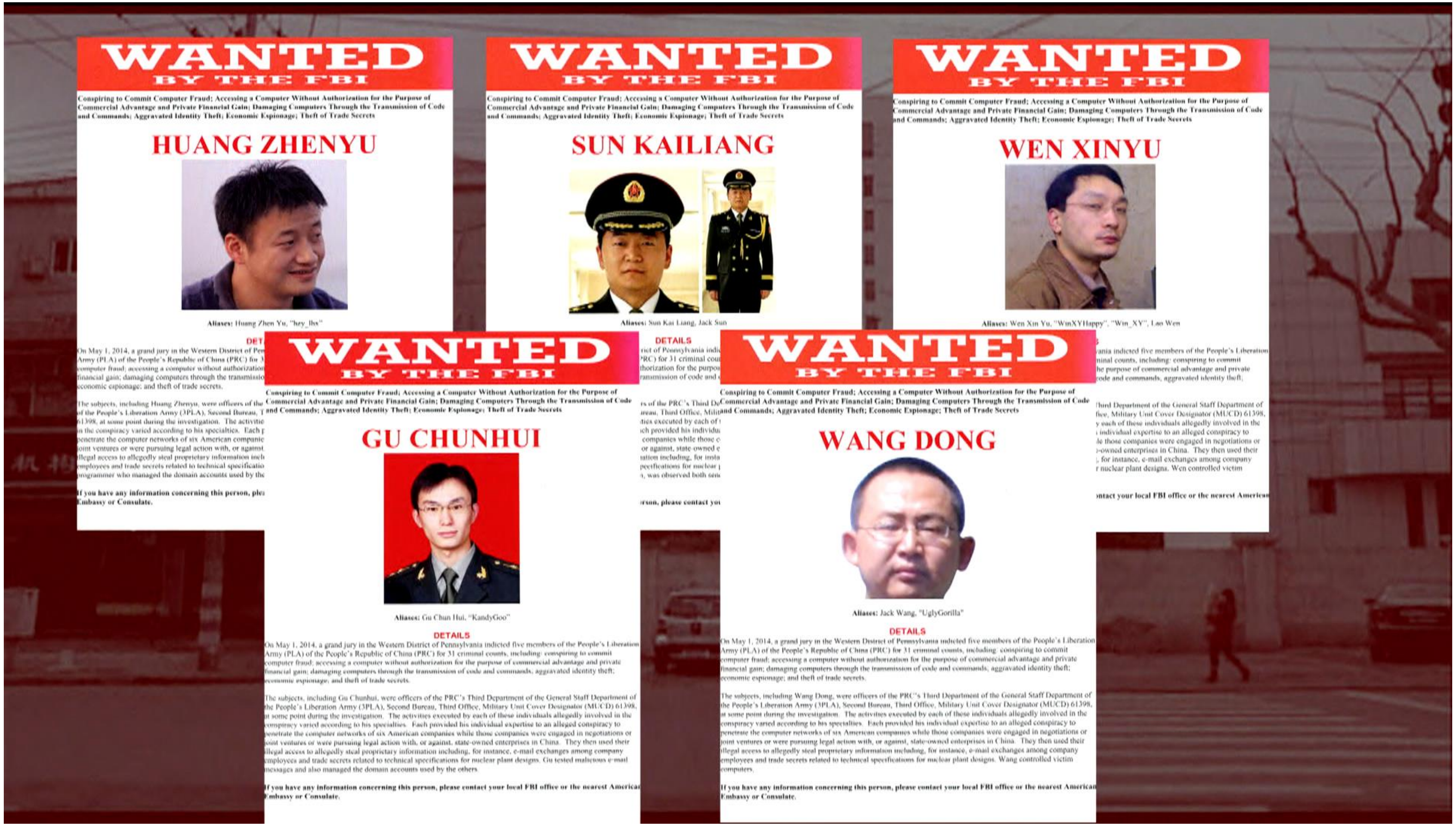
Nation-State

ESPIONAGE
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

WARFARE
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

American Hospital Association

NATION STATE THREATS TO INTELLECTUAL PROPERTY



WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

HUANG ZHENYU

Aliases: Huang Zhen Yu, "hzy_lhx"

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

SUN KAILIANG

Aliases: Sun Kai Liang, Jack Sun

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WEN XINYU

Aliases: Wen Xin Yu, "WinXYHappy", "Win_XY", Lao Wen

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

GU CHUNHUI

Aliases: Gu Chun Hui, "KandyGoo"

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, including Gu Chunhui, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs. Gu tested malicious e-mail messages and also managed the domain accounts used by the others.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WANG DONG

Aliases: Jack Wang, "UglyGorilla"

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

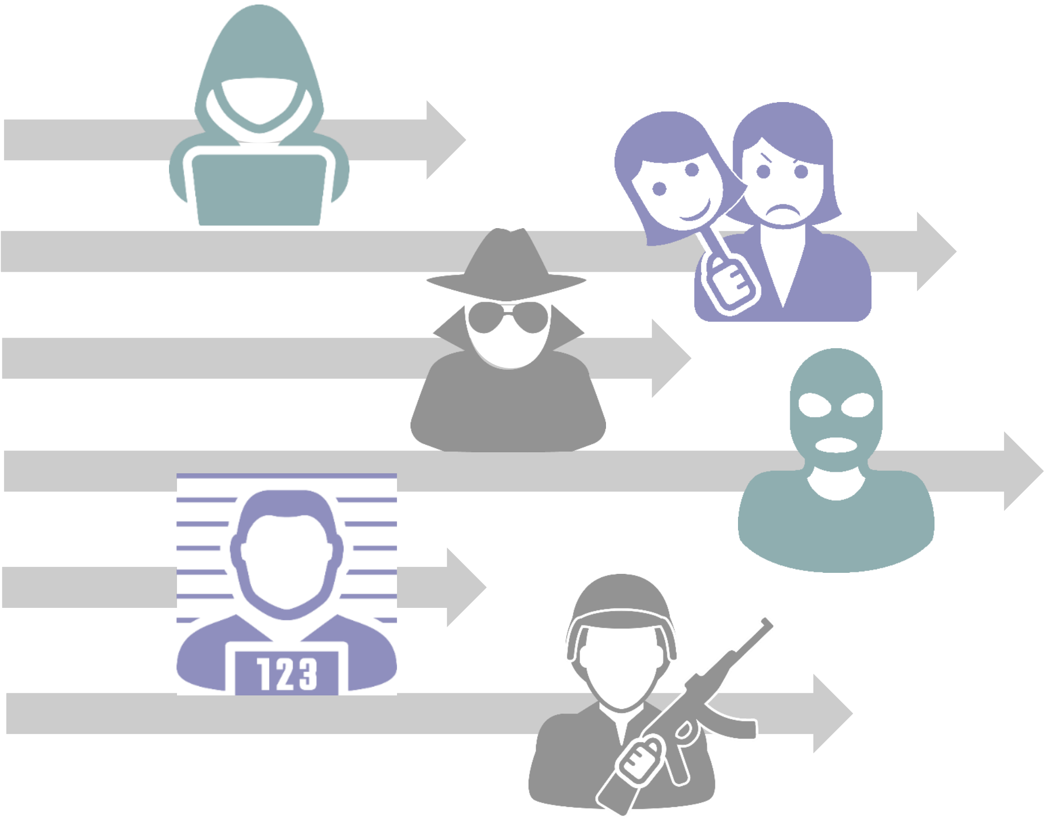
The subjects, including Wang Dong, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs. Wang controlled victim computers.

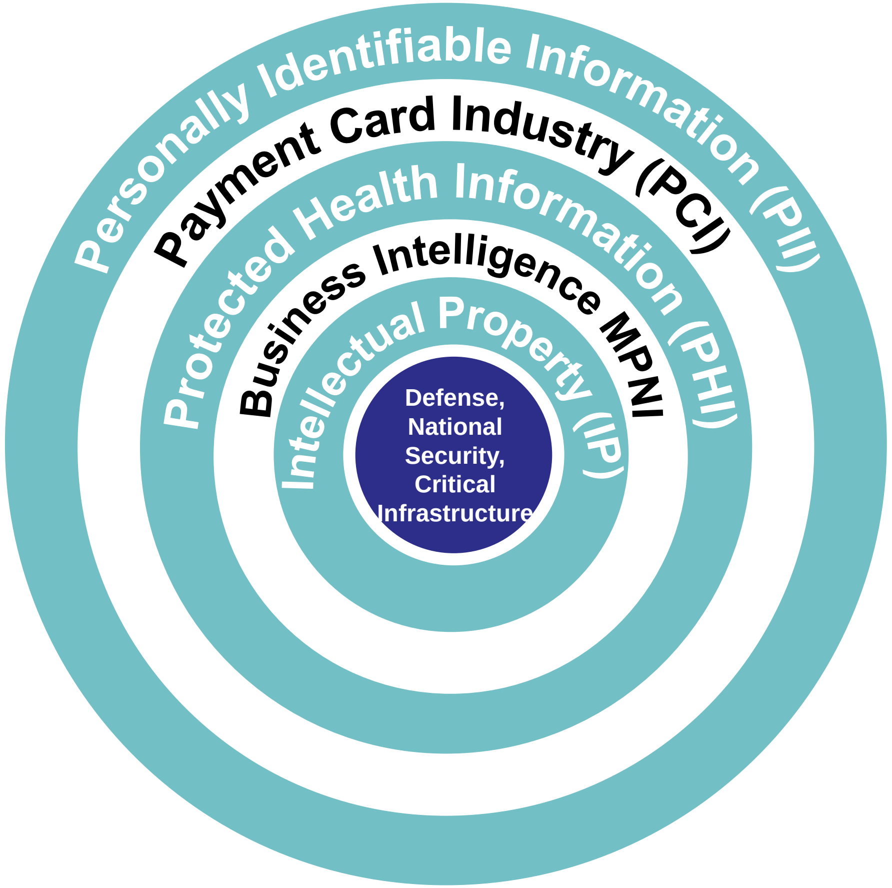
If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

American Hospital Association

TODAY'S CYBER THREAT LANDSCAPE

Targeted Data





Personally Identifiable Information (PII)

Payment Card Industry (PCI)

Protected Health Information (PHI)

Business Intelligence MPNI

Intellectual Property (IP)

Defense, National Security, Critical Infrastructure

American Hospital Association

TODAY’S CYBER THREAT LANDSCAPE

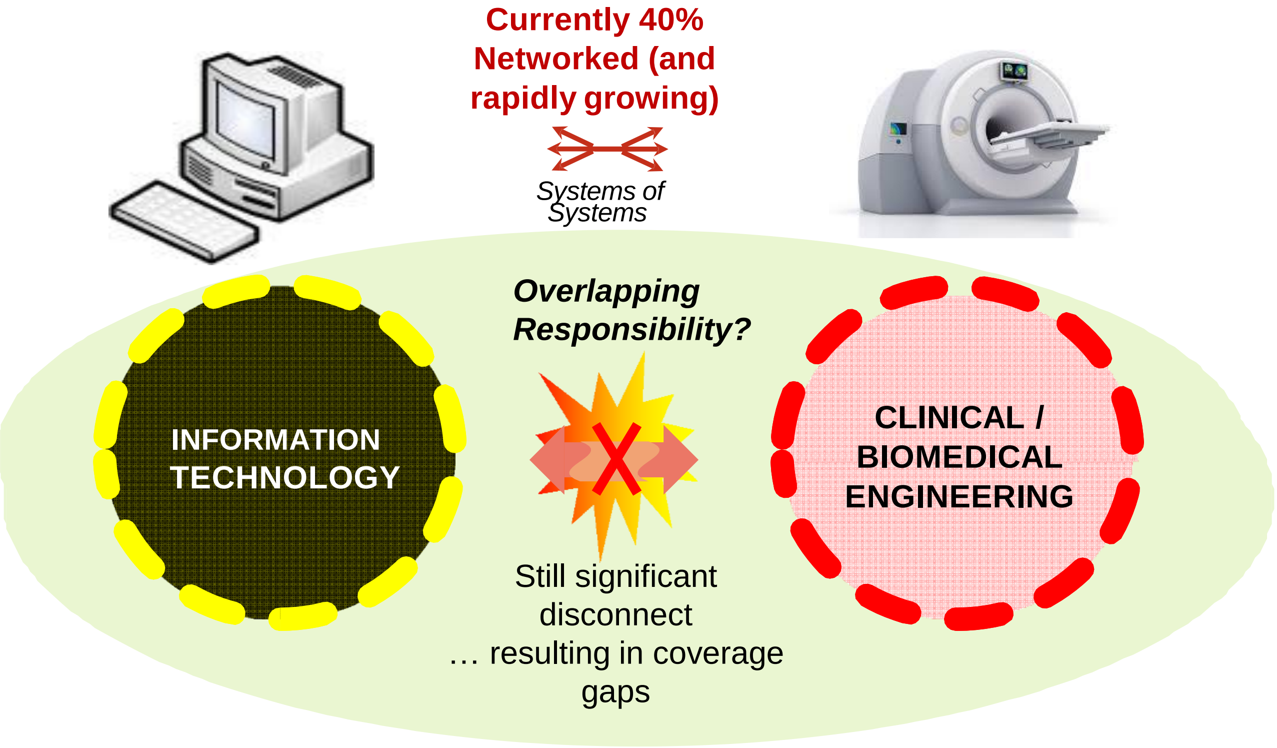
Challenges to the Healthcare Sector

- Legacy computer systems
- Multiple wireless networks – open networks
- Internet enabled medical devices – wireless connections
- Mandatory transition from paper to electronic health records
- “Bring your own device” (BYOD) policy
- Only sector which stores and combines PII, PHI, PCI, **Medical Research and Intellectual Property**
- Mergers & Acquisitions create PHI inventory challenges
- Victims are often unaware when PHI is stolen
- Third party vendors with network access
- Higher payout on the black market
- Cybercrime displacement from financial services

American Hospital Association

Medical Devices & Systems: Shared Responsibility

Degree of Integrated Support



Currently 40% Networked (and rapidly growing)

Systems of Systems

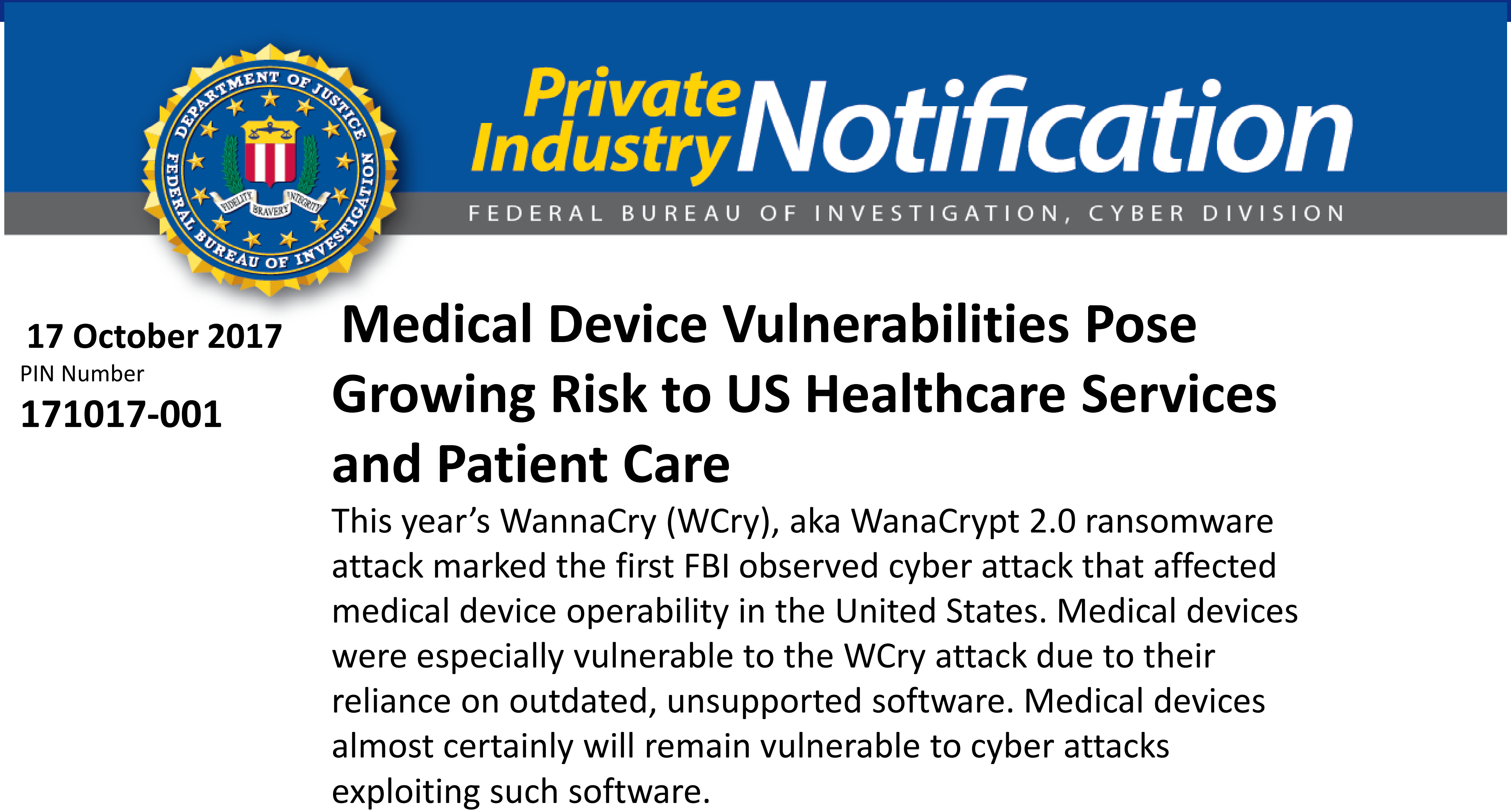
Overlapping Responsibility?

INFORMATION TECHNOLOGY

CLINICAL / BIOMEDICAL ENGINEERING

Still significant disconnect … resulting in coverage gaps

American Hospital Association



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 October 2017

PIN Number

171017-001

Medical Device Vulnerabilities Pose Growing Risk to US Healthcare Services and Patient Care

This year's WannaCry (WCry), aka WanaCrypt 2.0 ransomware attack marked the first FBI observed cyber attack that affected medical device operability in the United States. Medical devices were especially vulnerable to the WCry attack due to their reliance on outdated, unsupported software. Medical devices almost certainly will remain vulnerable to cyber attacks exploiting such software.

American Hospital Association

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

29 December 2017

PIN Number

171228-001

Recent WannaCry Attribution to North Korea Demonstrates Persistent Cyber Targeting of US Interests

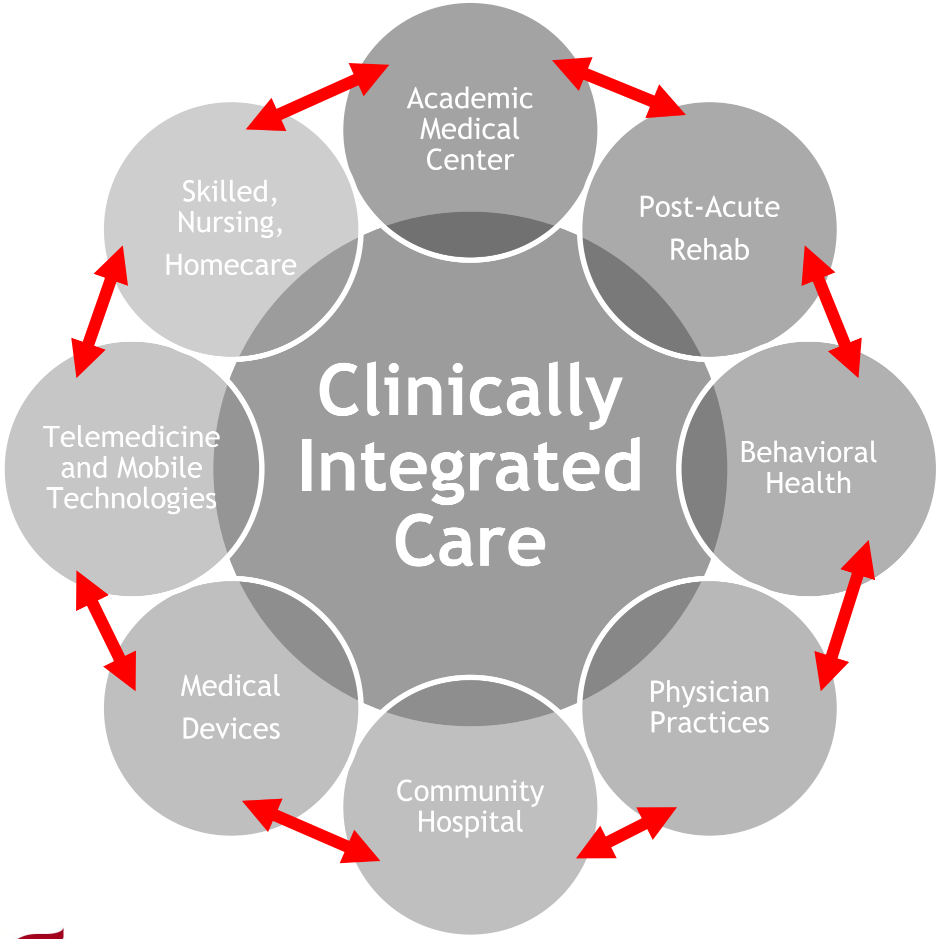
Summary

On 19 December, the US Government publicly attributed the 2017 WannaCry malware outbreak to North Korea cyber actors. The WannaCry event underscores the continued intent and increasing capability of Pyongyang to conduct cyber attacks against US and international interests. The North Korean government has devoted significant resources to developing its cyber operations, which have grown increasingly sophisticated. The FBI encourages the US private sector to remain vigilant, evaluate network security, and report suspicious network activities to their local FBI offices or FBI CyWatch.

American Hospital Association

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Emerging Cybersecurity Risk Issues - The Movement Toward Clinically Integrated Care



Various forces—including the move toward payment tied to quality, clinical outcomes and episodes of care—are driving clinical integration across provider types, leading to new and more complex data sharing and integration requirements for providers. Clinical integration is also including telemedicine and mobile technologies.

American Hospital Association

Emerging Cybersecurity Risk Issues - Telemedicine in Transforming Healthcare

Expanded insurance coverage & growing demand has meant an increase in telemedicine requiring an increased information exchange. Telemedicine expenses are now included in bundled payment models by CMS. This will lead to acceleration of adoption of telemedicine.

The percentage of providers that have telemedicine programs:

72% of Hospitals

52% of Physician Groups

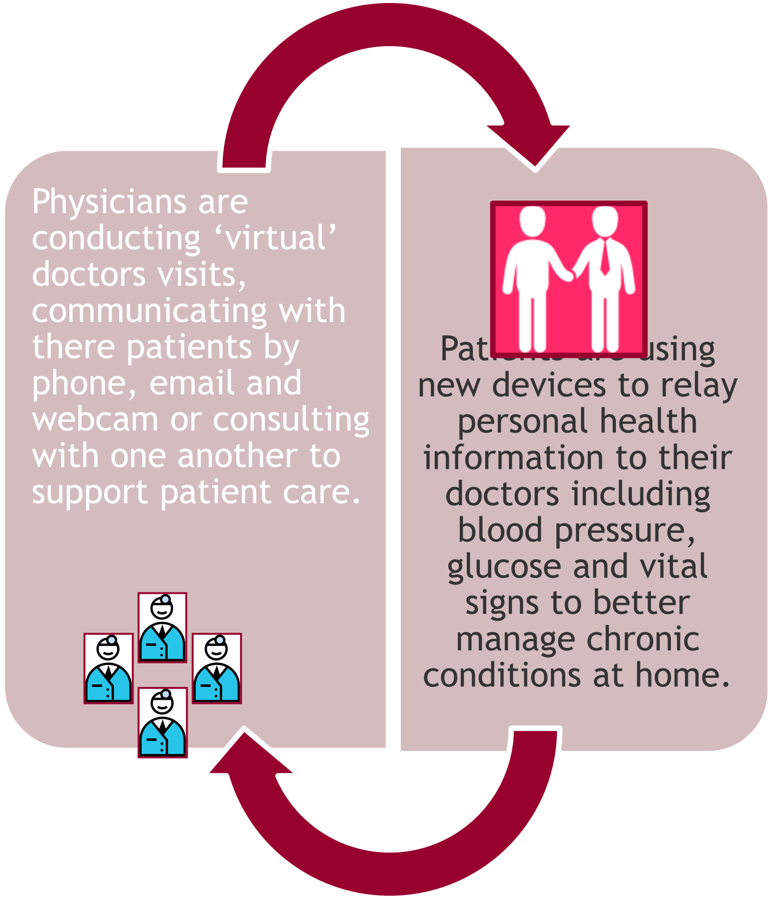
The number of virtual doctor visits in the U.S.

2015
1 million

2016
1.2
million

In 2016, more than 15 million Americans received some kind of medical care remotely. This number is expected to grow by

30% in 2017.



Physicians are conducting ‘virtual’ doctors visits, communicating with there patients by phone, email and webcam or consulting with one another to support patient care.

Patients are using new devices to relay personal health information to their doctors including blood pressure, glucose and vital signs to better manage chronic conditions at home.

American Hospital Association

American Telemedicine Association (virtual doctor visits); Avizie survey of 280 health-care executives, March 2016 (providers); National Business Group on Health survey of 140 large employers (benefits). The Wall Street Journal.

How Telemedicine is Transforming Healthcare. By Melinda Beck. The Wall Street Journal. June 26, 2016.

Questions ?

John Riggi

202-626-2272

jriggi@aha.org

American Hospital Association