Cybersecurity: Expanding patient access to health services also expands the cyber threat surface

Richard Staynings

Chief Security Strategist, Cylera
Faculty, University of Denver
Chief Security Officer, Cyber Associates

CYLERA

UNIVERSITY OF DENVER

Abstract

This session will explore the changing healthcare technology delivery landscape, the rapid adoption of ML and other forms of AI across healthcare, innovative new healthcare IoT and IT technologies and the democratization of health data to mobile apps, medical wearables and remote patient services. Data truly is king, and not just for clinical decision support, but for medical research and so much more.

But medical data is valuable to hackers both via its theft, and through extortion by prevention of access to that data or the systems that process it, and this is one of many reasons why providers are the target of growing cyber-attacks. As our services expand beyond hospital walls so does the threat surface and this drives up risks and leads to demands for new regulation for healthcare security and privacy.

But effective cybersecurity can be an enabler of new health services. Services which without advances in cybersecurity would simply be considered too risky to implement. Two decades ago, the idea of providing patients access to their own medical data via the internet seemed a pipe dream. Today we allow patients to upload their personal medical data from a consumer fitness app to their PCP managed EHR. We allow patients to be treated and monitored in their homes via remote medical services and even to die in their own homes supported by necessary medical equipment, all of which has to be securely managed by a provider. But how do we ensure that medical data and systems are secure and that patient safety risks are not being introduced through increased convenience to those patients?

Healthcare globally is undergoing perhaps its greatest transition since the discovery of Penicillin

Digital Health is driving patient outcomes and improving provider efficiency

But what do we mean by the term ‘Digital Health’?

“THE APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTS) TO EXCHANGE MEDICAL INFORMATION FOR VARIOUS INTENDED USES “

Meyers, A., & Wulfovich, S. (2020). Digital Entrepreneurialship

- Telehealth
- Electronic medical records
- Big data and analytics
- Remote patient monitoring
- Patient reported outcomes

- Virtual and augmented reality
- Blockchain
- Artificial intelligence
- Mobile medical apps
- Digital therapeutics

Digital Health has turned the industry on its head.

It’s changed the way we work and changed how patients interact with their care teams.

Covid Transformed: Telehealth, Telemedicine & other Remote Services

Medical wearables / apps will transform healthcare

Patients able to contribute data to their own medical record

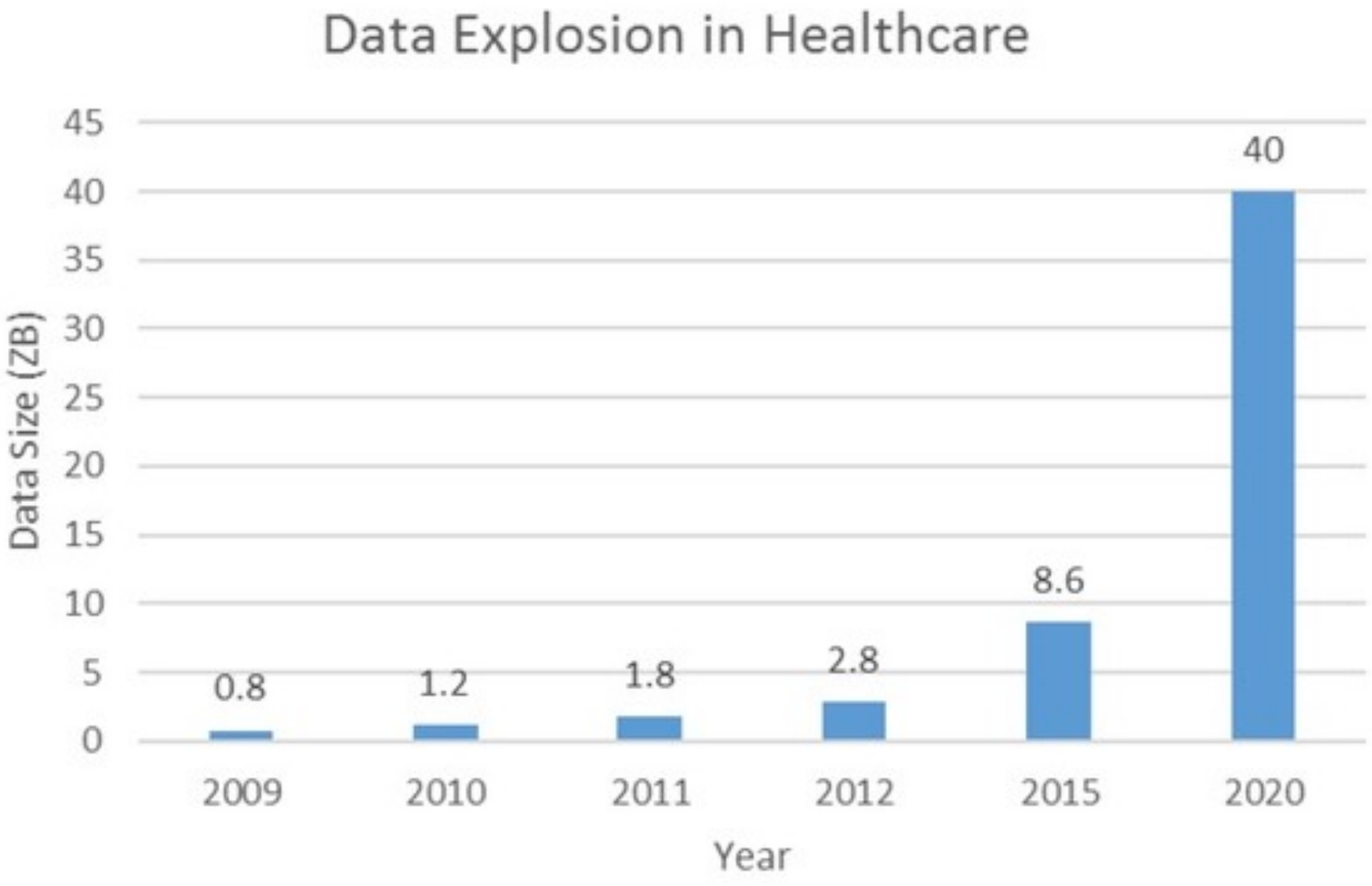
My Health Record

Leading to a massive growth in the size of patient records

What once filled up a manilla file at our GP / PCP, now takes up huge volumes of digital data across **multiple** clouds and across **multiple** local hospital data centers.

Much of it duplicated!

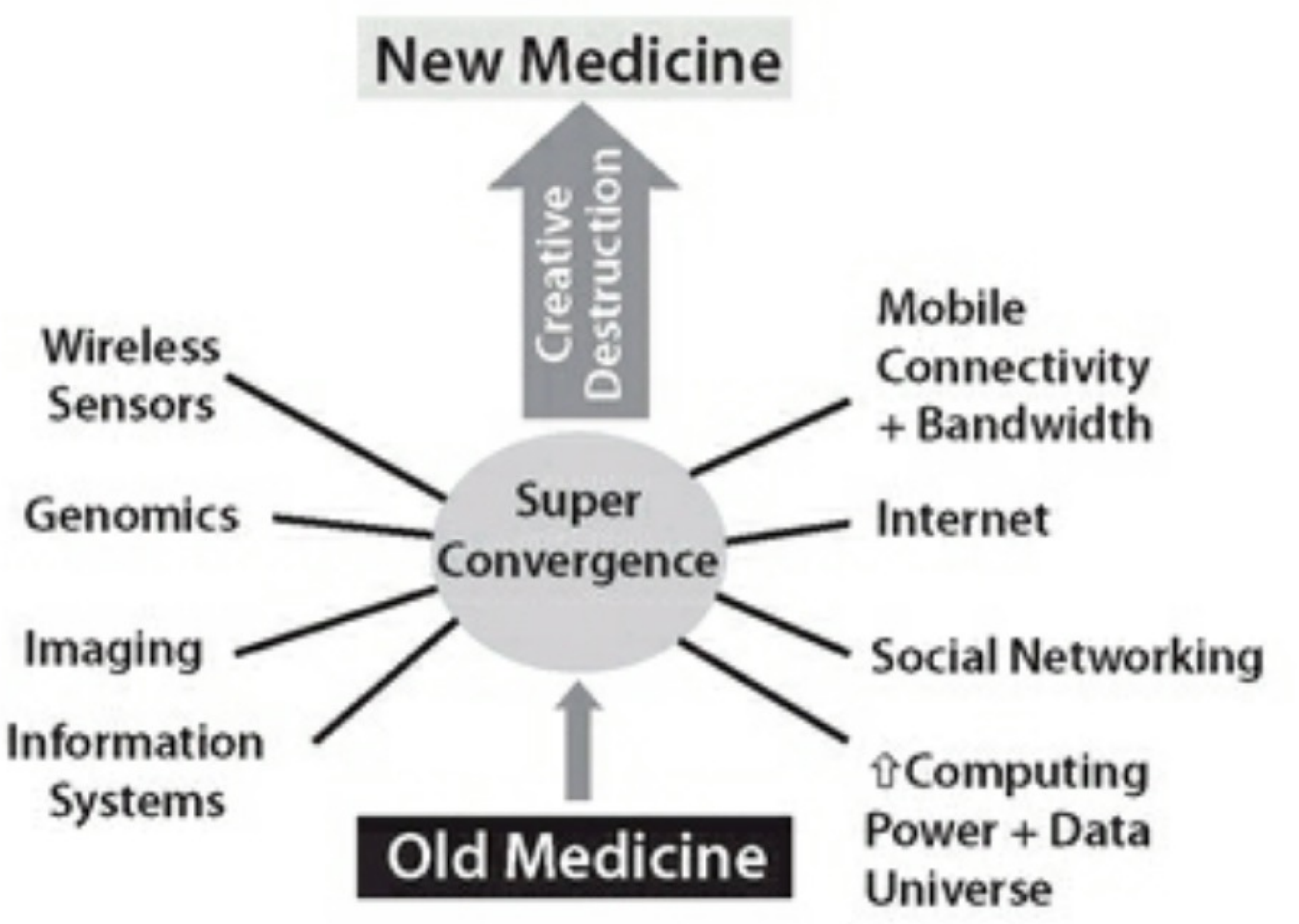
Explosion of medical data



1 ZB = 1 billion TB

Hong, Big Data in Health Care, Data and Information Management 2 (3), Dec 2018

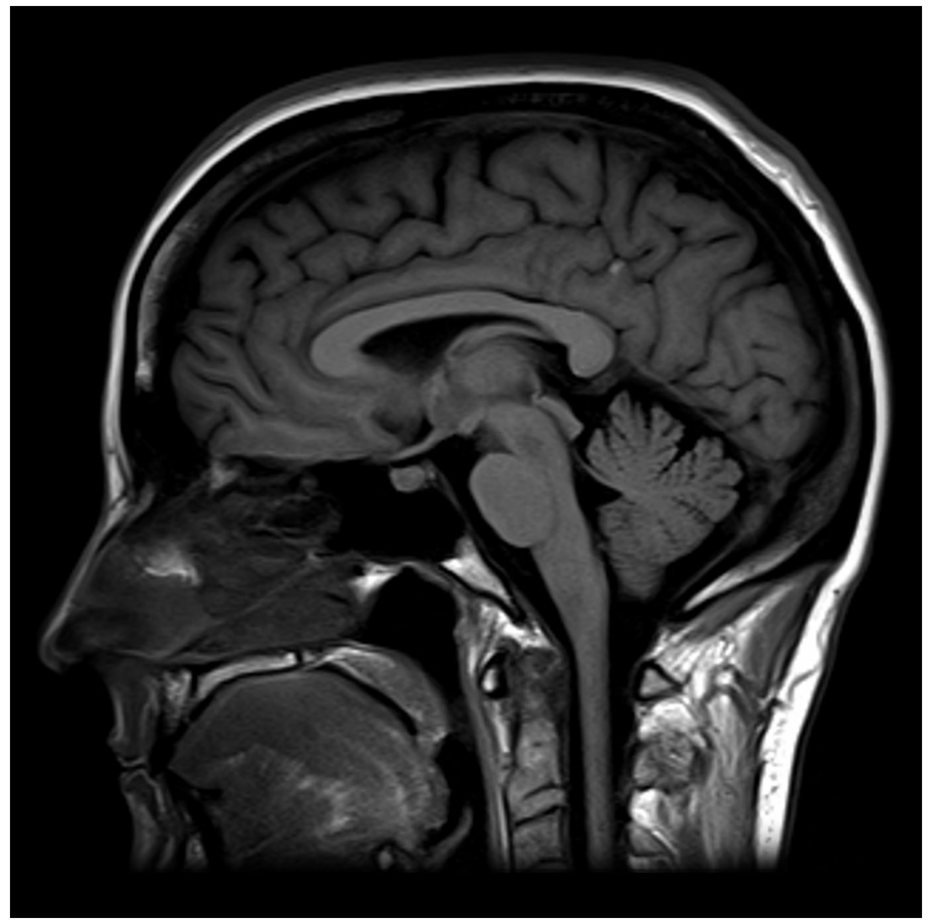
For the first time in history, we can digitize humans!



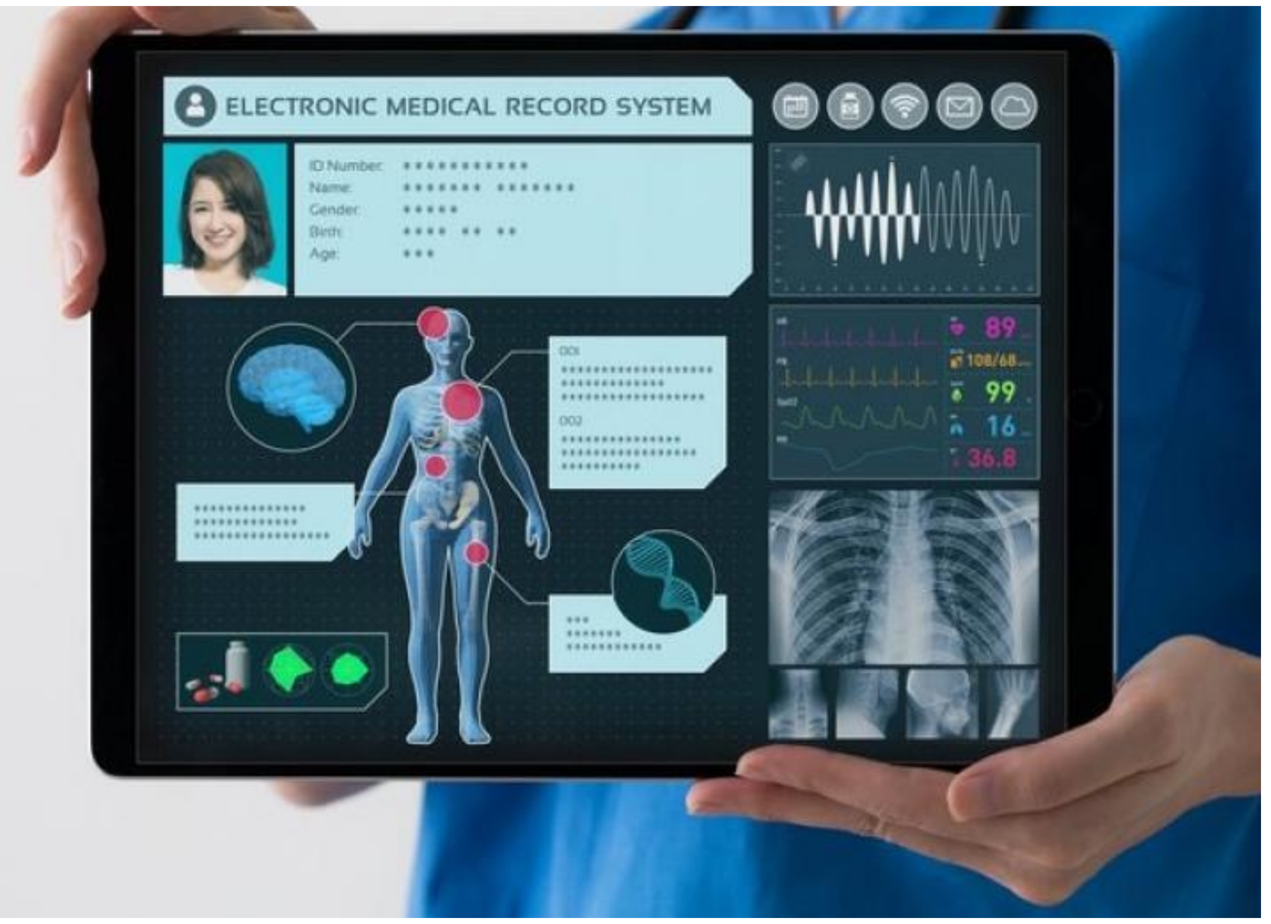
Topol, Creative destruction of Medicine, 2013

Physiology

Biology



Anatomy



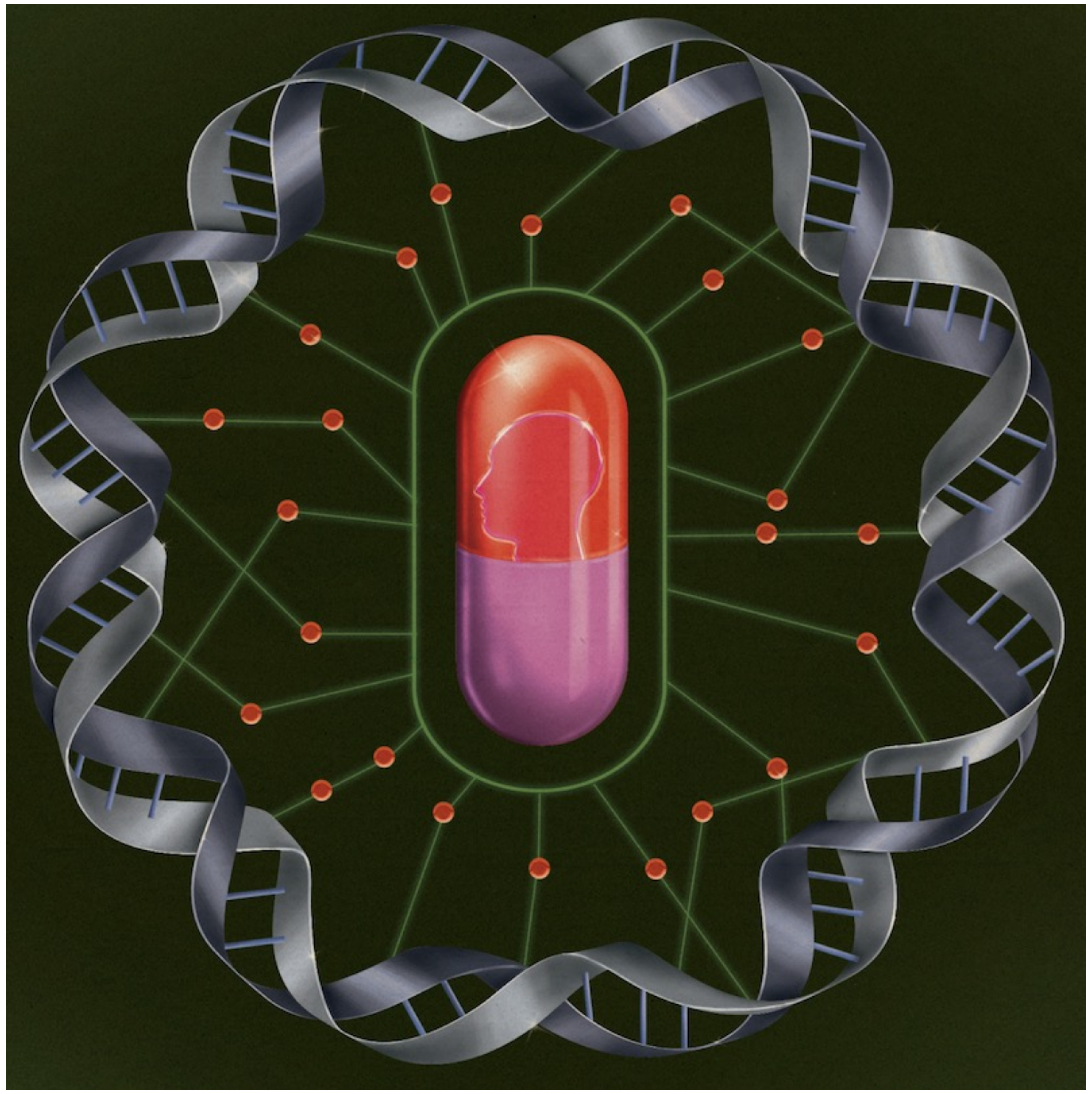
EHR

Big Data is changing clinical decision support

And Personalized Medicine will transform healthcare

Past

- evidence-based medicine
- shaped by guidelines
- indexed to population
- not to individuals
- relies on median



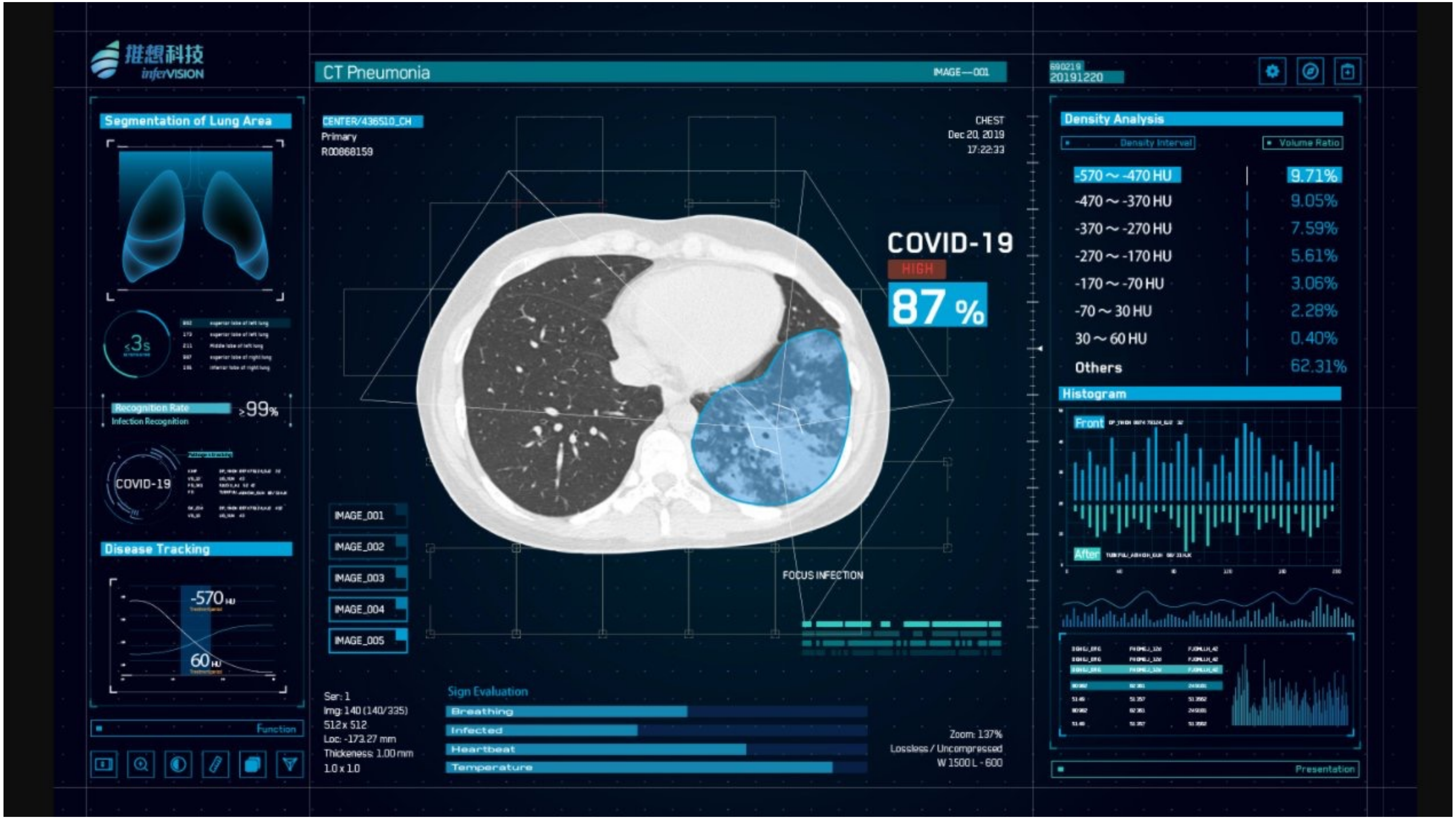
Future

- personal data based medicine
- individual features
- anchored to individual
- tailored care

Using a patient's DNA

Artificial Intelligence in medicine is transformational

AI enhanced diagnosis is driving COVID care



Density Interval	Volume Ratio
-570 ~ -470 HU	9.71%
-470 ~ -370 HU	9.05%
-370 ~ -270 HU	7.59%
-270 ~ -170 HU	5.61%
-170 ~ -70 HU	3.06%
-70 ~ 30 HU	2.28%
30 ~ 60 HU	0.40%
Others	62.31%

Ai algorithms help detect brain tumors

But healthcare data is valuable

- Its valuable to take care of patients
- Its also valuable to other nation states looking to compete with the United States
- Its valuable to cyber criminals looking to monetize stolen data
- And it presents compliance and cybersecurity risks
- The more data you have the more difficult it is to protect

However: New Technologies Expand the Attack Surface

!
ATTACK SURFACE
CONCEPT, TYPES, TOOLS AND ATTACK SURFACE REDUCTION STRATEGIES

Breaches of Confidentiality

Date	Entity	#	Cause
2015	Anthem	78M	Hacking
2019	Quest Diagnostics	12M	Hacking
2015	Premera Blue Cross	11M	Hacking
2015	Excellus Health Plan	10M	Hacking
2019	Lab Corp	8M	Hacking
2014	CHS	6M	Hacking
2011	Science Applications International Corp	5M	Theft
2014	CHS Prof Services Corp	4.5M	Hacking
2015	UCLA Health	4.5M	Hacking
2013	Advocate Medical Group	4M	Theft

HHS breach report portal

Attacks against Availability

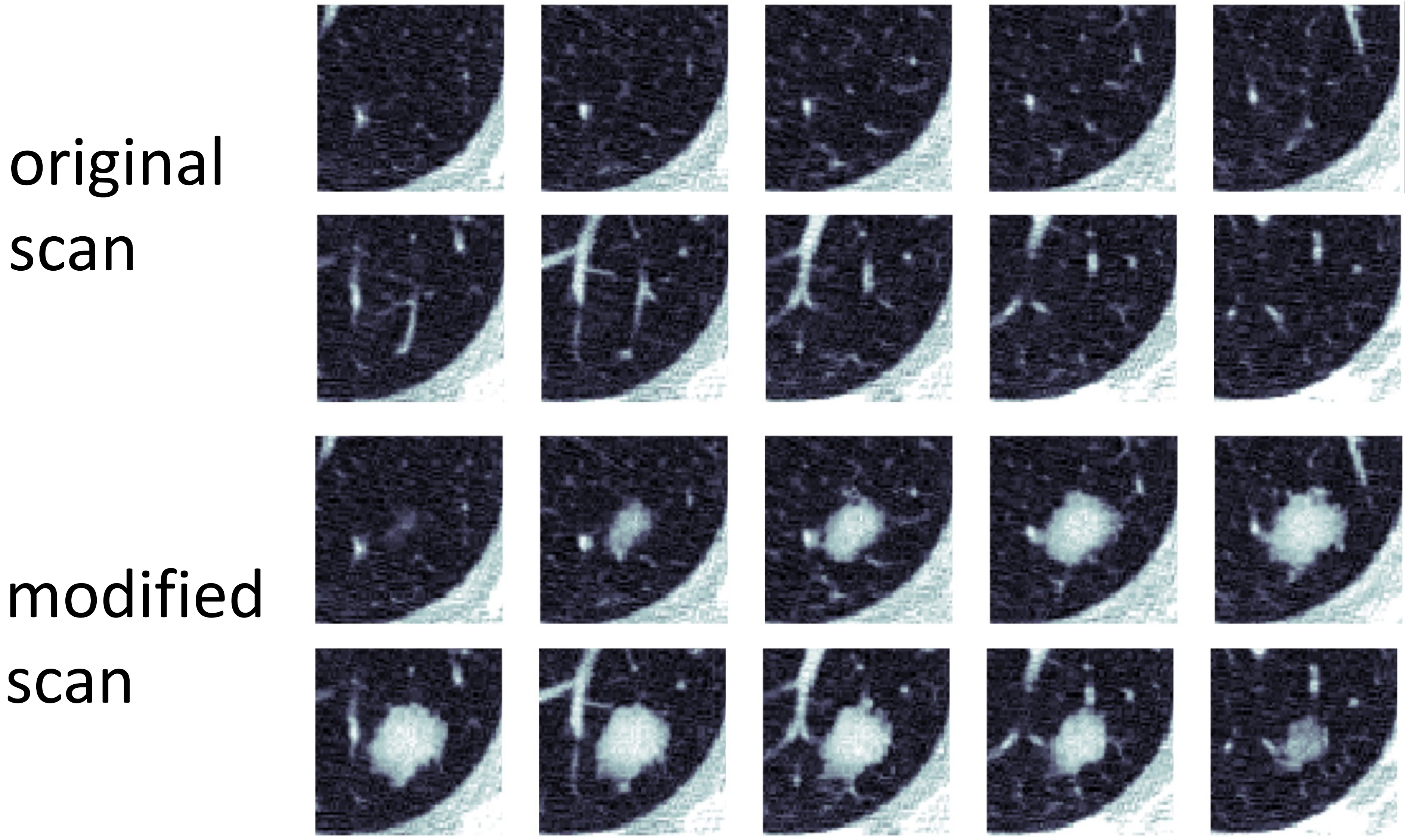
BROOKSIDE
MEDICAL CENTER
Mansion Street Womens Health, P.L.L.C.
Great Lakes Plastic & Hand Surgery
Cereal City Medical
New Day Family Medicine & Medical Spa P.C.

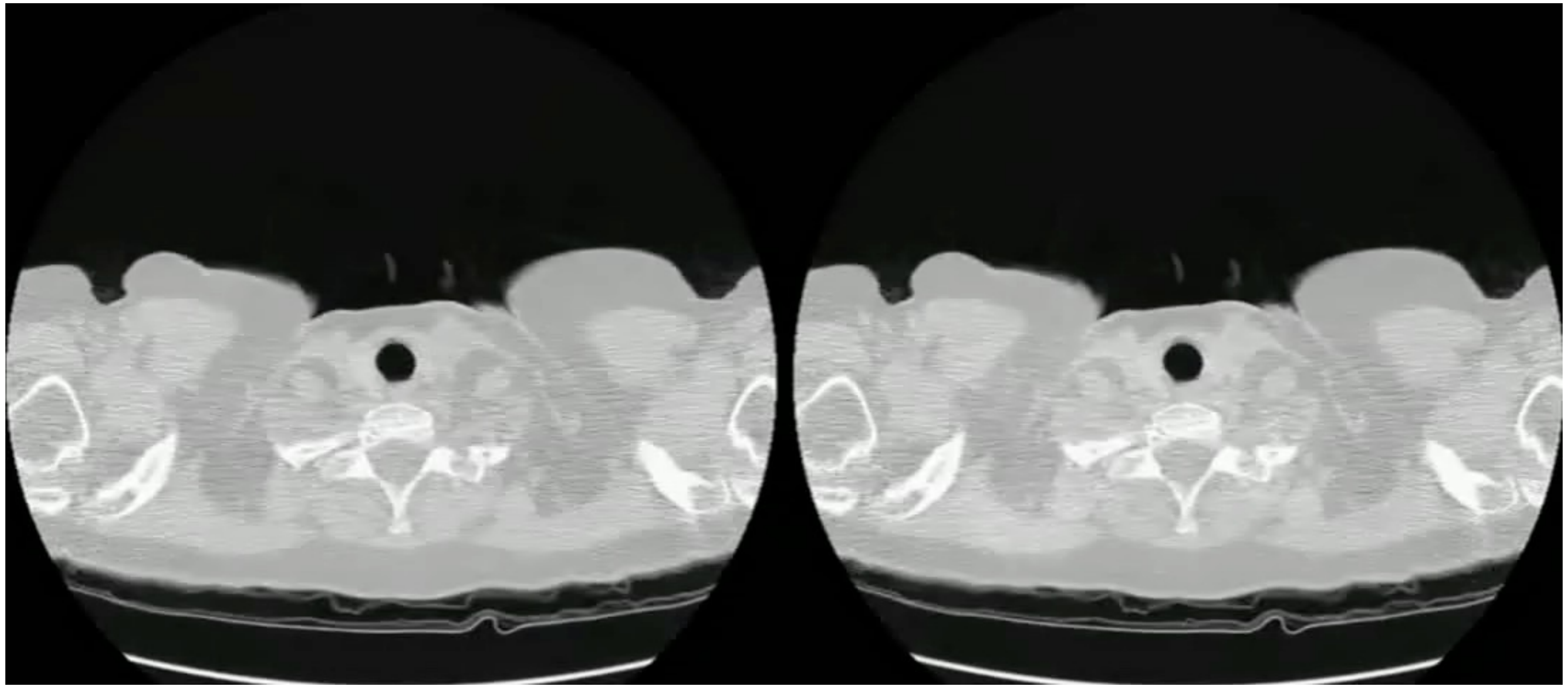
- Medical practice in Michigan
- Apr 2019: ransomware attack
- Encrypted all medical records
- $6,500 ransom demanded
- FBI advised not to pay ransom
- Doctors did not pay
- Hackers deleted all medical records
- Impossible to recover records
- **Doctors decided to shut down clinic and retire**

Attacks against Integrity of Medical Data

Hacking medical images

- Intercept images on network between scanner and PACS
- Add or subtract nodules on CT images using deep-learning





Original

Fake nodules

Radiologists fooled by:

- added fake nodules (99%)
- removed nodules (94%)

Ben-Gurion University of the Negev

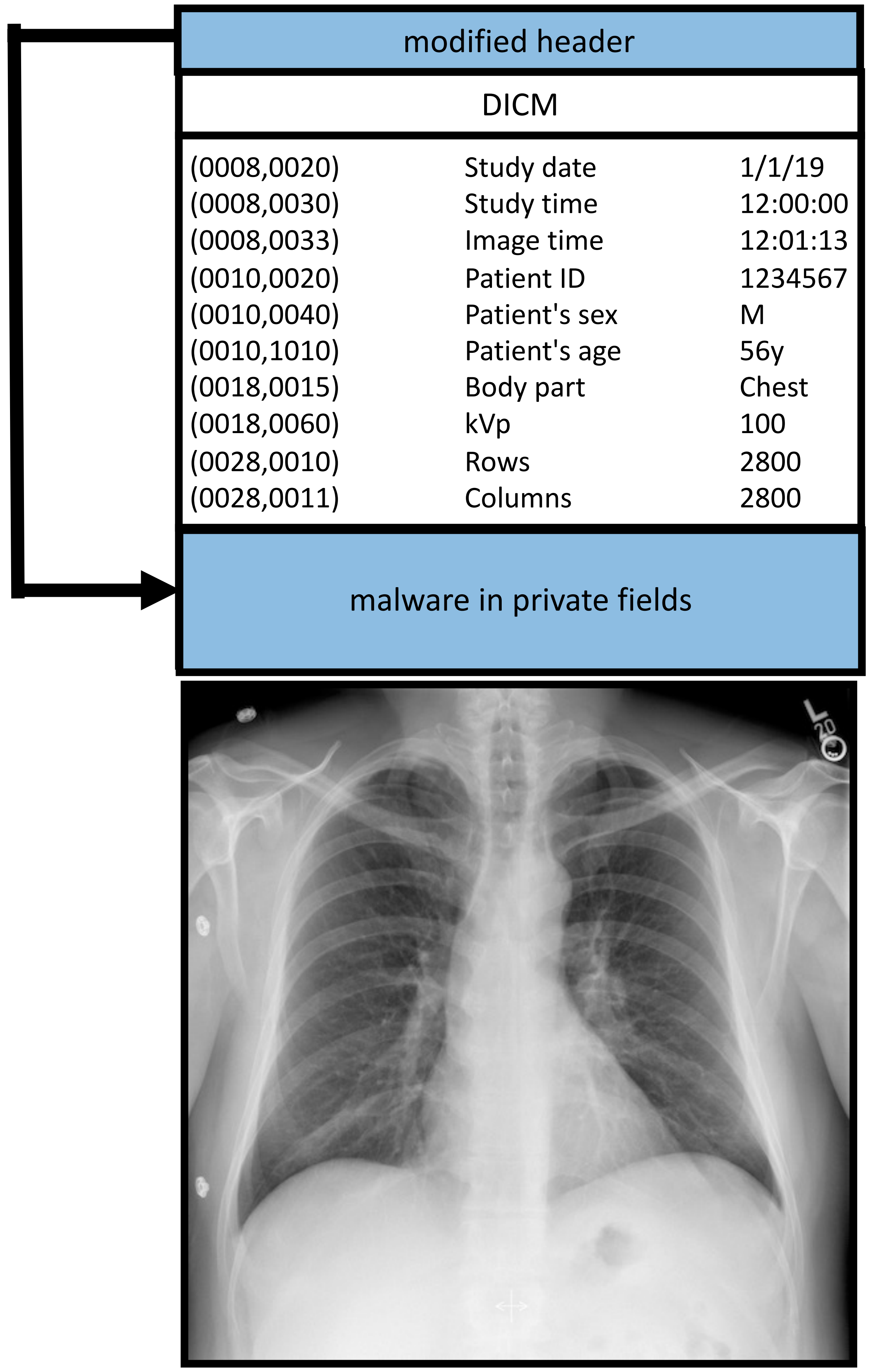
Mirsky et al, arXiv:1901.03597v2, Apr 2019

Medical data can contain malware

- Modified DICOM files
- Header (preamble)
  - used for dual personality files
  - replaced by executable file header
- Private fields
  - replaced by malware

CYLERA

Picado Ortiz, Apr 2019, labs.cylera.com/2019/04/16/pe-dicom-medical-malware/



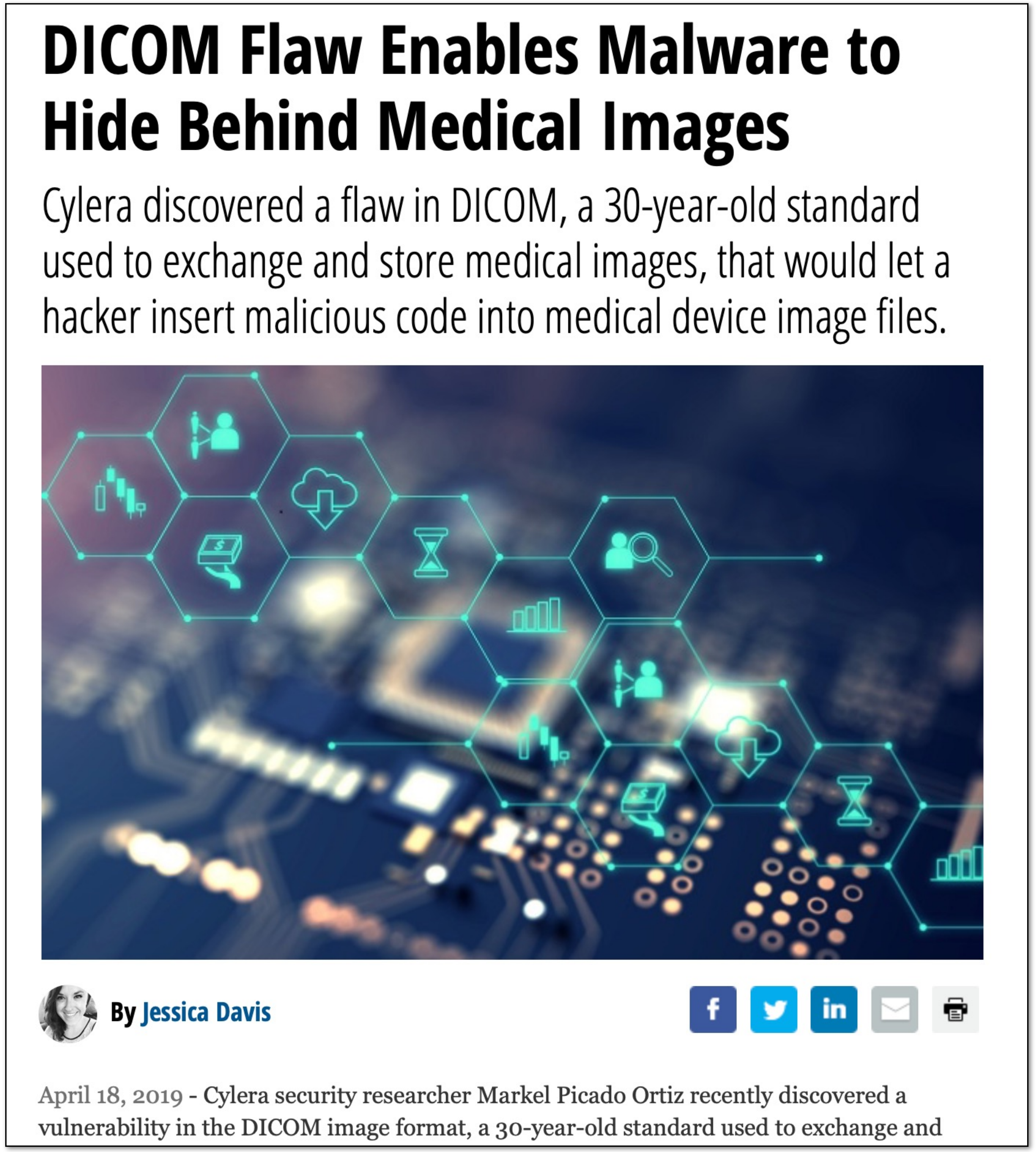
modified header

DICM

(0008,0020)	Study date	1/1/19
(0008,0030)	Study time	12:00:00
(0008,0033)	Image time	12:01:13
(0010,0020)	Patient ID	1234567
(0010,0040)	Patient's sex	M
(0010,1010)	Patient's age	56y
(0018,0015)	Body part	Chest
(0018,0060)	kVp	100
(0028,0010)	Rows	2800
(0028,0011)	Columns	2800

malware in private fields

DICOM file

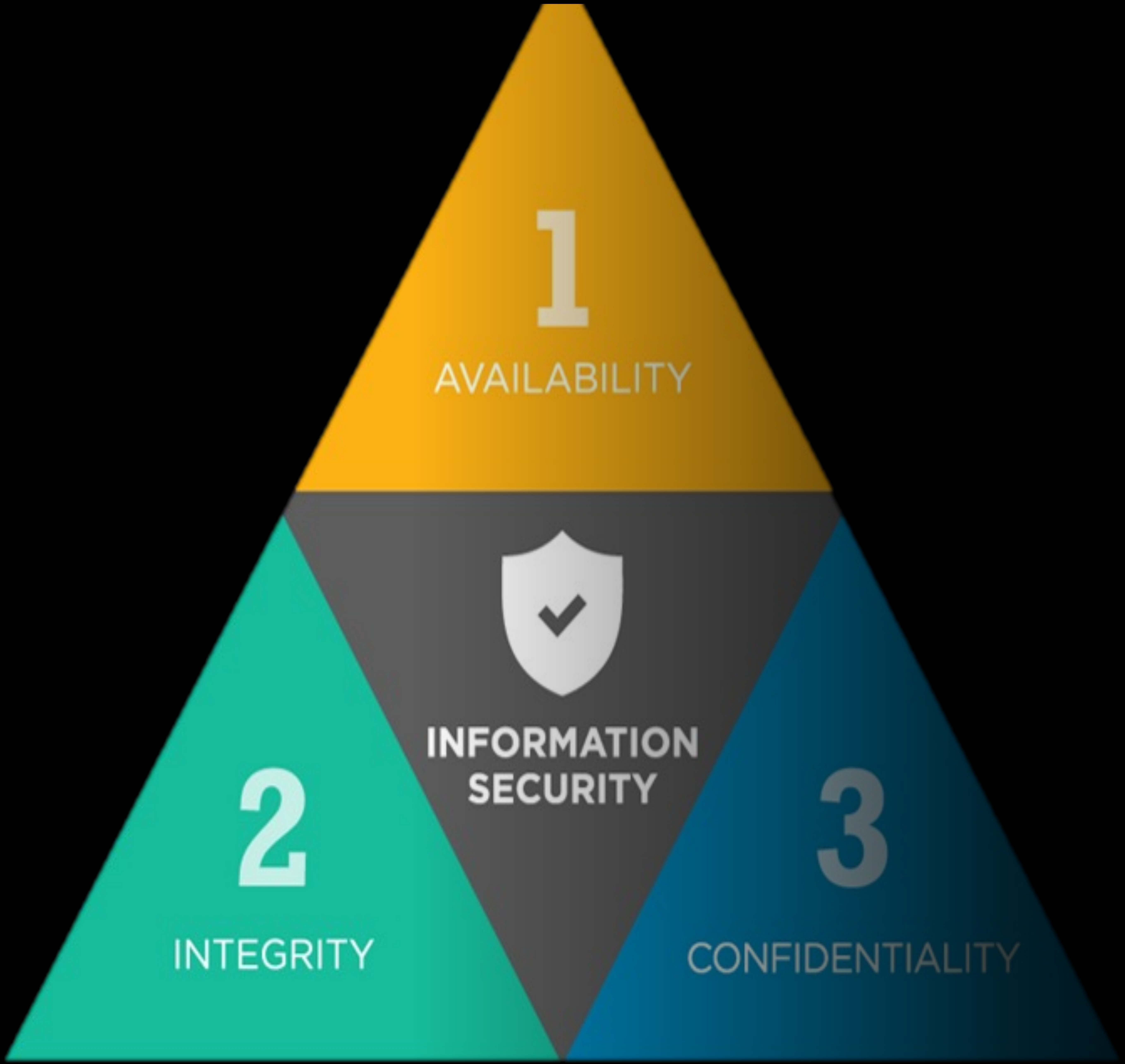


DICOM Flaw Enables Malware to Hide Behind Medical Images

Cylera discovered a flaw in DICOM, a 30-year-old standard used to exchange and store medical images, that would let a hacker insert malicious code into medical device image files.

By Jessica Davis

April 18, 2019 - Cylera security researcher Markel Picado Ortiz recently discovered a vulnerability in the DICOM image format, a 30-year-old standard used to exchange and



Cybersecurity
The CIA Triad

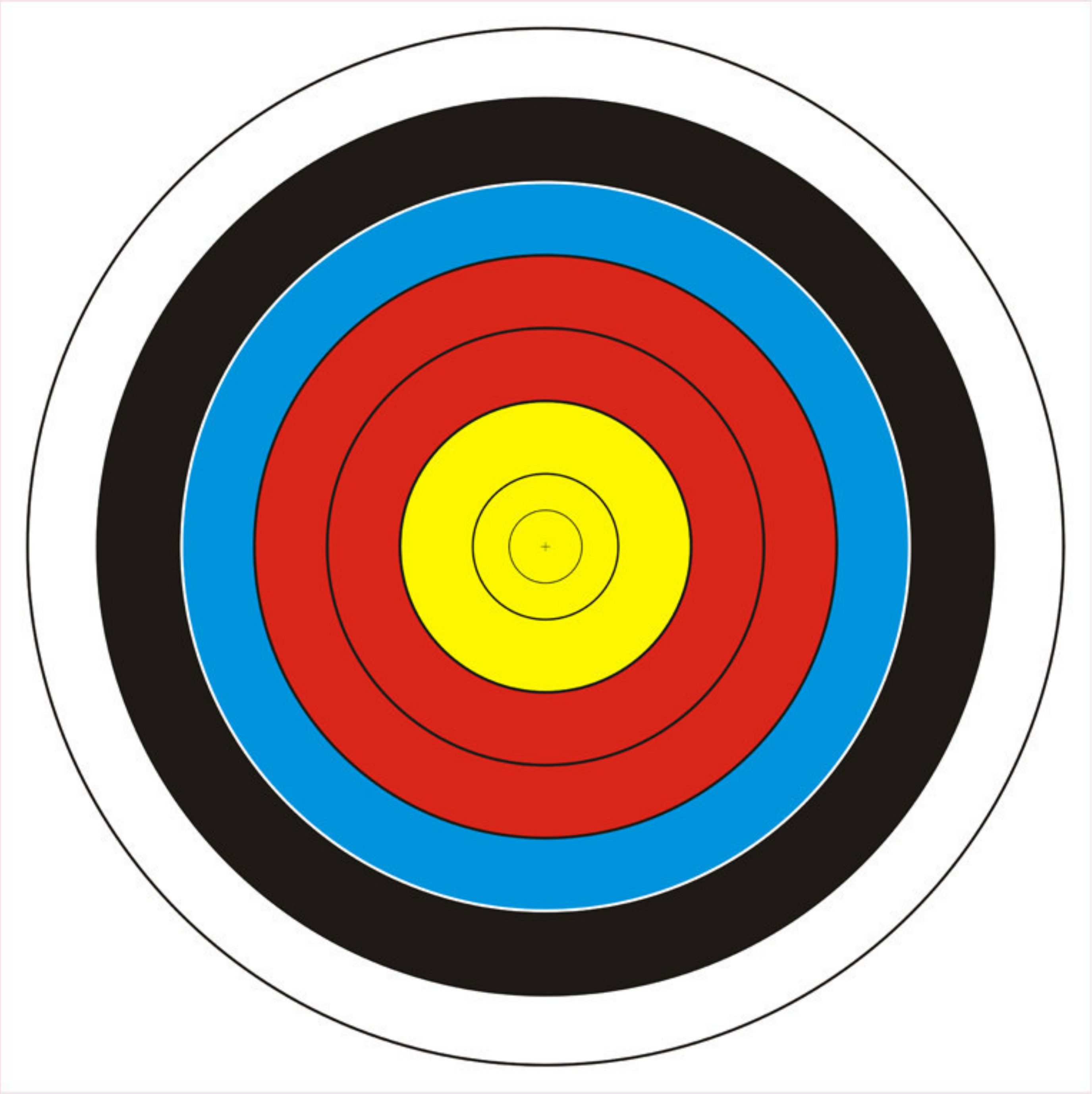
Regulatory focus on CONFIDENTIALITY

BUT

INTEGRITY and AVAILABILITY are actually MORE important

Healthcare is being targeted

- Reported ransomware events against healthcare nearly doubled in 2020 Q3 (USA Today)
- Healthcare providers are typically more desperate to pay ransom to protect PHI and get their systems back up and running (Check Point)
- Healthcare networks typically require the use of older, unsupported software running on medical devices in particular



- UCSF reportedly paid $1.14M to recover their encrypted files in 2021
- UHS, one of the largest healthcare providers, suffered a Ryuk ransomware event, typically precipitated by commodity threats Emotet and Trickbot
- Events are not isolated to North America. India reported the second most ransomware attacks in Q3 2020

Ransomware is now a $6 trillion dollar industry

Between 2 and 3 US hospitals are being attacked by ransomware EVERY WEEK

That results in:

- Hospitals forced on divert
- Cancelation of appointments
- Patient safety concerns
- Loss of revenue
- Loss of reputation
- OCR investigation & fines
- Class Action Lawsuits

Cyber Attacks Against Healthcare Don’t End Well

2021 ransomware attack cost $112.7m in lost revenue

Scripps
DEVELOPING STORY
SCRIPPS HEALTH HIT BY CYBER ATTACK
FOX 5
10:08 | 62°
POSSIBLE HUMAN SMUGGLING OPERATION OFF COAST OF SAN DIEGO, LEAV
HEADLINES

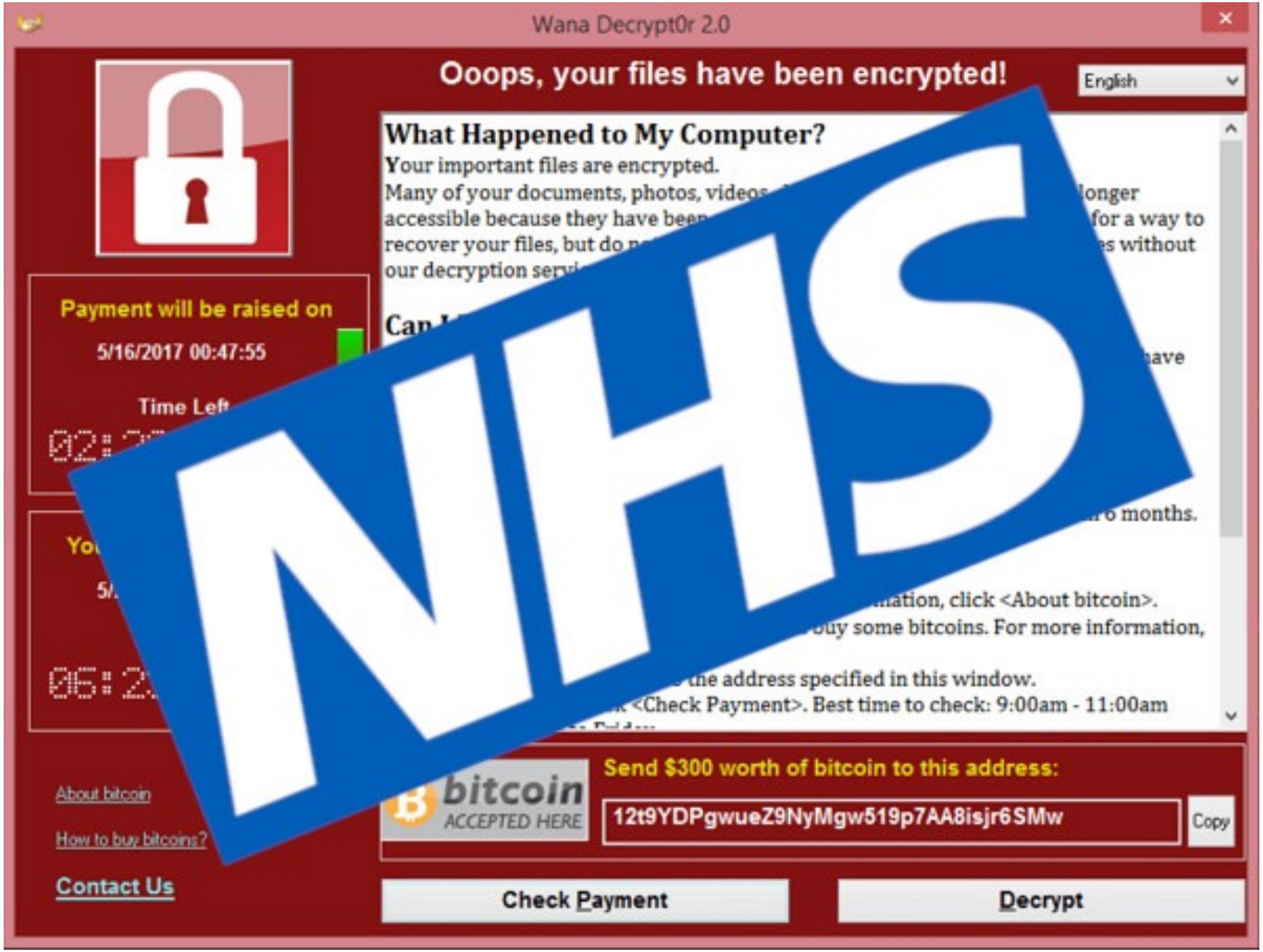
CommonSpirit

Will likely cost more

Irish Health System Executive attacked

THE IRISH TIMES

North Korean WannaCry attack shut down much of the UK NHS in 2017



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos longer
accessible because they have been for a way to
recover your files, but do n s without
our decryption serv

Can I

have

6 months.

ation, click <About bitcoin>.
buy some bitcoins. For more information,

the address specified in this window.
k <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:2

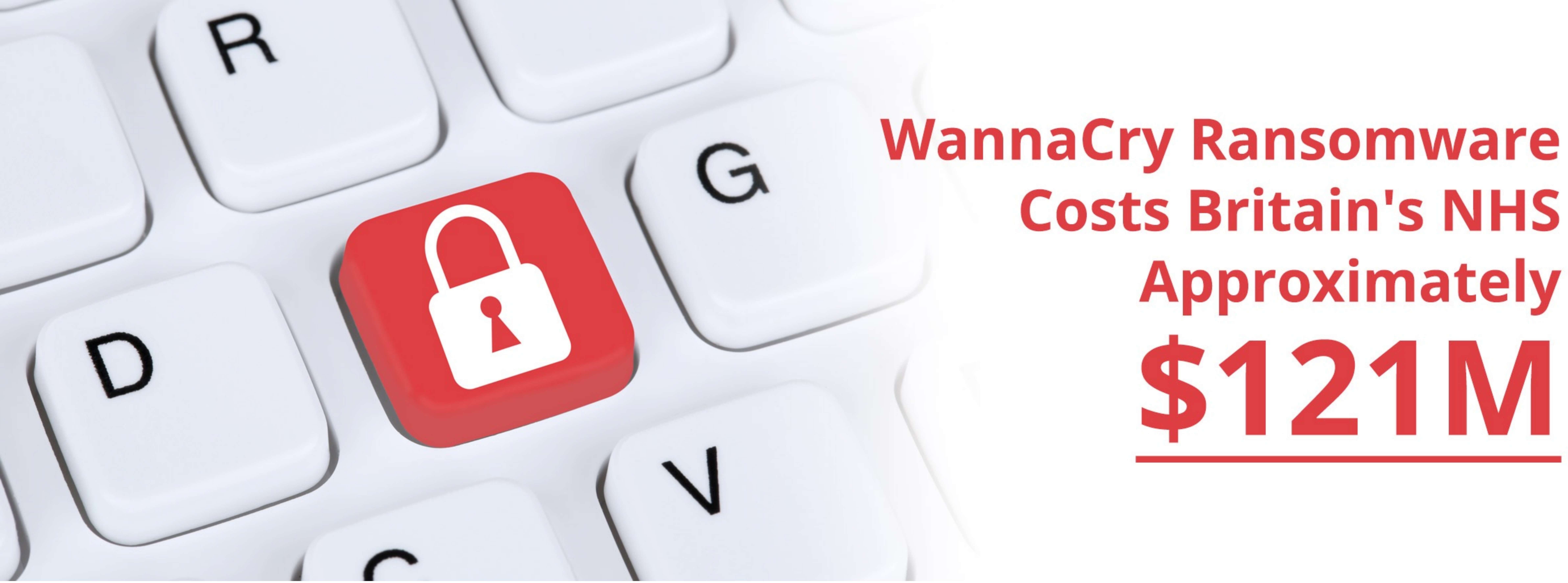
Yo

5/

06:2

Send $300 worth of bitcoin to this address:

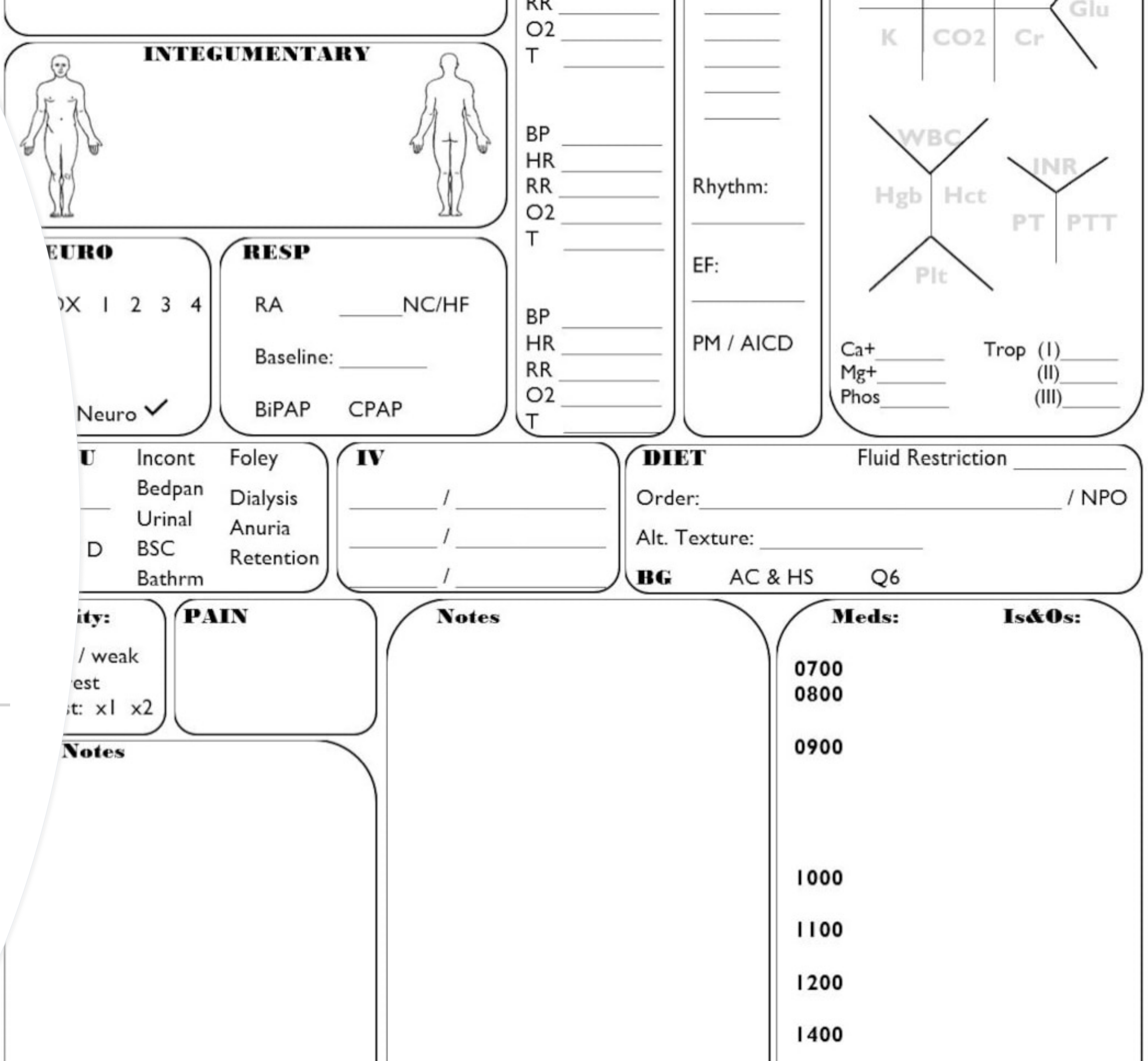
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



5 years later the NHS still has a massive elective surgery backlog

As providers we are now dependent upon technology to diagnose, treat, monitor and manage patients.

In the US few staff under 50 could successfully revert to paper charts when tested



RR ______
O2 ______
T ______

BP ______
HR ______
RR ______
O2 ______
T ______

BP ______
HR ______
RR ______
O2 ______
T ______

______
______
______
______
______

Rhythm:
______

EF:
______

PM / AICD

Glu
K | CO2 | Cr

WBC
Hgb | Hct
Plt

INR
PT | PTT

Ca+ ______
Mg+ ______
Phos ______

Trop (I) ______
(II) ______
(III) ______

INTEGUMENTARY

EURO

X I 2 3 4

Neuro ✓

RESP

RA ______NC/HF

Baseline: ______

BiPAP CPAP

U

______

D

Incont
Bedpan
Urinal
BSC
Bathrm

Foley
Dialysis
Anuria
Retention

IV

______ / ______
______ / ______
______ / ______

DIET Fluid Restriction ______

Order: ______ / NPO

Alt. Texture: ______

BG AC & HS Q6

ity:

/ weak
est
t: x1 x2

PAIN

Notes

Notes

Meds: **Is&Os:**

0700
0800
0900
1000
1100
1200
1400

This places us at risk

Risk that if HIT / HIoT systems go down that patient treatment will suffer.

Failure of IT may also lead to patient safety concerns including increases in morbidity and even mortality.

SIGN IN
SUBSCRIBE

THE WALL STREET JOURNAL.

U.S.

A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death

A lawsuit says computer outages from a cyberattack led staff to miss troubling signs, resulting in the baby’s death, allegations the hospital denies

Death by Ransomware

On the evening of 11 September 2020 paramedics in Düsseldorf, Germany, were alerted to an inbound ambulance and the deteriorating condition of a 78-year-old woman suffering from an aortic aneurysm.

Due to a ransomware attack and rapidly failing IT systems, the hospital was unable to accept the patient who was redirected to another facility 32km away in Wuppertal delaying the patient’s treatment by an hour. The patient died shortly after arrival in Wuppertal.

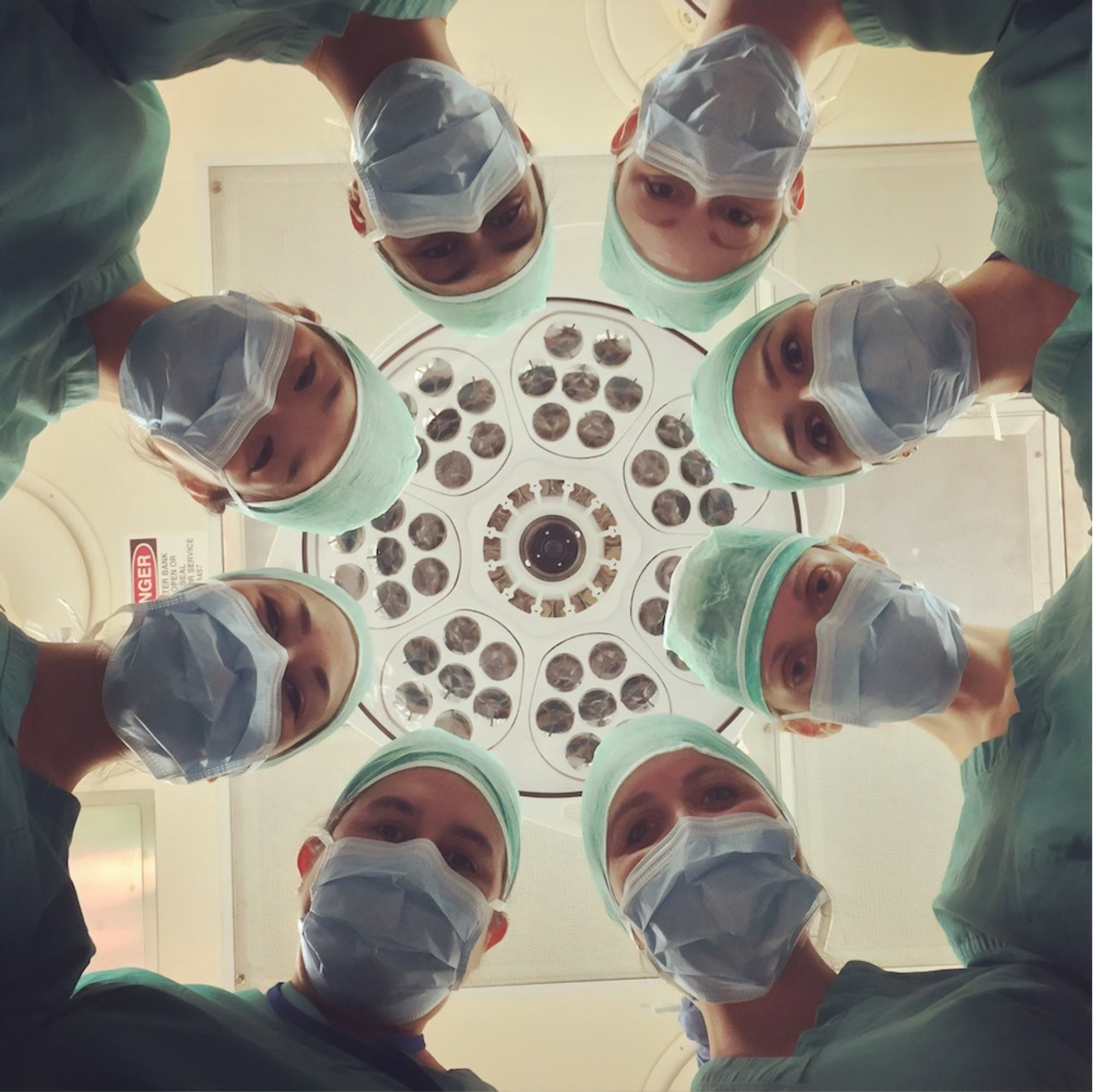
German authorities have yet to extradite the Russian suspects.

Today healthcare operates in a highly technology dependent and interconnected system of medical and other healthcare IoT devices and core health IT systems.

When part of that system fails, treatment rapidly declines.

So, we need to do a better job of protecting healthcare from cyber attack

The industry is undergoing a period of radical change. And with change, comes risk.



We need to do a better job of educating clinicians to look for signs of cybersecurity risk and to identify when a medical device or HIT system is displaying indicators of compromise (IoCs).

https://www.cyberthoughts.org/2018/04/hacking-healthcare-live-bits-and-bytes.html

We need to understand what IT and HIoT devices connect to healthcare networks and what risks each of those devices poses to the medical network.

We need automation and orchestration to remediate those risks.

With adequate and effective cybersecurity healthcare can expand into new cutting-edge high-risk technologies like personalized medicine using a patient’s DNA

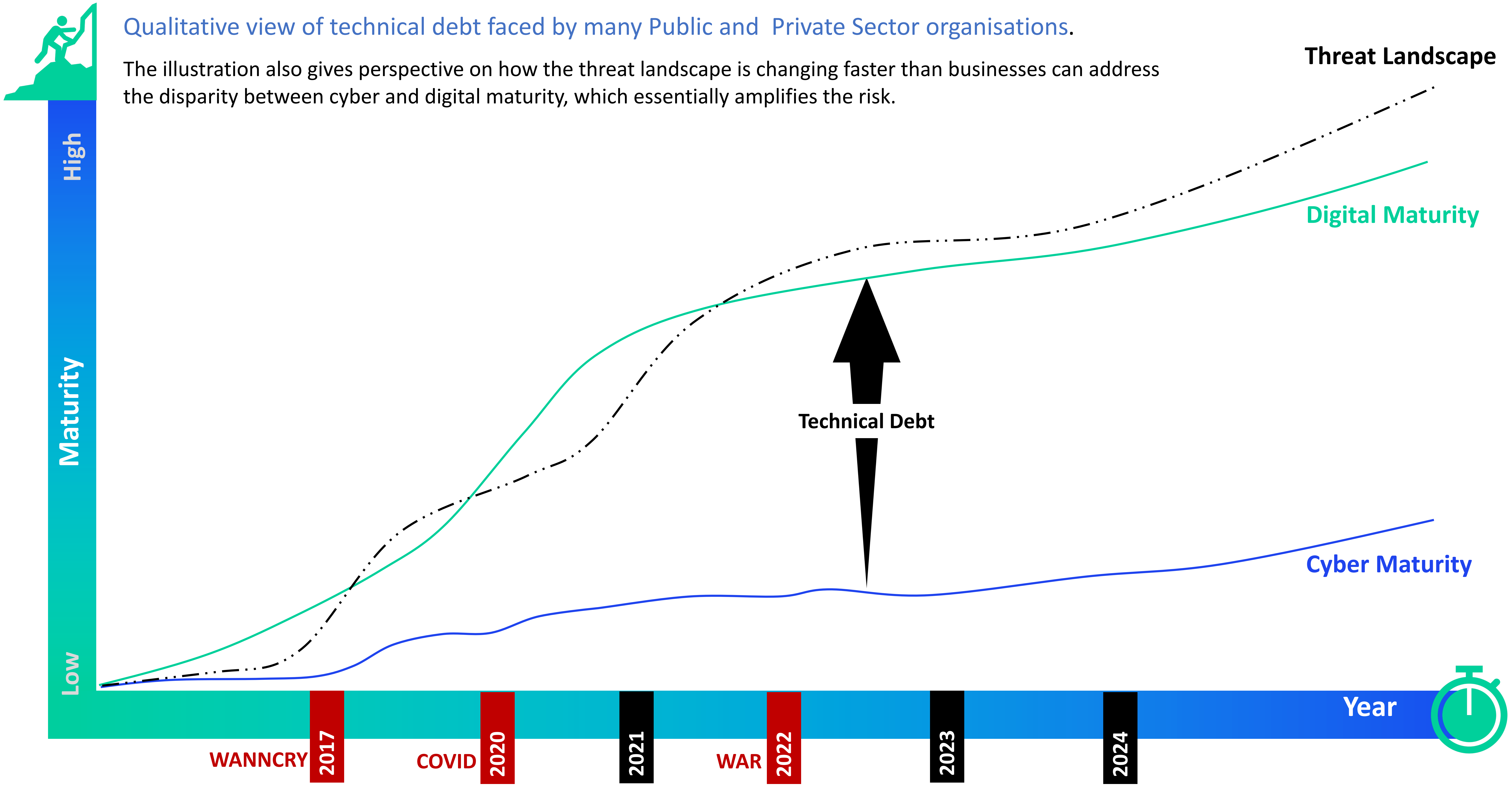
But Clinical and Security staff need to work together to solve medical and cybersecurity risks.

Security needs to be integral to medical solutions not a strap-on after the fact.

Maturity Paradox

Qualitative view of technical debt faced by many Public and Private Sector organisations.

The illustration also gives perspective on how the threat landscape is changing faster than businesses can address the disparity between cyber and digital maturity, which essentially amplifies the risk.



Security can’t keep up

Cybersecurity is now the major driver of Patient Safety

… and you can’t insure against patient loss!

But Improved Cybersecurity needs to be a Priority and right now it isn’t

A culture of ‘Security-First’ needs to permeate all healthcare organizations to manage down enterprise risks

Security is the enabler of new safe medical services

But it needs a different approach and better tools to defend against rising attacks

We need better AI-based tools to identify risks, and automatically remediate them because quite frankly, Healthcare Security Leaders have more important things to deal with!

Questions

@rstaynings

richardstaynings

Richard Staynings

Chief Security Strategist, Cylera

https://cyberthoughts.org/

https://cylera.com

CYLERA

A copy of this deck can be downloaded from
https://pubs.cyberthoughts.org/2022.11.07-Cybersecurity.pdf

UNIVERSITY OF DENVER