CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT

HIPAA Enforcement and the Pandemic

The View from OCR Industry Experts

November 18, 2020

Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

Webinar Logistics

1. Slide materials – Link In Chat Box

   (Should have also received in reminder email earlier today)

2. All attendees are in “Listen Only Mode”
3. Please ask content related questions in **“Q&A”**
4. In case of technical issues, use / check **“Chat”**
5. **Please participate in all polls**
6. Please complete Exit Survey when you leave our session
7. Recorded version, final slides, and Certificate of Attendance will be shared with you within 48 hours

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Introduction to Clearwater

- Leading provider of cyber risk management and HIPAA compliance software and solutions for healthcare
- 100% success rate when deliverables submitted to the Office For Civil Rights (OCR)
- Founded in Nashville in 2009, colleagues in 20+ states, growing rapidly
- Portfolio company of Altaris Capital Partners, a healthcare PE firm with $4.8B under management
- Approximately 400 customers, including 68 IDNs, many with multi-year enterprise programs

BLACK BOOK 2017 · BLACK BOOK 2018 · BLACK BOOK 2019 · BEST IN KLAS CYBERSECURITY ADVISORY SERVICES 2018

Your Presenters:

Jon Moore, *MS, JD, HCISPP*

Chief Risk Officer & SVP, Consulting Services

- 25+ Years Executive Leadership, Technology Consulting and Law
- 14+ Years Data Privacy & Security
- 10+ Years Healthcare
- Former PwC Federal Healthcare Leadership Team
- Former IT Operational Leader PwC Federal Practice
- BA Economics Haverford College, MS E-Commerce Carnegie Mellon University, JD Dickinson Law Penn State University, HCISPP
- Speaker and Published Author on Security, Privacy, IT Strategy and Impact of Emerging Technologies

Your Presenters:

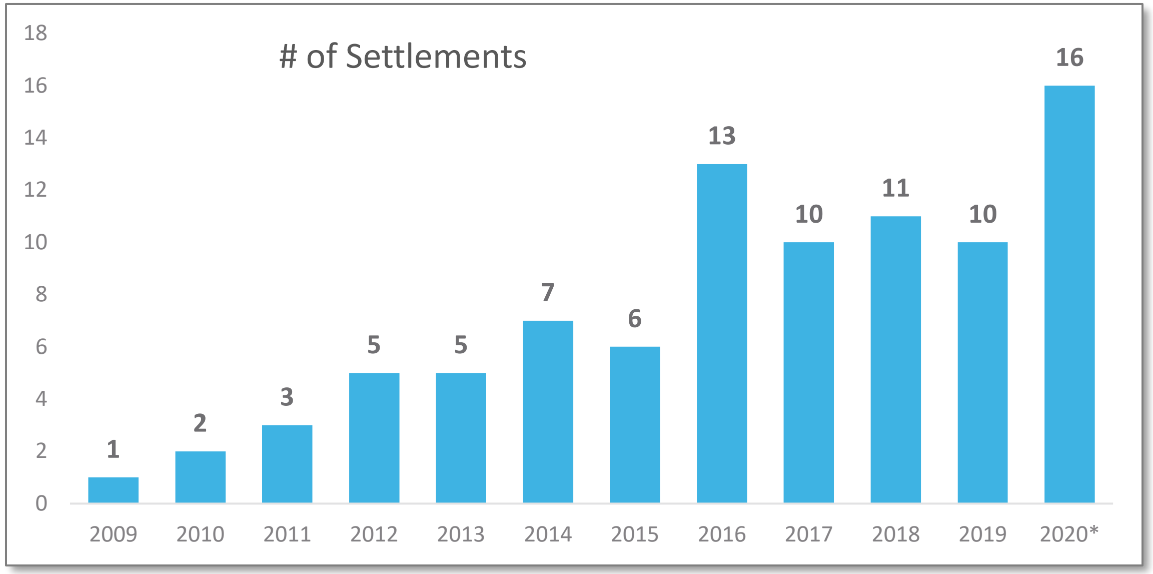
Iliana Peters, JD, LLM, CISSP

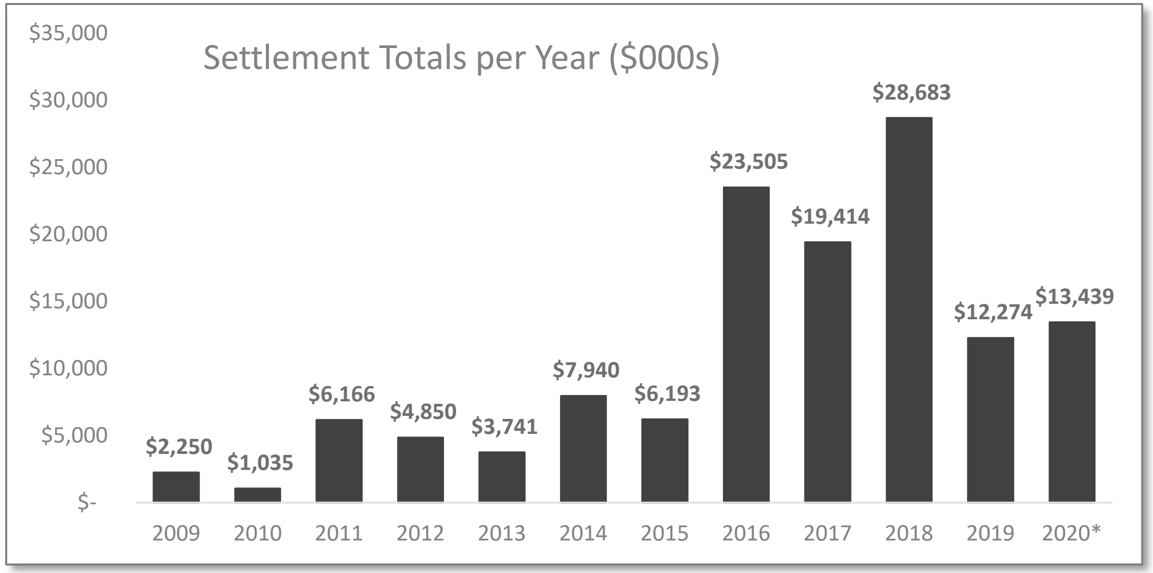
Shareholder, Polsinelli PC, Former Acting Deputy Director HHS Office for Civil Rights

- Recognized by the healthcare industry as a preeminent thought leader and speaker on data privacy and security, particularly regarding HIPAA, the HITECH Act, the 21st Century Cures Act, the Genetic Information Nondiscrimination Act (GINA), the Privacy Act, and emerging cyber threats to health data
- For over a decade, she both developed health information privacy and security policy, including on emerging technologies and cyber threats, for the Department of Health and Human Services, and enforced HIPAA regulations through spearheading multi-million dollar settlement agreements and civil money penalties pursuant to HIPAA.
- Member: ABA, AHLA, ISC2, Hispanic National Bar Association

Enforcement Actions Hit a New Record Number

At end of July 2020 only three announced settlements for the year. Now we are at 17 a new record.





11 Cases in HIPAA Right of Access Initiative

On November 12th OCR announced settlement of its 11th HIPAA Right of Access Initiative enforcement action. The HIPAA Right of Access Initiative was announced as an enforcement priority in 2019 to support individuals' right to timely access to their health records at a reasonable cost.

RIVERSIDE PSYCHIATRIC MEDICAL GROUP

HOUSING WORKS

WISE PSYCHIATRY

Patricia King MD & Associates

Dignity Health

nyspinemedicine
SCHOTTENSTEIN PAIN & NEURO

AIMS
All Inclusive Medical Services

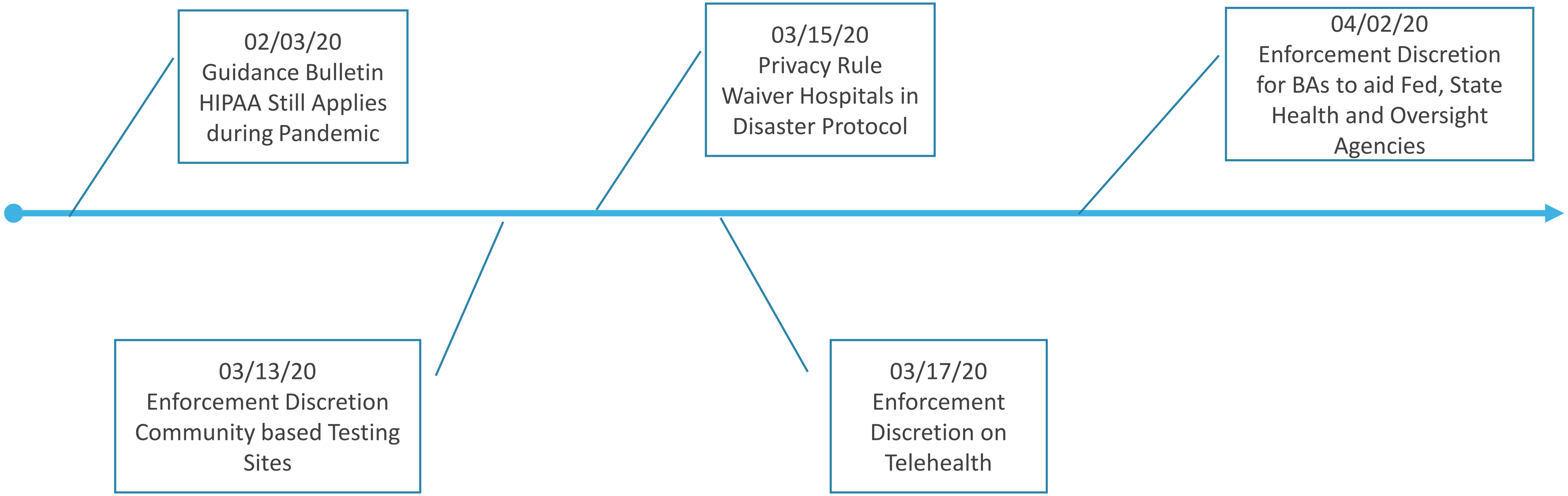
Beth Israel Lahey Health

Dr. Rajendra Bhayani

*These cases only involve 1 patient.

Waivers and Enforcement Discretion

OCR Announcements during COVID Pandemic



02/03/20
Guidance Bulletin
HIPAA Still Applies during Pandemic

03/13/20
Enforcement Discretion
Community based Testing Sites

03/15/20
Privacy Rule
Waiver Hospitals in Disaster Protocol

03/17/20
Enforcement Discretion on Telehealth

04/02/20
Enforcement Discretion for BAs to aid Fed, State Health and Oversight Agencies

Risk Analysis an Ongoing Problem

Asked to characterize the state of HIPAA compliance generally, Severino lamented a laundry list of lapses involving some of the law's most elementary privacy provisions. "For enforcement purposes, there's **still a lot of low-hanging fruit**," the OCR director said. "There are a lot of entities that are **not doing the basic steps** to make sure they have proper, for example, **cybersecurity protections** in place. . . – February 2020

88%

of ePHI-related cases failed to conduct an OCR-Quality Risk Analysis

{ Not detailed or comprehensive enough
Not following OCR/NIST guidance
Not enough documentation/evidence }

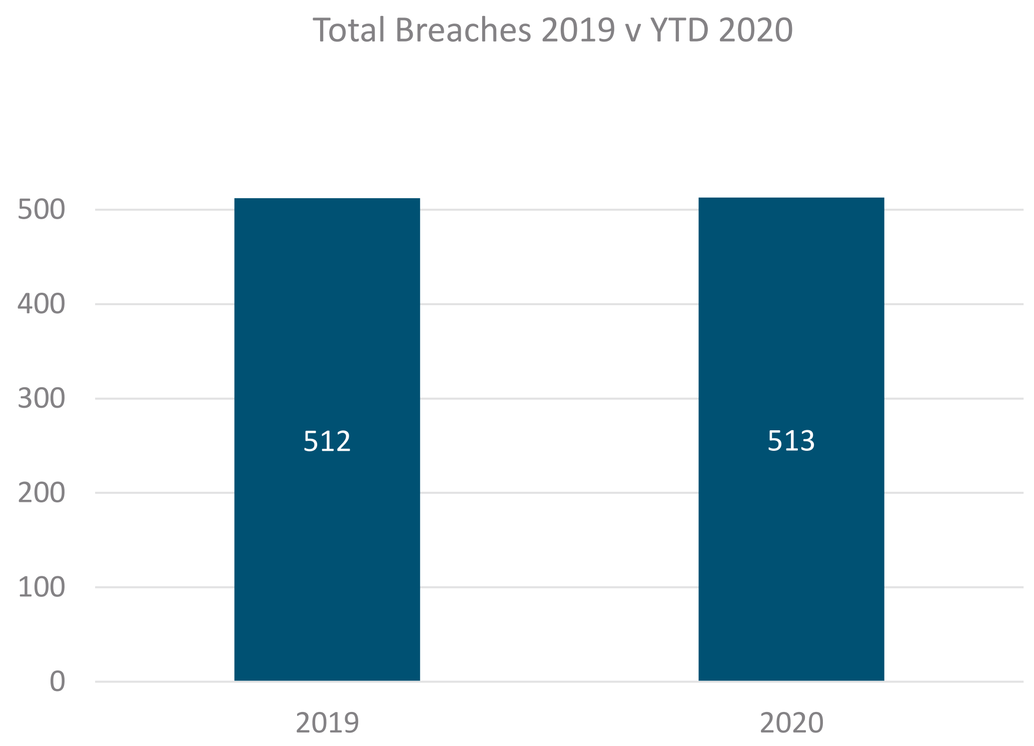
https://digital.mwe.com/27/7458/landing-pages/hipaa-boss-sees--low-hanging-fruit--ripe-for-enforcement---law360.pdf

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Increases in Breaches

The number of breaches of 500 records or more reported to OCR has now surpassed last years total with a month and a half to go in the year.

Year over year we are 13.5% ahead of last year.

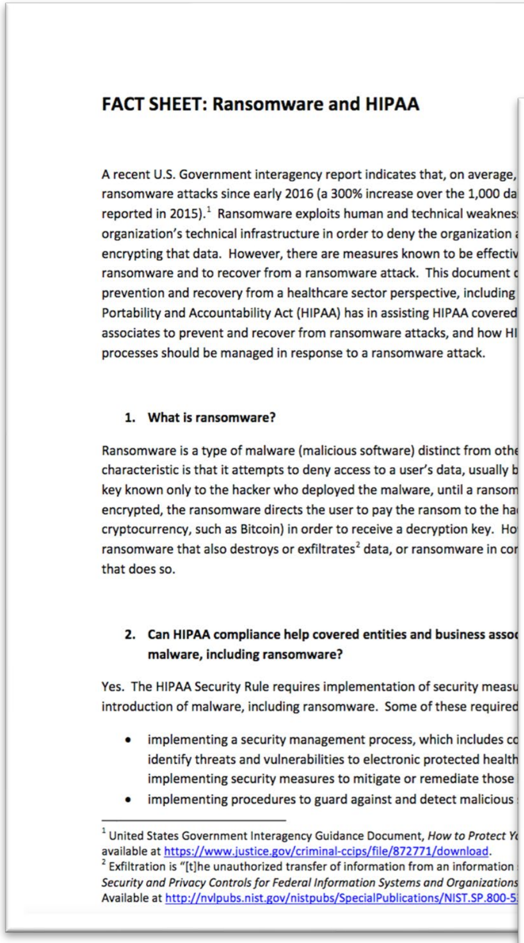


Risk Assessment Following Ransomware Attack

A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402

To demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach, a risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)) must be conducted:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.



FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average,
ransomware attacks since early 2016 (a 300% increase over the 1,000 da
reported in 2015).[1] Ransomware exploits human and technical weaknes
organization's technical infrastructure in order to deny the organization
encrypting that data. However, there are measures known to be effectiv
ransomware and to recover from a ransomware attack. This document
prevention and recovery from a healthcare sector perspective, including
Portability and Accountability Act (HIPAA) has in assisting HIPAA covered
associates to prevent and recover from ransomware attacks, and how HI
processes should be managed in response to a ransomware attack.

1. **What is ransomware?**

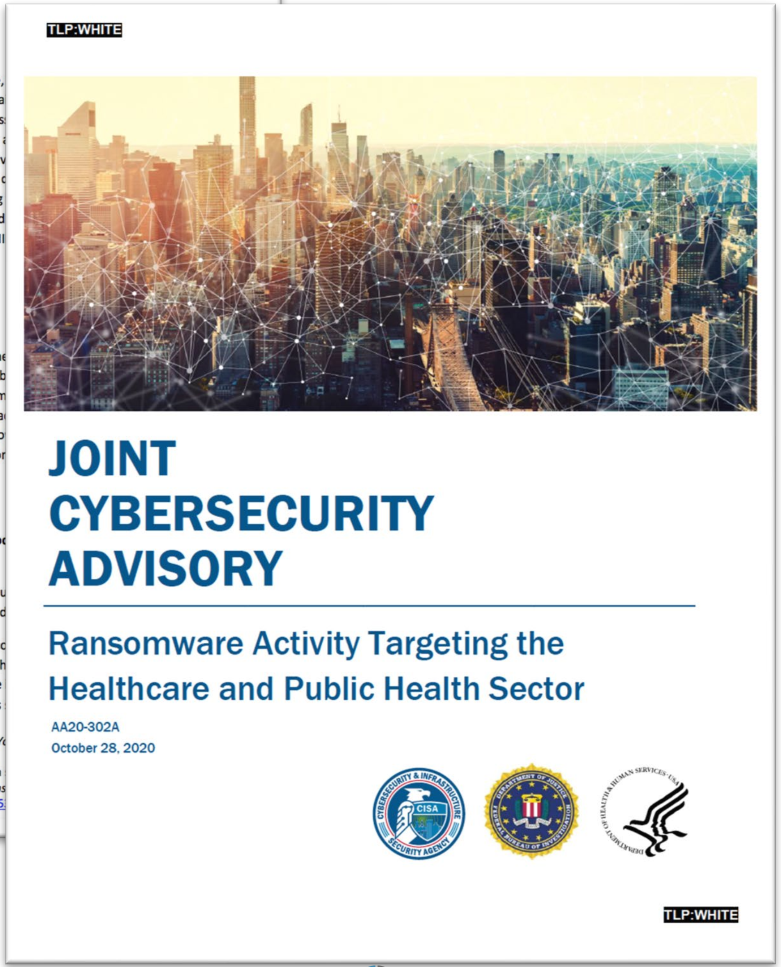
Ransomware is a type of malware (malicious software) distinct from othe
characteristic is that it attempts to deny access to a user's data, usually b
key known only to the hacker who deployed the malware, until a ransom
encrypted, the ransomware directs the user to pay the ransom to the ha
cryptocurrency, such as Bitcoin) in order to receive a decryption key. Ho
ransomware that also destroys or exfiltrates[2] data, or ransomware in cor
that does so.

2. **Can HIPAA compliance help covered entities and business assoc**
   malware, including ransomware?

Yes. The HIPAA Security Rule requires implementation of security measu
introduction of malware, including ransomware. Some of these required

- implementing a security management process, which includes co
  identify threats and vulnerabilities to electronic protected health
  implementing security measures to mitigate or remediate those
- implementing procedures to guard against and detect malicious

[1] United States Government Interagency Guidance Document, *How to Protect Yo*
available at https://www.justice.gov/criminal-ccips/file/872771/download.
[2] Exfiltration is "[t]he unauthorized transfer of information from an information
Security and Privacy Controls for Federal Information Systems and Organizations
Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-5



TLP:WHITE

JOINT CYBERSECURITY ADVISORY

Ransomware Activity Targeting the Healthcare and Public Health Sector

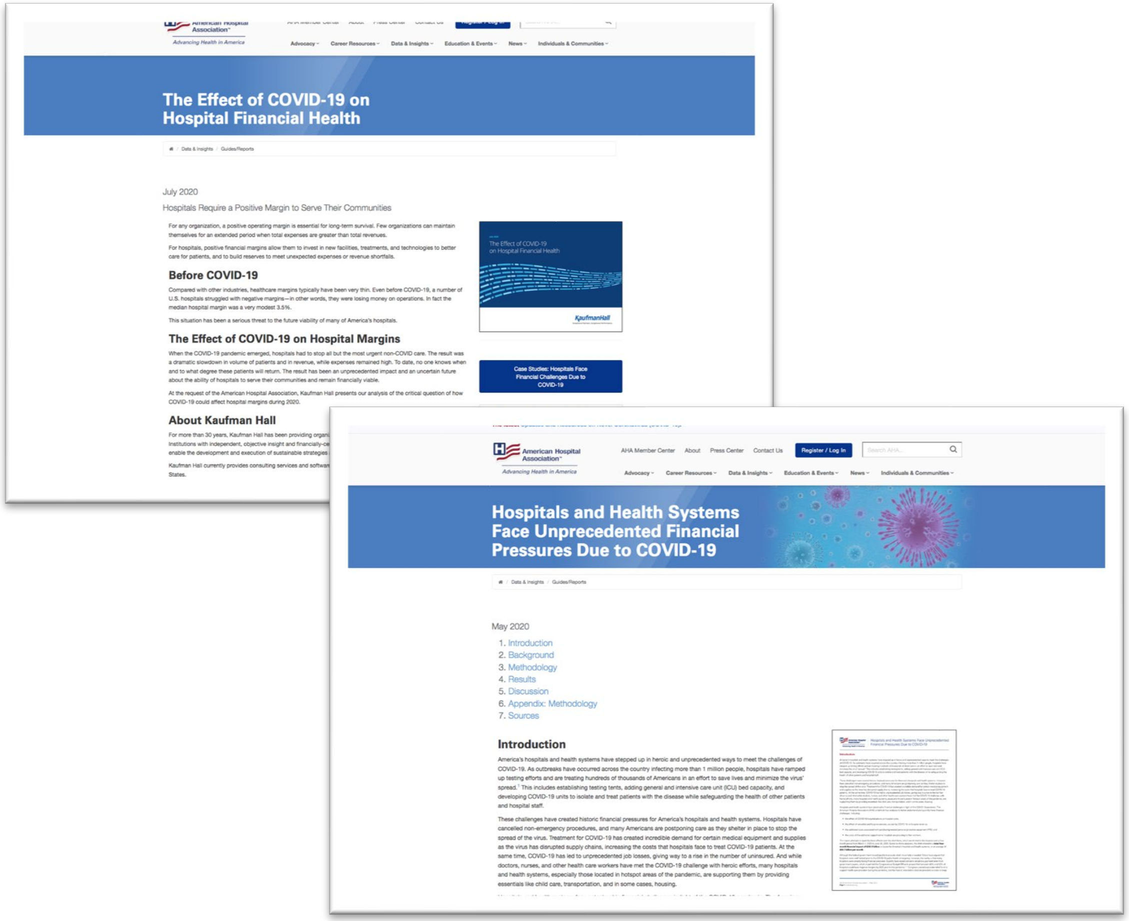
AA20-302A
October 28, 2020

TLP:WHITE

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Pandemics Financial Impact and Compliance

The Pandemic and resulting shut down of elective procedures has resulted in many provider organizations experiencing significant financial impact. The AHA estimates a **total four-month financial impact of $202.6 billion** in losses for America's hospitals and health systems, or an average **of $50.7 billion per month.**


American Hospital Association
Advancing Health in America
AHA Member Center
About
Press Center
Contact Us
Register / Log In
Search AHA...
Advocacy
Career Resources
Data & Insights
Education & Events
News
Individuals & Communities
Data & Insights / Guides/Reports
The Effect of COVID-19 on Hospital Financial Health
KaufmanHall
Case Studies: Hospitals Face Financial Challenges Due to COVID-19

The Effect of COVID-19 on Hospital Financial Health

July 2020

Hospitals Require a Positive Margin to Serve Their Communities

For any organization, a positive operating margin is essential for long-term survival. Few organizations can maintain themselves for an extended period when total expenses are greater than total revenues.

For hospitals, positive financial margins allow them to invest in new facilities, treatments, and technologies to better care for patients, and to build reserves to meet unexpected expenses or revenue shortfalls.

Before COVID-19

Compared with other industries, healthcare margins typically have been very thin. Even before COVID-19, a number of U.S. hospitals struggled with negative margins—in other words, they were losing money on operations. In fact the median hospital margin was a very modest 3.5%.

This situation has been a serious threat to the future viability of many of America's hospitals.

The Effect of COVID-19 on Hospital Margins

When the COVID-19 pandemic emerged, hospitals had to stop all but the most urgent non-COVID care. The result was a dramatic slowdown in volume of patients and in revenue, while expenses remained high. To date, no one knows when and to what degree these patients will return. The result has been an unprecedented impact and an uncertain future about the ability of hospitals to serve their communities and remain financially viable.

At the request of the American Hospital Association, Kaufman Hall presents our analysis of the critical question of how COVID-19 could affect hospital margins during 2020.

About Kaufman Hall

For more than 30 years, Kaufman Hall has been providing organi
institutions with independent, objective insight and financially-ce
enable the development and execution of sustainable strategies

Kaufman Hall currently provides consulting services and softwar
States.

Hospitals and Health Systems Face Unprecedented Financial Pressures Due to COVID-19

May 2020

1. Introduction
2. Background
3. Methodology
4. Results
5. Discussion
6. Appendix: Methodology
7. Sources

Introduction

America's hospitals and health systems have stepped up in heroic and unprecedented ways to meet the challenges of COVID-19. As outbreaks have occurred across the country infecting more than 1 million people, hospitals have ramped up testing efforts and are treating hundreds of thousands of Americans in an effort to save lives and minimize the virus' spread.[1] This includes establishing testing tents, adding general and intensive care unit (ICU) bed capacity, and developing COVID-19 units to isolate and treat patients with the disease while safeguarding the health of other patients and hospital staff.

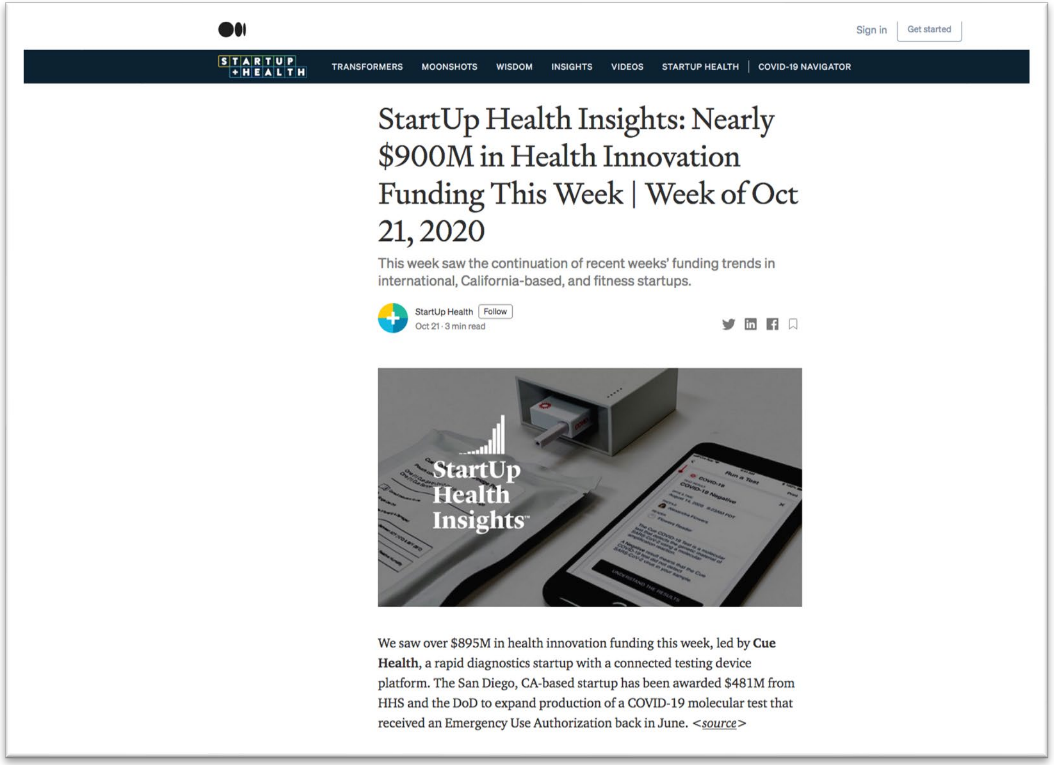
These challenges have created historic financial pressures for America's hospitals and health systems. Hospitals have cancelled non-emergency procedures, and many Americans are postponing care as they shelter in place to stop the spread of the virus. Treatment for COVID-19 has created incredible demand for certain medical equipment and supplies as the virus has disrupted supply chains, increasing the costs that hospitals face to treat COVID-19 patients. At the same time, COVID-19 has led to unprecedented job losses, giving way to a rise in the number of uninsured. And while doctors, nurses, and other health care workers have met the COVID-19 challenge with heroic efforts, many hospitals and health systems, especially those located in hotspot areas of the pandemic, are supporting them by providing essentials like child care, transportation, and in some cases, housing.

https://www.aha.org/guidesreports/2020-05-05-hospitals-and-health-systems-face-unprecedented-financial-pressures-due

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Exploding Investment in Healthcare IT

Despite, or perhaps because of, the Pandemic there has been increasing investment in healthcare IT. This included almost $900M during the week of October 21, 2020.



StartUp Health Insights: Nearly $900M in Health Innovation Funding This Week | Week of Oct 21, 2020

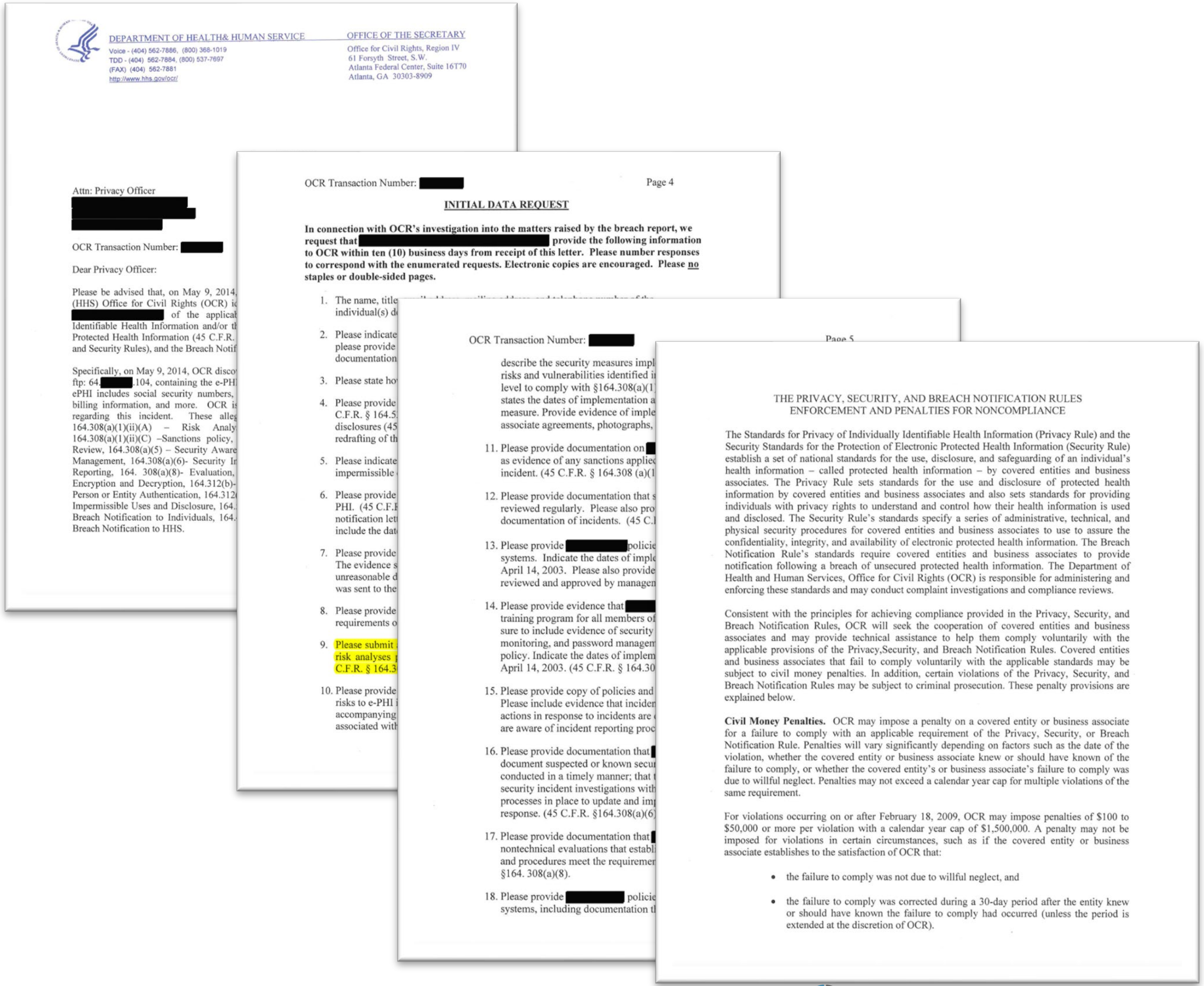
This week saw the continuation of recent weeks' funding trends in international, California-based, and fitness startups.

StartUp Health Follow
Oct 21 · 3 min read

We saw over $895M in health innovation funding this week, led by **Cue Health**, a rapid diagnostics startup with a connected testing device platform. The San Diego, CA-based startup has been awarded $481M from HHS and the DoD to expand production of a COVID-19 molecular test that received an Emergency Use Authorization back in June. <*source*>

Letters from OCR

If OCR continues its practice of sending a letter to inquiry to every organization reporting a breach of 500 records or more, there will be more organizations receiving letters from OCR than ever before.



DEPARTMENT OF HEALTH& HUMAN SERVICE
Voice - (404) 562-7886, (800) 368-1019
TDD - (404) 562-7884, (800) 537-7697
(FAX) (404) 562-7881
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region IV
61 Forsyth Street, S.W.
Atlanta Federal Center, Suite 16T70
Atlanta, GA 30303-8909

Attn: Privacy Officer
[redacted]

OCR Transaction Number: [redacted]

Dear Privacy Officer:

Please be advised that, on May 9, 2014,
(HHS) Office for Civil Rights (OCR) i
[redacted] of the applicab
Identifiable Health Information and/or th
Protected Health Information (45 C.F.R.
and Security Rules), and the Breach Notif

Specifically, on May 9, 2014, OCR disco
ftp: 64.[redacted].104, containing the e-PH
ePHI includes social security numbers,
billing information, and more. OCR is
regarding this incident. These alleg
164.308(a)(1)(ii)(A) – Risk Analy
164.308(a)(1)(ii)(C) –Sanctions policy,
Review, 164.308(a)(5) – Security Aware
Management, 164.308(a)(6)- Security In
Reporting, 164. 308(a)(8)- Evaluation,
Encryption and Decryption, 164.312(b)-
Person or Entity Authentication, 164.312
Impermissible Uses and Disclosure, 164.
Breach Notification to Individuals, 164.
Breach Notification to HHS.

OCR Transaction Number: [redacted] Page 4

INITIAL DATA REQUEST

In connection with OCR's investigation into the matters raised by the breach report, we request that [redacted] provide the following information to OCR within ten (10) business days from receipt of this letter. Please number responses to correspond with the enumerated requests. Electronic copies are encouraged. Please no staples or double-sided pages.

1. The name, title
individual(s) d
2. Please indicate
please provide
documentation
3. Please state ho
4. Please provide
C.F.R. § 164.5
disclosures (45
redrafting of th
5. Please indicate
impermissible
6. Please provide
PHI. (45 C.F.
notification let
include the dat
7. Please provide
The evidence s
unreasonable d
was sent to the
8. Please provide
requirements o
9. Please submit
risk analyses
C.F.R. § 164.3
10. Please provide
risks to e-PHI
accompanying
associated wit

OCR Transaction Number: [redacted] Page 5

describe the security measures impl
risks and vulnerabilities identified i
level to comply with §164.308(a)(1
states the dates of implementation a
measure. Provide evidence of imple
associate agreements, photographs,

11. Please provide documentation on [redacted]
as evidence of any sanctions applied
incident. (45 C.F.R. § 164.308 (a)(1
12. Please provide documentation that s
reviewed regularly. Please also pro
documentation of incidents. (45 C.
13. Please provide [redacted] policie
systems. Indicate the dates of imple
April 14, 2003. Please also provide
reviewed and approved by managem
14. Please provide evidence that [redacted]
training program for all members of
sure to include evidence of security
monitoring, and password managem
policy. Indicate the dates of implem
April 14, 2003. (45 C.F.R. § 164.30
15. Please provide copy of policies and
Please include evidence that inciden
actions in response to incidents are
are aware of incident reporting proc
16. Please provide documentation that [redacted]
document suspected or known secu
conducted in a timely manner; that
security incident investigations with
processes in place to update and im
response. (45 C.F.R. §164.308(a)(6)
17. Please provide documentation that [redacted]
nontechnical evaluations that establ
and procedures meet the requiremen
§164. 308(a)(8).
18. Please provide [redacted] policie
systems, including documentation t

THE PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES
ENFORCEMENT AND PENALTIES FOR NONCOMPLIANCE

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) and the Security Standards for the Protection of Electronic Protected Health Information (Security Rule) establish a set of national standards for the use, disclosure, and safeguarding of an individual's health information – called protected health information – by covered entities and business associates. The Privacy Rule sets standards for the use and disclosure of protected health information by covered entities and business associates and also sets standards for providing individuals with privacy rights to understand and control how their health information is used and disclosed. The Security Rule's standards specify a series of administrative, technical, and physical security procedures for covered entities and business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information. The Breach Notification Rule's standards require covered entities and business associates to provide notification following a breach of unsecured protected health information. The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews.

Consistent with the principles for achieving compliance provided in the Privacy, Security, and Breach Notification Rules, OCR will seek the cooperation of covered entities and business associates and may provide technical assistance to help them comply voluntarily with the applicable provisions of the Privacy,Security, and Breach Notification Rules. Covered entities and business associates that fail to comply voluntarily with the applicable standards may be subject to civil money penalties. In addition, certain violations of the Privacy, Security, and Breach Notification Rules may be subject to criminal prosecution. These penalty provisions are explained below.

Civil Money Penalties. OCR may impose a penalty on a covered entity or business associate for a failure to comply with an applicable requirement of the Privacy, Security, or Breach Notification Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity or business associate knew or should have known of the failure to comply, or whether the covered entity's or business associate's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

For violations occurring on or after February 18, 2009, OCR may impose penalties of $100 to $50,000 or more per violation with a calendar year cap of $1,500,000. A penalty may not be imposed for violations in certain circumstances, such as if the covered entity or business associate establishes to the satisfaction of OCR that:

- the failure to comply was not due to willful neglect, and
- the failure to comply was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR).

Clearwater Insights…

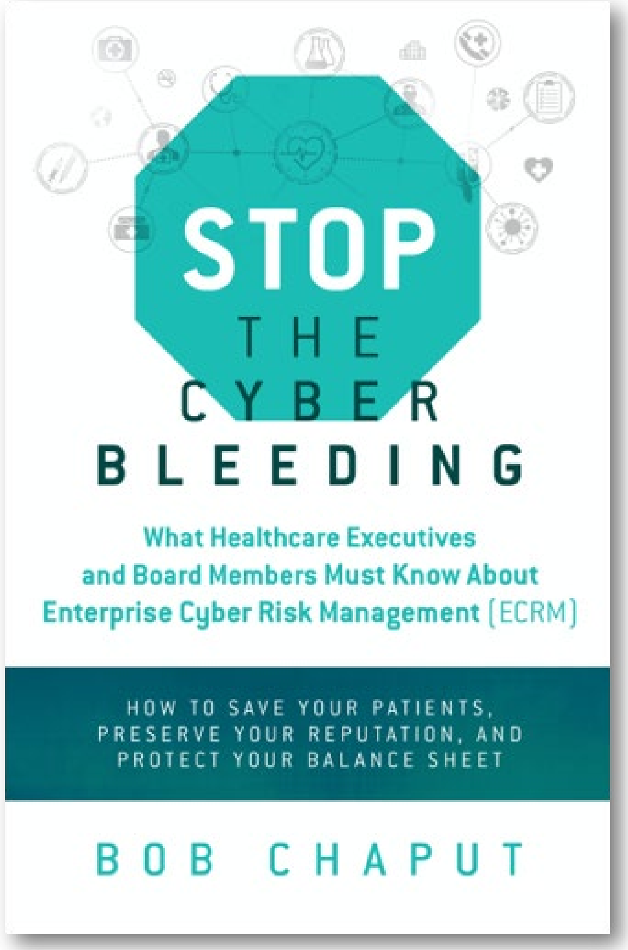
CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

IRM | Analysis®

ENTERPRISE CYBER RISK MANAGEMENT SOFTWARE

GUIDED TOUR
Wednesday, December 9
@11am CT

See how an OCR-Quality® Risk Analysis is done.



STOP THE CYBER BLEEDING

What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)

HOW TO SAVE YOUR PATIENTS, PRESERVE YOUR REPUTATION, AND PROTECT YOUR BALANCE SHEET

BOB CHAPUT

INTERESTED IN A COPY?

https://www.clearwatercompliance.com/stopthecyberbleeding

Learn more and register for these webinars at https://clearwatercompliance.com/upcoming-educational-events/

Thank You & Questions

Jon Moore
Jon.moore@clearwatercompliance.com

Thank you for taking the time to complete the survey when you leave the session. We value and use your feedback!

CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT

www.ClearwaterCompliance.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-compliance-llc/

Twitter | @clearwaterhipaa