KPMG

Healthcare cybersecurity:

Can you meet the challenge?

Over the last decade, technology advances have changed the game for healthcare organizations. The industry's ongoing adoption of consistent data standards has led to an expanded sharing of patient healthcare information. While this cyber evolution has certainly raised the quality and efficiency of healthcare delivery, it comes with a downside: serious security breaches and potential regulatory, reputational and financial risks have expanded.

How has this happened?

To understand the environment, we can start with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which established national standards for the protection of sensitive patient information. Later, the Privacy Rule made "covered entities"— doctors, clinics, hospitals, research centers, and others holding protected health information (PHI)—more responsible for safeguarding PHI and assigned penalties for failure.

HIPAA's goal was to ensure the protection of individuals' health information while allowing the data necessary for high-quality care and public health to be shared. But once information was transmitted over the internet, it became fair game for criminals.

Healthcare under siege

The headlines tell the stories: hospital records held for ransom; patient information sold on the Dark Web; files purloined. What kind of information is compromised? Everything. Names, birthdays, Social Security numbers, phone and address, lab tests, prescriptions, and more.

The fight to protect patient information is not a cops-and-robbers battle. It's more of an ongoing institutional war against a sophisticated army of financial terrorists. And they strike wherever they can. Nearly fifty million Americans were affected by health data breaches in 2022.[1]

Three-quarters of breaches include the human element, either through error or malicious intent, and 83% involve external actors. In cases involving external actors, the motivation for the attack is financial.[2]

In the first six months of 2023, physicians, laboratories, hospitals and medical device developers have paid millions in fines for violating HIPAA provisions.[3] Fines, of course, are only the tip of the iceberg. In February 2023, a hospital in Florida paid $10 million in ransom to regain control of its systems.[4] And six months before that, one of the nation's largest hospital operators suffered a devastating breach that has cost it an estimated $150 million to date.[5] When a breach becomes public knowledge, as it must, the financial, reputational, and legal consequences can be severe.

Many healthcare organizations are aware of the cyber risks they face, and they're not alone. A 2022 KPMG survey[6] of 1880 senior executives, technology heads, and operations directors in large global organizations found that five in six believe that having the technology to protect clients, partners, and customers is important to building trust with those constituencies. But at the same time, over one-third of respondents admitted that concerns over their data protection abilities have undermined stakeholder trust.

1 Southwick, Ron, "Nearly 50 million Americans impacted by health data breaches in 2022," Chief Healthcare Executive, February 15, 2023

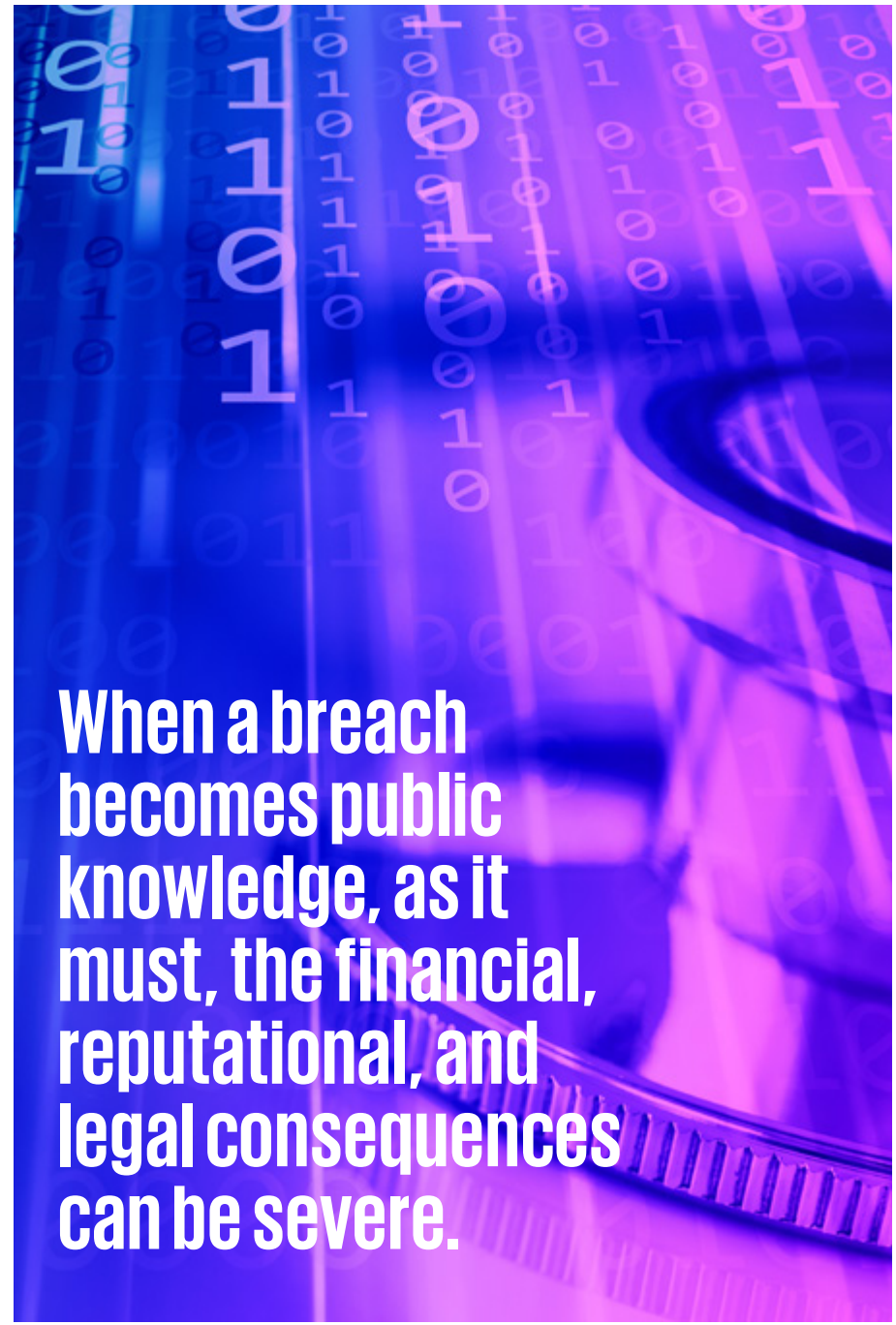
2 Data Breach Investigations Report, Verizon, 2023

3 Lyngaas, Sean and Rind, David, "Apparent cyberattack forces Florida hospital system to divert some emergency patients to other facilities," CNN, February 3, 2023

4 McKeon, Jill, "CommonSpirit Health Ransomware Attack Leads to $150M in Losses to Date," Health IT Security, February 21, 2023

5 The HIPAA Journal, August 23,2023

6 KPMG Cyber Trends, 2022



Third-party danger zone

Perhaps most concerning to companies have been the cyber breaches that were not their fault, but for which they nonetheless bore responsibility.

The risks of third-party cyber infiltration are rising. Today, in fact, there are more data breaches from suppliers and business partners than from within healthcare providers.[7] With serious liability at stake, it's not surprising that companies seek better ways to ensure that they – and those they work with – have a "clean bill of health" in their IT environment. Thus, it behooves every organization in the healthcare industry to not only have appropriate controls in place, but also to promote that fact as a selling point.

Six steps to assess your security posture

1. Understand your regulatory and contractual requirements
2. Determine the controls framework that meets your needs
3. Assess your current environment to identify security gaps
4. Develop and execute a plan to address identified gaps
5. Reassess the post-remediation environment
6. Execute an effective assurance program with third-party assessment

7 The HIPAA Journal, August 23, 2023

Meeting the cybersecurity challenge

The starting point for a cyber assessment is the establishment of a comprehensive security framework and the ability to evaluate it against standards.

It's a challenge, of course, for any company to determine how best to meet its obligations to assess, design, and implement controls related to securing PHI. There are vast gaps in preparedness among organizations. Some have "war rooms" that seek to detect each attempted breach and to isolate any intruders that manage to enter. Others are hacked at the most basic control levels. Where does your organization fit? How can you be sure?

Given the complexities, many turn for assistance to outside firms with expertise in assessing current control environments against regulatory and contractual requirements. These firms can provide readiness assessments as well as remediation support.

Additionally, some, such as KPMG, can provide organizations with attestation services, including SOC 2®, SOC 2® + HITRUST, and HITRUST CSF certification testing. The standards and methodologies of these industry-leading services are accepted throughout the healthcare ecosystem. While they are similar, they are not identical.

SOC 2®, for example, is an attestation examination performed by a service auditor. The objective is to examine and report on an organization's controls relevant to security, availability, processing integrity, confidentiality or privacy. SOC 2® + HITRUST goes further and addresses additional HITRUST criteria.

HITRUST itself is a risk-based information security framework based on numerous authoritative sources used to evaluate a company's security controls, processes and activities based on the HITRUST CSF requirements. An Authorized External Assessor, such as KPMG, must conduct the detailed evaluation and submit the assessment to HITRUST. To receive the HITRUST CSF Certification—a marketable seal of approval that only HITRUST can issue—appropriate controls need to be in place and functioning correctly.

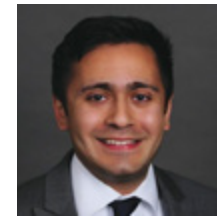
As cyber risks proliferate, the need for cyber assurance grows alongside. Organizations need assurance that the entities they partner with, buy from, and sell to are safe and can be trusted. With attestation services such as SOC 2 and SOC 2 + HITRUST, and third-party assessment service such as HITRUST Certification recognized throughout the industry, it's time to act. No healthcare company can afford to be cyber-insecure.

Contact us

Marc Scher
Partner, National
Healthcare Audit Leader
mscher@kpmg.com
(314) 308-8498

Nicole Romano
Partner,
Technology Assurance, Audit
nicoleromano@kpmg.com
(267) 256-1793

Meghan Kroll
Director,
Technology Assurance, Audit
mkroll1@kpmg.com
(267) 256-5581



Raghav Ahuja
Director,
Technology Assurance, Audit
rahuja@kpmg.com
(703) 286-8000

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates and related entities.