2020 Healthcare Data Breach Report

An Analysis of HHS Breach Reports in 2020

Security Research and Data Analysis

info@ci.security
800 604 4810
https://ci.security

Critical Insight
by CI Security

Table of Contents

OVERVIEW

How Covid-19 has impacted healthcare security

The pandemic has disrupted virtually all industries, but none more than healthcare. The pressure to modify existing operations and to create exceptions to sound security practices in support of a rapidly changing mission has created new attack vectors for cybercriminals. Here are some of the security issues that have been created by or exacerbated by the pandemic.

More employees than ever are working from home and as many as six in 10 are using personal devices to conduct company business.

Employee churn is creating issues with security training, particularly as previously retired or temporary clinicians are brought in to support surge operations.

While telemedicine use has declined somewhat since the early days of the pandemic, many healthcare organizations are still struggling to implement digital health initiatives in a secure manner, particularly when it comes to working with new clinical technology partners as part of new healthcare delivery models.

Early in the pandemic, brand new sites of care were being created on the fly; for example, drive-through testing. Now, as we move to vaccine distribution, patients are being treated at football stadiums, baseball parks, and other locations that are not part of the traditional healthcare system, creating new attack opportunities for cybercriminals.

Many healthcare organizations are challenged with the processes associated with documenting and securing new medical and non-medical equipment that was purchased to fight the pandemic.

Similarly, many healthcare organizations are still working through a backlog of new business associates and other vendors that were fast-tracked to support the demand for personal protective equipment (PPE) and other supplies and services. Organizations need to properly document those new agreements and relationships.

> “...many healthcare organizations are still struggling to implement digital health initiatives in a secure manner...”

Healthcare organizations are also not immune to more generalized attacks, such as the recent SolarWinds attack, in which hackers compromised the SolarWinds application monitoring platform called Orion, and then used that access to infiltrate Fortune 500 companies, the US military, government agencies, colleges, and universities. Many healthcare organizations also use SolarWinds.

Of course, the SolarWinds hack is just one indicator of a larger problem – the volume and frequency of cyberattacks is on the rise. The frequency of daily ransomware attacks increased 50% during the third quarter of 2020, compared to the first half of the year. And healthcare organizations were the No. 1 target of ransomware exploits.

Many healthcare organizations were under enormous financial pressure prior to the pandemic, but the last year has been especially challenging. In this environment, allocating resources to protect patient lives has obviously taken priority over protecting patient records. In fact, 82% of hospital CIOs in inpatient facilities with under 150 beds reported that they are not spending an adequate amount of money on protecting patient records from a data breach.

These factors have combined to put every healthcare organization on edge, particularly small- and mid-sized provider organizations that may lack of the staff and technical expertise to protect themselves. We fear that the situation with regard to protecting patient records will only get worse in 2021, but there are concrete steps that companies can take.

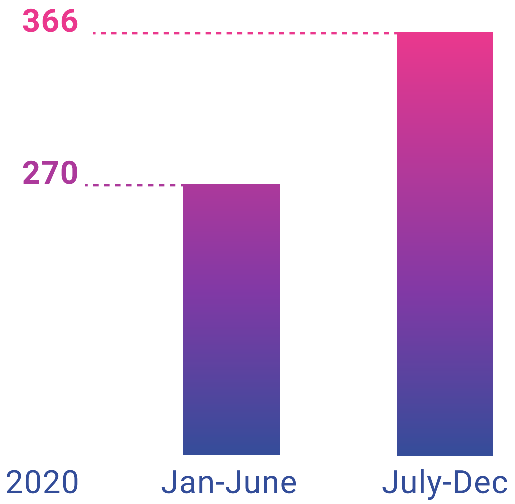
We analyzed data about the reported disclosure of records to get a clearer picture of exactly what breaches are occurring, how they are occurring, and who is being targeted.

Key takeaways from the data

The Covid-19 virus has been unrelenting, and so too are the cybercriminals who have taken advantage of the pandemic to breach healthcare organizations and gain unauthorized access to valuable patient data. There was thought at the beginning of the pandemic that criminals would stop attacking hospitals. Now we know those criminals have no conscience.

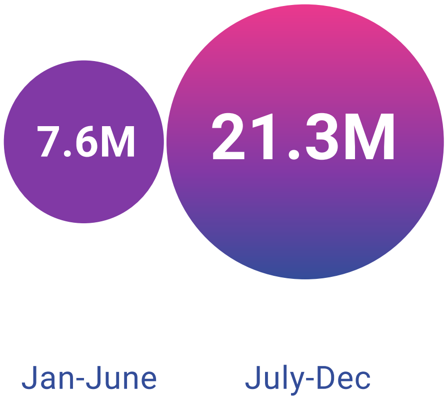
The number of breaches self-reported by healthcare providers to the U.S. Department of Health and Human Services and the total number of patient records accessed by cybercriminals skyrocketed in the second half of 2020, according to an analysis conducted by CI Security. Our mid-2020 report predicted this rise; we hoped we would be wrong.

Breach Reports



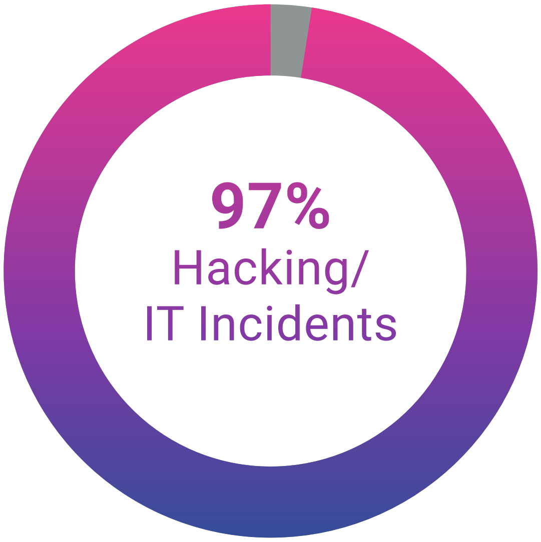
The total number of reported breaches among healthcare organizations increased by 36% from 270 in the first half of 2020 to 366 in the second half of the year.

Records Breached



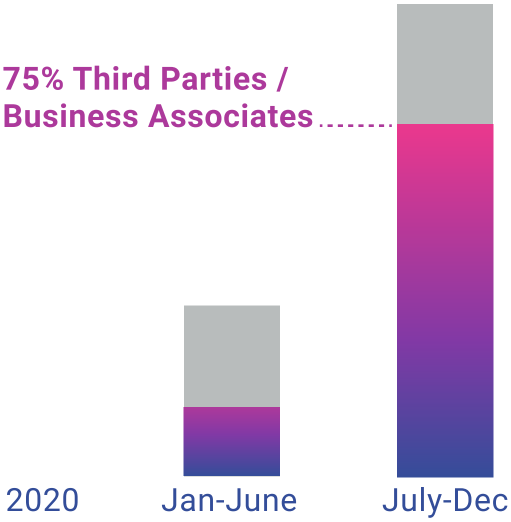
The number of individual patient records that were breached in the second half of 2020 nearly tripled compared to the first half of the year from 7,691,199 to 21,358,070.

Type of Breach



Of the 21.3 million records breached in the second half of 2020, 97% were attributed to malicious hacking incidents, rather than other causes such as unauthorized disclosure, improper disposal, theft, or loss.

Source of Breach



Nearly 75% of all records breached were tied to business associates and other third parties, rather than the healthcare providers, health plans or healthcare clearinghouses. That's up from 46% in the first half of 2020.

The sharp rise in the number of reported breaches over the past six-month period was not unexpected – in fact, we predicted this significant upturn in our 2020 H1 Breach Report, released last July – as we described our concerns over the fact that the number of reported breaches unexpectedly dropped in the first half of 2020 (compared to the second half of 2019) as the pandemic wreaked havoc on the healthcare system.

The most likely explanation was that healthcare providers were so consumed by the sudden onset of the pandemic, and so busy asking for exceptions to their standard security plans in order to respond to rapidly changing Covid-related conditions, they didn't report breaches in a timely manner; or that they were breached, but didn't know it yet.

For example, in two highly publicized breaches – University of Vermont Medicine and Blackbaud -- attackers infiltrated each organization during the first half of 2020, but the breaches were not discovered and reported until later in the year.

Even more alarming, however, is the apparent shift in tactics among cybercriminals, who have evolved their methods to attack the soft underbelly of healthcare networks – third party business associates who provide services such as billing or insurance reimbursement. Or, in the case of Blackbaud, criminals went after fundraising software that stores donor information in the cloud.

Our analysis indicates that the decline in breach reports in the first half of 2020 represents an aberration. The long-term trend lines point to an increase in breaches into 2021 and beyond. However, there are measures that healthcare organizations can take to protect themselves and to make sure that their business associates don't become the weak link in their overall security defenses.

What To Do Right Now

Cybercriminals are focusing on business associates not only because they might be easier to attack than healthcare providers, but also because they have more records to steal, and they might be more financially able to pay ransom demands.

A single breach of a business associate -- one that serves multiple healthcare organizations -- can drive multiple breach reports to HHS, as each client healthcare organization has to report their organization's exposure. Business associates accounted for 75% of all the records exposed in the second half of 2020. The numbers also tell the story of attackers getting more records when they went after business associates in the last part of 2020: There were nearly 7.7 million records breached in the first half of 2020 and more than 21.3 million in the second half of the year, an increase of 177%.

According to data from the HHS Breach Portal, where organizations are required to report incidents that affect 500 or more records, criminals worked all angles of the healthcare system, attacking life science and research labs, rehabilitation facilities, hospital systems and healthcare organizations. Here's what you can do to fight back:

1. **Review every contract:** Healthcare organizations should go back and review every existing contractual agreement with business associates to make sure that financial and other liability responsibilities have been spelled out in the event of a cybersecurity incident or vendor outage. Push hard for language that spells out your need to gain insight into their cybersecurity processes and procedures, including certifications, risk mitigation and incident response plans. Make sure to add language that expands liability in cases where the business associate fails to adhere to their own cybersecurity processes.

> "...organizations need to focus on maturing their cybersecurity program."

2. **Make security a procurement priority:** Before the acquisition of any product or service, make sure that security capabilities are reviewed and let the vendor's cybersecurity program play a primary role in the buying decision. In the best-case scenario, security professionals on your team will research the vendor's capabilities and will be able to provide assurance that the product or service is in compliance with your organization's security plan. Short of that, try to get a list of business and technology risks that are clearly spelled out before the contract is signed. Ask cybersecurity questions early in the process and go into agreements with eyes wide open to the possible risks.

3. Telehealth requires special attention: By its very nature, telehealth implies that data is moving outside of the confines of the hospital or healthcare facility. Organizations should make sure that telehealth agreements define and document where data is stored, how it is protected, and who is responsible for each step in telehealth information management workflows. Particular attention should be paid to digital health agreements that might have been made in haste during the early days of the pandemic. Make sure they are up to the organization's cybersecurity standards.

4. Protect work-from-home environments: With employees working from just about everywhere, organizations need to focus on business operations that are supported by employees using their personal devices at remote locations. Don't assume that employees, in the midst of fighting a pandemic, are focusing on security, or even have the technical expertise to deploy security best practices. Organizations must create and enforce policies, integrate work-from-anywhere into risk management programs, deploy top-notch endpoint protection, and create special training programs because it seems like working from home is here to stay.

5. Take advantage of cloud providers: It's likely that the hyperscale cloud services providers like Amazon and Azure, or SaaS providers like Salesforce or Workday have far better security expertise than many smaller, overworked healthcare IT departments. When considering moving data to the cloud, make sure to verify the security claims of the cloud provider and negotiate liability terms. Also, be sure to involve cybersecurity and risk management professionals; spend time in the planning process, and execute carefully so that the complex process of moving/managing data in the cloud goes out without a hitch. Once the data is in the cloud, you still need to monitor for cyber issues. Data security in the cloud may be an improvement over local security capabilities, but don't assume that it's cybersecurity cure-all.

6. Deploy Identity and Access Management (IAM) software: During the last year, most healthcare organizations quickly on-boarded contract nurses and other staffers to support surge operations. They have also moved team members from one department to another, expanded access to applications and app modules, shared drives and taken other emergency measures – all in the name of getting mission done. Also, many employees have been furloughed because of financial constraints. IAM allows organizations to identify and track human (and other) resources, define what applications and data employees should have the right to access, and allows organizations to better manage moves, adds, changes and dismissals. IAM provides an effective way to make sure that employees only have access to data they need to do their job, which limits the amount of possible exposure should the employee's access be compromised.

7. Re-visit security basics: Now is a great time to double-check that existing policies and procedures are being enforced, and to determine where it makes sense to adopt enhanced security measures. Some places to start include multi-factor authentication rather than simple passwords; encrypting data wherever possible; making sure patches are up to date; testing backups; eliminating employee personal devices on the business network; developing a business continuity plan in consultation with clinical, research and business leaders; and having a clear disaster recovery plan and incident response program. In addition, healthcare organizations that allowed exceptions to security policies during the height of the pandemic need to go back and resolve any lingering issues. Asset management is another critical area; organizations need to know every person, vendor, and piece of equipment, and understand what each has access to.

Look at your security program holistically and evolve it: The data shows that criminals are constantly changing tactics, so there's no single silver bullet (or shield) that will stop attacks. Instead, organizations need to focus on maturing their cybersecurity program. A well-done security risk assessment should identify the needs for improvement, whether it be in protective measures or 24/7/365 managed detection and response. Small and mid-size organizations should especially consider working with outside experts given the fact they often have fewer cybersecurity staff, while having just as many reported hacking incidents as large hospital facilities.

CONCLUSION

You Need a Multi-Tiered Security Program

There is no magic pill that will cure healthcare security pains. Instead, effective protection against breaches requires a multitude of actions. That includes at a minimum, strong contract language with business associates, regular security assessments, penetration tests, powerful 24/7/365 intrusion detection and response capabilities, and a strong incident response plan.

That's the beginning of a holistic and mature cybersecurity and risk management program that your organization (and your patients) can depend on. And for healthcare organizations that might be struggling with the complexity, cost, or skills necessary to keep their name off the HHS "Wall of Shame"- don't be afraid to ask for assistance. There are professional organizations that can help.

OTHER INFORMATION

Disclaimer

This report is for information purposes only. At the time of publication, all information referenced in this report is current and accurate, based on data from the U.S. Department of Health and Human Services Office of Civil Rights Breach Portal ("Wall of Shame") on January 11, 2021.

This report may be changed, improved, or updated without notice.

CI Security is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

Major data breaches which affect the unsecured protected health information (PHI) of 500 or more individuals are required to be reported to HHS within 60 days of the discovery of the breach, as required by section 13402(e)(4) of the HITECH Act.

Reporting parameters: CI Security analysts reviewed Breach Portal data from the last 24 month, focusing on six-month periods:

2019 First-half of the year (2019 H1)

2019 Second-half of the year (2019 H2)

2020 First-half of the year (2020 H1)

2020 Second-half of the year (2020 H2)

OTHER INFORMATION

HHS Breach Portal Overview ("Wall-of-Shame 101")

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of 2009's American Recovery and Reinvestment Act, required covered entities and business associates (under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to provide notifications to Health and Human Services about all breaches of unsecured protected health information (PHI).

The Breach Notification Rule requires reporting of breaches within 60 days of discovery (in addition to other requirements, but we focus only on reporting in this report). All breaches of more than 500 or more individuals are reported via the HHS Breach Portal . Breaches of less than 500 individuals can be reported to HHS on an annual basis; those reports are not shown in the HHS Breach Portal.

The Office of Civil Rights (OCR – the office within HHS that is responsible for administering and enforcing the HIPAA Privacy, Security, and Brach Notification Rules) undertakes investigation and enforcement actions with respect to the reported breaches.

The HITECH Act requires that HHS report to several Senate Committees, on an annual basis, a summary of reported breaches, and the actions taken with respect to those breaches.

The latest report available is for 2015/2016/2017.

Breach Reports, submitted through the HHS Breach Portal site, contain several data elements, and these elements were the primary sources used for the generation of this report:

Type of Breach:
Hacking/IT Incident
Unauthorized Access/Disclosure
Theft
Loss
Improper Disposal

Types of Covered Entity:
Health Plan
Healthcare Clearinghouse
Healthcare Provider
Business Associate

Location of Breach:
Desktop Computer
Electronic Medical Record
Email
Laptop
Network server
Other portable electronic device
Paper/Films
Other

Contributors

Drex DeFord, CI Security's Healthcare Strategist

Vivian Zhou, CI Security's Healthcare Program Manager

Mike Hamilton, CI Security's Chief Information Security Officer & Co-Founder

Fred Langston, CI Security's Executive VP of Professional Services & Co-Founder

About CI Security

Healthcare organizations looking to improve their security programs work with CI Security. CI's Critical Insight Security Program gives hospitals, clinics, and life sciences organizations an integrated group of services to protect and defend themselves against cyber-criminals. Organizations looking for enterprise-level security programs on a small/mid-market budget turn to CI for its affordability.

CI is a mission-focused cybersecurity company providing Managed Detection and Response and healthcare consulting services. We protect and defend life-saving, life-sustaining organizations 24/7/365.

Sources

As Remote Work Becomes the Norm, Security Fight Moves to Cloud, Endpoints. (2020, May 8). DarkReading.
https://www.darkreading.com/cloud/as-remote-work-becomes-the-norm-security-fight-moves-to-cloud-endpoints/d/d-id/1337774

Global Surges in Ransomware Attacks. (n.d.). Global Surges in Ransomware Attacks.
https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/

Attacks Predicted to Triple in 2021, Black Book State of the Healthcare Industry Cybersecurity Industry Report. (n.d.). CISION PR Newswire.
https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525.html