IDENTIV SOLUTIONS BRIEF

Identity and Cybersecurity Solutions for Healthcare

Identiv helps healthcare organizations remain trusted by patients and perform the duty of care without worrying about data breaches.

Healthcare organizations are an ongoing criminal target due to the rich data they keep. Patients' personal information, medical history, as well as insurance information is easily stolen from poorly protected health institutions and used for various criminal purposes. As the 9/11 Dark Overlord hack and data exposure illustrate, life insurance and legal industries are also not safe when it comes to health-related hacks.

With the extensive, rapid shift of medical services to the digital world and vast sets of health data gathered amid the pandemic, criminals will likely seize this opportunity to infiltrate networks and hack sensitive patient information. Medical institutions must adopt better authentication practices in their operations to ensure that only authorized entities have access to patients' healthcare data.

Challenges Faced By the Healthcare Industry

COVID-19 Related Challenges

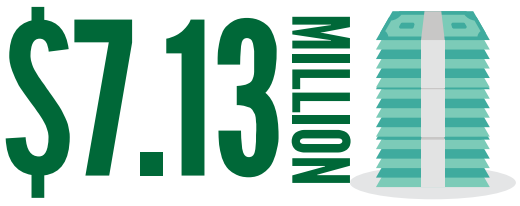
Since the outbreak of the coronavirus, remote healthcare services expanded exponentially as an alternative to hospital visits, enabling non-critical patients to receive medical attention while sheltering in place.

Healthcare organizations and government agencies are consumed with not only managing patient care but also the collection, monitoring, and management of COVID-19's progression and other related pandemic data.

As the healthcare industry continues to focus on the pandemic, these unprecedented changes in medical practices have left them further susceptible to another urgent problem: cybersecurity risks.

According to Black Book Market Research's 2020 report, about 75% of the healthcare industry indicated they are unprepared to handle these security risks. This research also revealed a 300% increase in data breach susceptibility among healthcare providers.

In addition, IBM reported data breaches in the healthcare sector amount to the highest average cost, about $7.13 million per breach amid the pandemic.



Cost of data breaches in healthcare amid the pandemic

Lack of Proper Security Controls

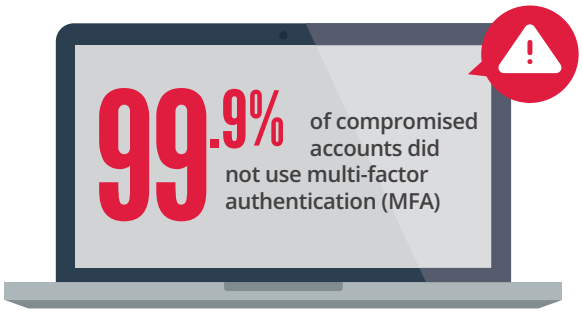
Complacency with weak passwords, lax security rules, and superfluous user permissions often make medical institutions susceptible to risk.

Access to healthcare databases is often shared by medical staff as well as other entities who handle patient's payment and insurance information.

Adding to those concerns around access are the Department of Health and Human Services' moves to improve interoperability and data sharing across the sector.

While healthcare's shift into greater data access is a natural progression, the industry is only further expanding its attack surface without proper security mechanisms.

The latest Microsoft statistics show that 99.9% of compromised accounts did not use multi-factor authentication (MFA); just 11% of organizations use MFA, overall. This means healthcare's security posture requires improvement.



Human Error and Negligence

Employees continue to be one of healthcare's biggest weaknesses with hackers consistently targeting user credentials to gain access into a system.

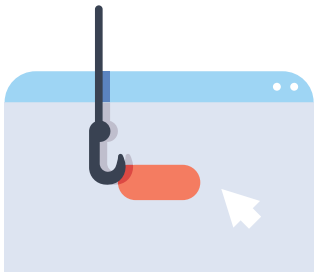
According to the Protenus Breach Barometer, insider incidents compromised 3.8 million records in 2019.

As per the FBI, phishing was the most common type of cybercrime in 2020, and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019 to 241,324 incidents in 2020.

According to a Microsoft spokesperson, stolen identities are the number one source of data loss and, on average, over 100 days pass before organizations discover there was a compromise.

In recent months, Centers for Medicaid and Medicare Services (CMS) and Walgreens have reported breaches stemming from app errors that connected patients to the wrong records, allowing them to view records from other individuals.

2020 PHISHING



was the most common type of cybercrime

How Identiv Can Help the Healthcare Industry

Healthcare organizations must do more to authenticate personnel accessing patient data to prevent personal identifiable information (PII) theft and other security breaches. They must improve their defenses by implementing strong authentication solutions that adhere to modern security standards like FIDO 2.0. This is exactly where Identiv can help.

FIDO 2.0

The FIDO Alliance's FIDO 2.0 protocols for passwordless authentication allow healthcare institutions to harness mobile technology for easier authentication in multiple channels.

Since FIDO2 credentials are cryptographically registered to a user's enrolled device, they cannot be easily shared by users, unlike passwords.

Leveraging cryptographic login credentials coupled with biometric strong authentication, fraudulent individuals can be prevented from accessing healthcare data.

MFA

Detecting a compromised identity can be challenging. It is always important to have good user behavior analytics, verification tools, and security logs to detect unusual activity, including logs from your endpoint management and endpoint security tools.

One way to close some of these security gaps is with the use of MFA, which can prevent a hacker from gaining full access to a network even if user credentials become compromised.

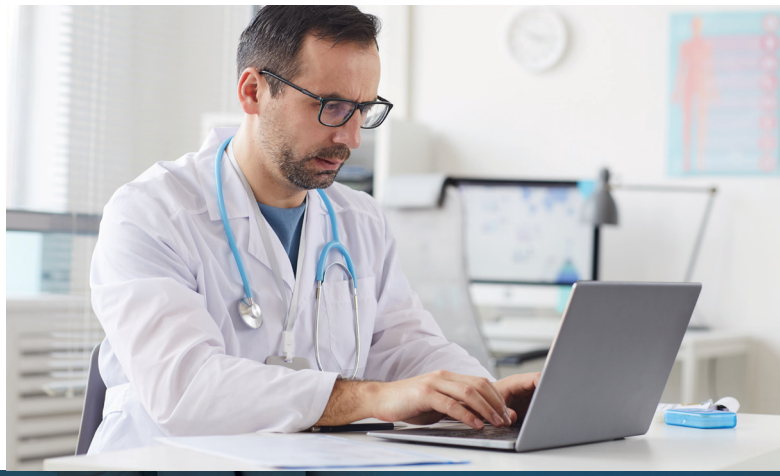
Benefits of Identiv's Cybersecurity Solutions

- **Protection of patients under the duty of care: Delivering FIDO-level strong authentication gives patients confidence they are the only ones accessing their data besides their trusted providers. This includes sharing medical records, giving consent, and other personal information patients believe their providers will do their very best to protect under HIPAA and duty of care.**
- **Strong authentication protocols: Identiv prevents breach of records by phishing or brute-force attacks with strengthened authentication protocols.**
- **Passwordless approach: Our uTrust FIDO2 NFC Security Keys provide a simple, strong authentication experience that eliminates the need for passwords.**
- **Multiple options: uTrust FIDO2 Security Keys support both contact (USB A/C) and contactless (NFC) use-cases, providing multi-protocol FIDO U2F, FIDO2, smart card, and OTP support.**
- **Security and identification in healthcare: We can improve secure facility access, video integration, badging, compliance, and RFID tracking at hospital sites.**
- **RFID-based data privacy: Identiv's HIPAA-compliant intelligent inlays protect patient privacy with RFID technology.**

Identiv's cybersecurity solutions keep healthcare staff and community members safe and protected.

Ready to secure your healthcare facility?
Speak to an expert today at sales@identiv.com or +1 888-809-8880.

uTrust FIDO2 NFC Security Keys



IDENTIV YOUR WORLD, **VERIFIED.**

Identiv, Inc. (NASDAQ: INVE) is a global leader in digitally securing the physical world. Identiv's platform encompasses RFID and NFC, cybersecurity, and the full spectrum of physical access, video, and audio security. For more information, visit **identiv.com** or email **sales@identiv.com.**