Implementing a Governance-Based Approach

to Identity in Healthcare

SailPoint

The digitization of healthcare has transformed the cyber-threat landscape. As demand for data sharing between healthcare organizations increases, so does the risk of non-compliance with regulations designed to protect patient records.

The consequences for non-compliance can be financially crippling with each regulatory violation costing the provider up to $1.5 million per year. In addition to the non-compliance fines, it's estimated that a single data breach can cost providers $4 million.

HIPAA and HITECH regulations are designed to protect sensitive health information from being improperly exposed or accessed. However, simply adhering to government requirements may not be enough to stem the tide of unwanted intrusions as evidenced in recent waves of health data breaches. Thus, the implementation of tools and systems – while they may verify compliance on an audit – do not put in place the policies and procedures to address the, often, more potentially-disastrous risks to the provider organization.

Going Beyond Compliance to Fill the Security Gap

Proving compliance with regulations is, of course, a very important goal. Still, even if the audit passes, the organization could be at risk if it does not address the larger security concern of employees' access to its data and applications. Taking a governance-based approach to security – where the tools used to meet compliance can see into every part of the organization – helps to ensure decisions about users' entitlements are based on all the relevant information. Connecting all the applications and systems a provider may utilize – and supporting applications like SSO with governance policies – is of paramount importance.

The question has become not if a healthcare provider will be attacked, but when.

90%
of healthcare providers have experienced a data breach in the past two years.
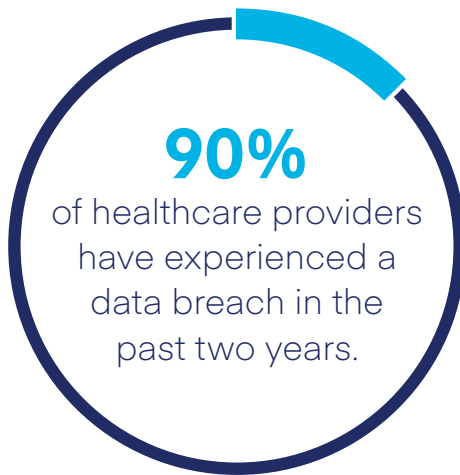
Often, providers have unique combinations of commonplace (such as Azure AD), proprietary (such as Epic) or other systems that are usually disconnected from each other all while holding important pieces of information – and not just about clients and patients. While a compliance tool may secure access to each of those systems independently, holistically knowing who has access to what, where that access overlaps and if it's a violation of security policies is instrumental in reducing the risk of breaches, theft and fraud as a healthcare organization.

Marrying the IT solution to good business policies and procedures ensures that both compliance and the security of your systems are addressed.

Only **16%**
of providers have a fully-functioning cybersecurity solution.

Implementing an identity management system to meet compliance with the applicable laws is the first step to securing an organization. But in order for providers to truly mitigate their risk, they must know who has access to what data and applications. Clinical and operational staff, contractors, partners, etc., may all have access to different sets of data. In order to safeguard and manage access to sensitive data, providers need consistent and unified policies and procedures that complement their compliance systems.

In 2016,
there were more than
$23 million
in HIPAA
settlements.

This partnership between compliance-driven tools and business processes certifies that employees have the right access to the right applications and data at the right time. Alignment between compliance driven tools and business processes ensures compliance to applicable regulations, while also mitigating the risk that inherently comes with users having access to and handling sensitive data.

Simply being compliant with regulations doesn't cover every piece of what a healthcare provider needs to be secure, but it is a perfect place to start the conversation – and project – concerning your organization's security and risk.

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.