Why is IAM so hard for Healthcare Providers?

4 Things to know about IAM

CORE SECURITY

01 Hard to Explain

Though your firewall may be strong, attackers are still going to get through by pretending to be an employee. So, how do you know you are letting the right people in? There should be authentication measures and monitoring in place to ensure that the identities on your network are acting like they should and not exfiltrating your data.

It's also hard to explain just how valuable your information is. A breach can affect your reputation which could end up with you losing money and the intellectual property.

The government knows how valuable it is. There are regulations in place, both by the government and the healthcare industry itself that force compliance on organizations.

They understand that the information you hold - such as a social security number - can affect your customers for the rest of their lives.

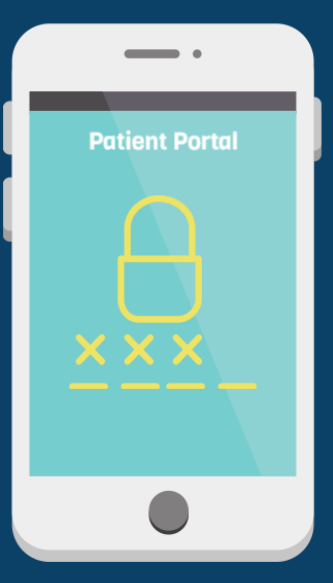
Think about it – stolen credentials like these can lead to leaked health information or cost them job opportunities

02 Hard to Enforce

While you can implement measures to create a more secure environment in the workplace, you can't force the general public to do the same - including your employees after in their off-hours or even your customers for that matter.

Forcing measures like multi-factor authentication on your customers can cause friction and upset their ease of use. One way to make this transition easier is to allow a mobile reset option. Customers can reset passwords on the go rather than having to call a help desk.

It's best to look for IAM solutions that include frictionless ways for your customers to interact and increase their safety.



03 Hard to Budget

Manual periodic access reviews requires a host of managers and system owners pulling user extracts, formatting files, adding contextual data and emailing files until the due date.

What price tag can you put on the time all of these resources spent being reviewed? Wouldn't it be worth the investment into a security tool that could help automate these efforts?

04 Hard to Ignore

Attacks using stolen or compromised user credentials will remain at the top of the attacker's playbook. Without appropriate IAM you will not be able to detect these attacks. This is no longer an issue to be ignored or to be patched with a bigger and better firewall.