Compliance Today - July 2021
How simplifying your IT environment can bolster security

By Gerry Blass and Jason Tahaney

Gerry Blass (gerry@complyassistant.com) is President and CEO at ComplyAssistant in Iselin, New Jersey, and **Jason Tahaney** (jason.tahaney@comop.org) is Director of Technology at Community Options Inc.

- linkedin.com/in/gerry-blass-917a482/
- linkedin.com/in/jason-tahaney-91653618/

In today's healthcare technology landscape, there is a greater need than ever before for everyone within the organization to be an active participant in cybersecurity. No longer is this simply the role of the health information management (HIM) team or information technology (IT) department. According to Pew Research Center, 71% of workers are doing their job from home all or most of the time.[1] This translates to an increased number of people sharing highly secure information online from home. For healthcare workers, the risk of threats such as phishing or malware attacks against valuable patient data is a real concern.

A simplified, streamlined IT environment is not only a more efficient way to work, but it can pay great dividends in boosting your organization's approach to cybersecurity. Multiple electronic health records systems, patient portals, and networked patient care technologies contribute to a complex infrastructure that can leave room for vulnerabilities, but with some strategic planning, you can ensure your environment reduces risk of breach. This article outlines practical guidance to ensure leaders at all levels within your organization are compliant and mitigate cybersecurity threats.

The power of the cloud

Oftentimes when it comes to simplifying the IT infrastructure within an organization, it's hard to know where to start. One of the first steps that leaders can take is to consider a cloud-based solution. By relying on cloud first, and on-premises solutions as a last resort, health leaders can save their organization countless resources, including time, money, and disaster recovery. Cloud solutions that are compliant with the Health Insurance Portability and Accountability Act provide assurance on a host of levels, with the ultimate goal of protecting patients and their private information. The recent uptick of cyberattacks in healthcare[2] is a telling reminder that corners can't be cut, and with cloud solutions, the chances of security breaches and compromise of proprietary patient data decrease significantly.

With cloud-based solutions, an organization is able to encrypt the data at risk. While some organizations have an easier time with this than others, it is essentially a way to deter malicious or negligent parties from getting access to sensitive data. Data encryption is a key line of defense in a cybersecurity framework, ensuring that the intercepted data are as difficult to decrypt as possible.[3]

While there are other steps that leaders can take to simplify their IT environment and in turn bolster security across the organization, which will be outlined later in this article, ensuring a proper cloud-based solution is one of the best ways to start. With cloud, you're guaranteed that there is already a service in place, and a continuity plan designed to drive your business forward safely and securely. It takes the guesswork out of the equation and

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

lightens the load for IT professionals, with the goal of simplifying things across the board.

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.