HealthManagement
Promoting Management and Leadership

New cybersecurity guidelines to fight hacking

As more medical equipment and mHealth devices get interconnected with **healthcare IT systems**, providers and other organisations are increasingly becoming targets of cyberattacks.

To help healthcare organisations manage cyber threats, the U.S. Department of Health and Human Services' Healthcare & Public Health Sector Coordinating Council (HPH SCC) recently issued **new guidance for enhancing cybersecurity.**

You might also like: New UK IT cybersecurity rules

The guidance document, entitled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, offers practical guidance for addressing what the Council has identified as the "most impactful threats... within the industry."

This document is a useful material for healthcare business managers faced with ever-increasing cybersecurity risks and the attending risks to patient safety and operational continuity, business reputation, financial stability, and regulatory compliance.

The guidance document leverages the well-known NIST Cybersecurity Framework to address the following threats:

- **E-mail phishing** attacks
- **Ransomware** attacks
- Loss or theft of equipment or data
- Insider, accidental, or **intentional data loss**
- Attacks against connected **medical devices** that affect patient safety

In each of these threat categories, the guidance identifies specific vulnerabilities, explains the impact that can result from each vulnerability, and suggests the best practices that healthcare businesses can implement to mitigate the risks associated with each kind of threats.

What's more, concrete and practical recommendations are presented in two volumes, one intended for small healthcare businesses and another for medium and large healthcare organisations. Small businesses get a concise 29 pages of easy-to-read advice.

For large organisations that have more information technology personnel and resources, a more fulsome 100-page document has been prepared by the Council. (Both these volumes are available at https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx).

Although the guidance document purports to provide "voluntary, consensus-based and industry-led guidelines, best practices, methodologies, procedures, and processes," healthcare businesses that experience a data breach or cybersecurity incident that could have been prevented by implementing the recommended practices are likely to be vulnerable to claims of negligence or failure to implement appropriate safeguards in private litigation or a government inquiry.

Healthcare administrators and business managers are encouraged to read this guidance as soon as possible to determine whether their organisation's cybersecurity strategy aligns with this most recent guidance.

Organisations with an established **risk assessment and risk management** planning processes may incorporate application of this guidance using their chosen methodologies, according to the Council. The guidance also includes some recommendations regarding risk assessment and promises a new assessment toolkit specific to this guidance in the future.

Source: JD Supra
Image credit: Pixabay

Published on : Tue, 12 Mar 2019