Navigating Regulations in a Digital Age

Reading time:
Tom Wilson
Last Modified on 01/05/2024 12:13 pm AEST

Tags: Medical Practitioner | Dental Practitioner | Webinars | Technology | On Demand

In this session, we will try to understand and answer the question about why healthcare practitioners are particularly prone to attacks from cyber criminals? What are the relevant cyber security and privacy regulatory requirements impacting medical and dental practice and how can you ensure your practice is and remains compliant?

Historically the healthcare sector has maintained a solid record of protecting patients' confidential information, however the rapid rise in digitisation and the increase in cyber risk exposure has meant that many healthcare practitioners feel overwhelmed keeping up the pace with compliance regulations. The lack of education, knowledge and technical comprehension can leave some healthcare practitioners exposed and at risk of hefty fines and legal action if found in breach of regulations.

With the aid of case studies, we will provide an introduction to understanding why healthcare practices can be targeted that will help healthcare practitioners understand privacy requirements, how to implement them in digital practice and how future regulations are likely to impact practitioners.

Learning outcomes

At the end of this webinar, participants will be able to:

1. Identify cyber security regulatory requirements under the Privacy Act 1988 for medical practitioners.
2. Identify what is sensitive and personal information under the Privacy Act 1988.
3. Identify a notifiable data breach under the Privacy Act 1988.

Presenters

Presented by **Priyanka Saha** and **Daniel Muchow** - joint Managing Directors of the Resilience by Design Group Pty Ltd (RBD).

Priyanka is a lawyer and expert in online safety, telecommunications, privacy, and cyber security. Priyanka is passionate about building safe and secure technology environments for medical practitioners to provide world class patient experiences. With over 15 years' experience working as an expert advisor, and program manager across Federal Government, Corporate and the education sector, Priyanka ensures the cyber programs are rigorously evaluated against best practice frameworks and professional development requirements.

Daniel has over 15 years' experience in cyber security, intelligence and risk management developed in operational roles across the public and private sectors. Daniel values the important role of the public sector in online safety and security. He has been a key contributor to the Australian Government's national cyber security review and served on the expert committee of the Victorian Government's Cyber Security Strategy Group.

RBD training materials are reviewed by medical practitioners and the RACGP, ACRRM, and RACS. RBD is a trusted eSafety provider, as well as a member of the Australian Government's Joint Cyber Security Centres and Be Connected Network Partner.

Watch the webinar

Related articles

CAREER LEADERSHIP PROGRAM >