Managing personal information in the healthcare sector

ORGANISATIONS MUST CAREFULLY consider how to handle the personal information of customers, employees, visitors and neighbours; for some organisations, this can be a challenge.

In Australia, we have the Australian Privacy Principles (APPs), which are contained in Schedule 1 of the *Privacy Act 1988*, and are the cornerstone of our privacy protection framework.

A breach of these 13 APPs can lead to regulatory action and penalties.

In addition to the APPs, there are privacy regulations around the world, such as General Data Protection Regulation (GDPR), that are fundamentally reshaping the handling of personal information; for example, if organisations based in Australia handle the personal data of citizens in the European Union, they must comply with the GDPR. Beyond the European Union, at least 132 countries now have a privacy law in place. Organisations that transfer personal data between these countries must consider each relevant law when looking at controls to protect privacy.

THE ROLE OF STANDARDS

Implementing and monitoring controls to support compliance with such regulation laws can be a challenge. To make this more manageable, the adoption of standards can help organisations to meet regulatory compliance, giving them confidence that they have taken the necessary steps. Such standards include ISO/IEC 27701, an internationally recognised standard that enables organisations to extend their existing ISO/IEC 27001 information security management system (ISMS) to address privacy requirements.

ISO/IEC 27701 identifies controls that must be in place to encourage the management of personally identifiable information (PII) in a systematic and transparent way. It clarifies the requirements for both PII controllers and processors.

Controls in the standard cover the entire life cycle of PII – through collection, analysis, sharing, storage and deletion. The individual that the PII relates to is at the centre of these controls. This is critical in the healthcare industry where patient records contain confidential information that individuals may not wish to be shared.

Health information, such as care plans, medication and clinical trials, is vital for medical breakthroughs in support of medical science research, but this data is sensitive personal information and needs to be managed carefully. Organisations holding vital health information or providing health services covered by the Privacy Act require a robust system with suitable controls to manage the PII. Standards like ISO/ IEC 27001 can help organisations to manage risk and improve performance. The introduction of ISO/IEC 27701 helps respond to the more detailed requirements set by privacy regulators, and can support organisations to ensure that privacy is a fundamental part of their organisational governance. ●

For more information, please call 1300 730 134, email info.aus@bsigroup.com or visit bsigroup.com/en-au.