The little book of personal health information (PHI)

Leveraging ISO 27799 within the ISO/IEC 27000 series

Contents

1. What is PHI?

Personal health information (PHI) involves safeguarding the confidentiality, integrity, and availability in digital healthcare environments. It outlines guidelines for managing information security risks, vouching critical health information systems resilience against disruptions, and upholding accountability. Committing to these principles enables organizations to safeguard patient data, foster trust, and bolster overall information security.

In the ever-evolving landscape of healthcare information security, organizations navigate a complex terrain influenced by technological advancements, regulatory demands, and the critical need for patient privacy.

Welcome to the BSI little book of patient health information, designed to illuminate the path to robust information security in healthcare within the ISO/IEC 27000 framework.

2. The need for PHI regulations

As healthcare embraces digitalization, the safeguarding of PHI is paramount. Standards guide the development of vigorous organizational information security management practices, involving control selection, implementation, and management tailored to the organization's risk environment(s).

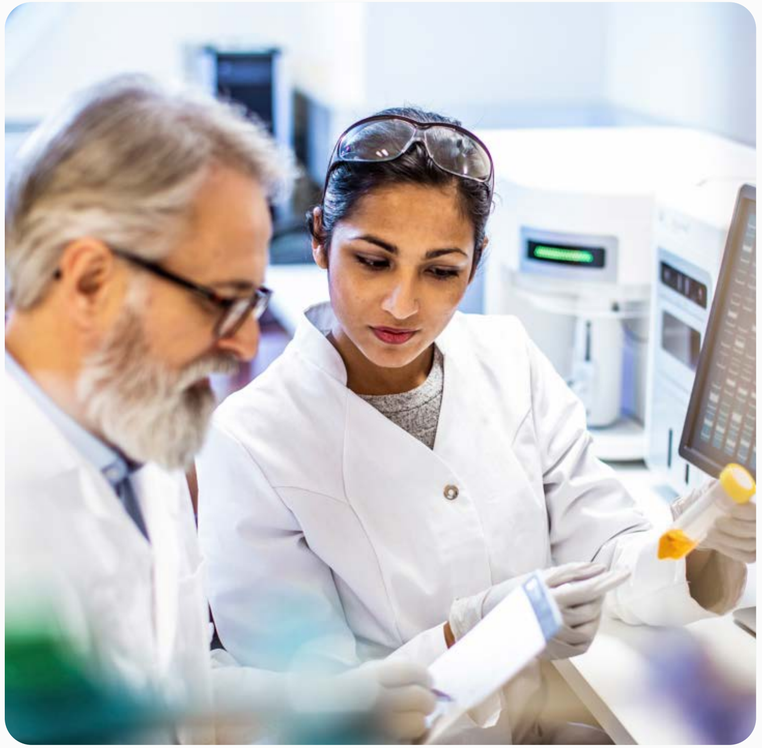
ISO 27799 serves as a beacon, designed to meet the unique needs of healthcare organizations on the best practices to promote confidentiality, integrity, auditability, and availability of health data.

This comprehensive guide caters to a diverse audience, including healthcare entities, security advisors, and third-party service providers.

Embarking on the ISO 27799 certification journey is an a ISO/IEC 27000 framework requirement and a strategic move to fortify your organization. By aligning with this standard, healthcare environments can anticipate reduced security incidents, enhanced staff morale, and increased public trust in systems handling PHI.

Throughout this guide we unravel the intricacies of ISO 27799, providing clear, concise, and healthcare-specific guidance for robust information security across healthcare ecosystems.

In addition to the intrinsic value of safeguarding PHI, it's imperative to understand the fiscal ramifications associated with breaches and non-compliance. Today, cybercrimes cost the world approximately $600 billion yearly, corresponding to almost 0.8 % of the global GDP. As healthcare data is the most crucial asset, healthcare institutions are investing significantly in protecting the data from the risk of cyberattacks.



Current industry challenges

Rapid technological advancements

In the ever-evolving landscape of healthcare, rapid technological advancements pose both opportunities and challenges. The integration of Internet of Medical Things (IoMT) devices and digital health technologies introduces novel possibilities for patient care and data management. However, this influx of technology brings forth heightened concerns regarding the security and privacy of PHI. The dynamic nature of these advancements requires healthcare organizations to continually reassess their information security strategies to adapt to emerging threats.

Increasing sophistication of cyberthreats

The healthcare sector is witnessing a surge in the sophistication of cyberthreats targeting sensitive health data. From ransomware attacks to targeted breaches, adversaries are becoming more adept at exploiting vulnerabilities in digital health ecosystems. The interconnected nature of healthcare networks, coupled with the expanding attack surface introduced by IoMT devices, underscores the urgency for robust cybersecurity measures. Organizations must stay vigilant against evolving threats to safeguard patient confidentiality and data integrity.

Warranting interoperability without compromising security

As healthcare embraces interoperability for seamless data exchange, assuring the secure flow of information becomes a paramount challenge. Balancing the need for data sharing across diverse healthcare systems while maintaining stringent security measures is a delicate equilibrium. The industry grapples with establishing standardized protocols that facilitate interoperability without compromising the confidentiality and integrity of PHI. Striking this balance is crucial for fostering collaboration among healthcare entities while upholding patient trust in the security of their health information.

Emerging technologies and risks

Impact of IoMT

The integration of IoMT introduces transformative capabilities in healthcare, ranging from remote patient monitoring to smart medical devices. However, this interconnected ecosystem brings forth a new set of cybersecurity challenges. Crafting robust security measures that encompass IoMT devices is essential to mitigate risks and uphold the integrity of health data in this digitally interconnected era.

Addressing risks in emerging technologies

As healthcare embraces emerging technologies, including artificial intelligence (AI) and telehealth solutions, organizations must proactively address associated risks. From promoting the confidentiality of AI-driven diagnostic data to safeguarding telehealth communication channels, a comprehensive approach to risk management is indispensable. By integrating security considerations into the fabric of emerging technologies, healthcare entities can foster innovation while maintaining the highest standards of patient data protection operability.

Interplay between security and usability

Achieving a balance between security and usability is a pivotal consideration in the development and implementation of healthcare technologies. Simultaneously, organizations must implement robust security measures without compromising the user experience. Striking this delicate balance endorses that security becomes an enabler rather than an impediment to the effective use of digital health solutions. As the healthcare industry continues its digital transformation, aligning security measures with user expectations becomes integral to the success of information security initiatives.

The average cost of a healthcare breach in the U.S. has risen to over $10 million, marking a 9.4% increase from 2021 and a staggering 41% increase over the past two years.*

*Cost of a data breach (IBM data breach 2023)

3. Strength of data protection legislation

As healthcare systems transition towards digitalization, the need to safeguard PHI against evolving threats has become increasingly critical. By examining how data protection laws intertwine with ISO certification standards, we understand the significance of international standards in fortifying the security and integrity of PHI within the healthcare landscape.

Data protection around different parts of the globe

1. Americas

The protection of health data is regulated by various laws and standards. For instance, the United States has the Health Insurance Portability and Accountability Act (HIPAA), which establishes minimum standards for safeguarding health information. HIPAA compliance aligns closely with ISO 27799 requirements, particularly in assuring confidentiality, integrity, and availability of PHI. Healthcare organizations seeking ISO certification can leverage HIPAA compliance efforts to streamline its ISO 27799 implementation process.

Similarly, countries like Canada and Brazil have adopted laws influenced by the General Data Protection Regulation (GDPR), reflecting a commitment to protecting personal data, including health information. ISO 27799's emphasis on risk management and security controls resonates with GDPR principles, providing a framework for healthcare organizations to enhance its data protection practices in alignment with international standards.

2. Asia

Countries exhibit varying degrees of data protection regulations across Asia. China, for example, is in the process of implementing the Personal Information Protection Law (PIPL), indicating a growing recognition of the importance of data privacy. ISO 27799’s holistic approach to information security management can complement emerging regulations like PIPL, offering healthcare organizations comprehensive guidance on safeguarding PHI in compliance with both local and international standards.

Countries such as Hong Kong and South Korea have robust data protection laws akin to GDPR, highlighting a commitment to safeguarding privacy and security in healthcare.

ISO 27799’s sector-specific focus on health informatics aligns seamlessly with the requirements of these regulations, facilitating a structured approach to managing PHI security risks.

3. Europe

GDPR stands as a cornerstone of data privacy legislation. GDPR’s stringent requirements for protecting personal data, coupled with its extraterritorial applicability, have significant implications for healthcare organizations worldwide. ISO 27799 provides a complementary framework for healthcare entities to achieve GDPR compliance by addressing specific security considerations unique to the healthcare sector.

Furthermore, GDPR’s mandate for electronic health data sharing by 2025 underscores the need for healthcare organizations to prioritize information security measures.

ISO 27799’s emphasis on continuous improvement aligns with GDPR’s principles of accountability and transparency, fostering a culture of ongoing compliance and risk mitigation.

4. Asia Pacific

Countries such as Taiwan and Singapore have enacted Personal Data Protection Acts closely resembling GDPR provisions. ISO 27799's alignment with global best practices enables healthcare organizations in these countries to adopt a standardized approach to PHI protection, facilitating interoperability and information sharing while maintaining compliance with regulatory requirements.

However, challenges persist in regions like Thailand, where the Personal Data Protection Act (PDPA) may be weakened by critical omissions. ISO 27799 can serve as a guiding framework for healthcare organizations operating in such environments, providing a roadmap for strengthening data protection measures and addressing regulatory gaps effectively.

Global Differences

- The EU's GDPR is stricter than the US's HIPAA in that it also covers marketing information in addition to medical data and puts a limit on how long data can be held. It also has more rigorous data breach notification rules.
- Brazil and South Korea also protect incomplete, anonymized personal data if to be used to identify an individual when combined with other data.
- In China, data controllers must inform the authorities if the data indicates any prohibited activities by the data subject.
- India broadly exempts government bodies.

The healthcare industry has held the highest average cost of a breach for 12 consecutive years.*

*Cost of a data breach (IBM data breach 2023)

4. Global impact of ISO/IEC 27000:
Evolution of healthcare data security

The implications of these intertwined standards are vast; healthcare organizations can foster continued trust by demonstrating adherence to them, thus safeguarding the confidentiality and availability of health data. This adherence becomes particularly crucial considering global movements toward more stringent regulation of health data.

Across key global markets, there is a noticeable uptick in healthcare data protection legislation and evolving AI regulations. The US, with its impending HIPAA updates, heavily underscores risk assessment and data protection both at the heart of ISO/IEC 27000 standards. Meanwhile, Asia-Pacific regions like Singapore with its PDPA and other nations following the requirements of GDPR, signal an emphasis on the criticality of data security and privacy certifications.

In essence, the interplay of the ISO/IEC 27000 series is not merely a collection of standards but a synchronized mechanism delivering a more resilient future for PHI management – the question addressed in this report is what the most appropriate ones are to serve the stakeholders in the digital health technology field. As the terrain of global health data protection evolves, these standards remain pivotal, shaping how healthcare entities build and maintain trustworthy digital fortresses around the sensitive data they are purposed to protect.

The new revision, anticipated in 2024, of ISO 27799 offers an advantageous opportunity for further input and refinement to this standard, with the opportunity to promote alignment with emergent technologies and continuously evolving regulatory requirements globally. A central question to pose to the project team is where they see its place in the sector going forward.

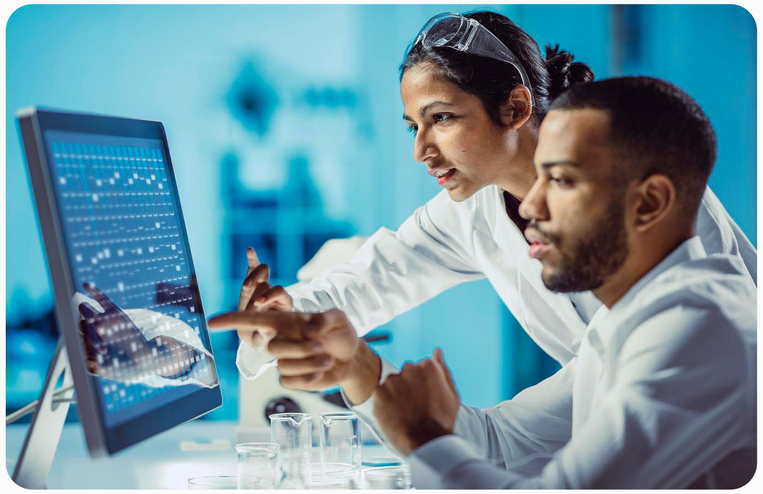
5. Navigating health informatics standards

Interrelated standards within information security management systems (ISMS) include ISO 27799, ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701. ISO/IEC 27001 provides the framework for establishing an ISMS, while ISO/IEC 27002 offers detailed guidance on implementing security controls. ISO 27799 extends this guidance specifically for the healthcare sector, supplementing ISO/IEC 27001 and aligning with ISO/IEC 27002 to address the unique challenges of managing PHI securely in healthcare organizations.

ISO/IEC 27701 further enhances this framework by providing additional guidelines for privacy information management within the context of ISO/IEC 27001 and ISO 27799. It extends the scope of ISO/IEC 27001 to include privacy controls and addresses specific privacy concerns within the healthcare sector, safeguarding a comprehensive approach to managing information security and privacy requirements.

The joining of ISO standards provides the foundation for PHI security within health informatics. Their synergistic application details how organizations can responsibly manage sensitive health data. ISO/IEC 27001 articulates the framework for an ISMS, while ISO/IEC 27002 presents optimized control sets to reflect contemporary security practices.

ISO 27799 serves as a health sector-specific extension of ISO/IEC 27001/27002, poised for a critical update, to align with newer standards and evolving global healthcare regulations. The precise role of ISO 27799 within various healthcare settings, specifically as it relates to manufacturers versus care providers, is a particular focus.



Given the swift pace of change within healthcare data security and AI regulation, leveraging established ISO standards helps organizations pre-emptively address future regulatory requirements and maintain agility in the face of legislative change.

The Anthem cyberattack, involving phishing/malware to patient health records, affected over 78 million PHI records, leading to a settlement of $115 million to resolve litigation.*

*Cost of a data breach (IBM data breach 2023)

6. Aligning personal health information:

The synergy between ISO/IEC 27001, ISO/IEC 27701, ISO 27799, and ISO/IEC 27002

In healthcare information security, ISO standards like ISO/IEC 27001, ISO/IEC 27701, ISO 27799, and ISO/IEC 27002 work together to build strong defenses against evolving threats.

ISO/IEC 27001 sets the stage for a systematic approach to safeguarding sensitive information, requiring a risk assessment and a catalog of security controls outlined in Annex A. Notably, this catalog originates from its sister standard, ISO/IEC 27002 – Information Security, Cybersecurity, and Privacy Protection – Information Security Controls.

ISO 27799 builds on the guidance provided in ISO/IEC 27002, making it specifically relevant to the healthcare environment and presented in the language of healthcare professionals. The integration of ISO 27799 into the synergy of ISO/IEC 27001, ISO/IEC 27701, and ISO/IEC 27002 further enhances the information security strategy.

ISO/IEC 27701 extends the scope of ISO/IEC 27001 and ISO 27799 by providing additional guidelines for privacy information management. It aligns with ISO/IEC 27001 by extending the ISMS requirements to include privacy controls and aligns with ISO 27799 by addressing the specific privacy concerns within the healthcare sector. Incorporating ISO/IEC 27701 into the existing framework assures that privacy considerations are adequately addressed alongside information security measures.

ISO/IEC 27701 provides best practices and guidance on implementing the controls necessary for information security management and privacy information management. In the healthcare context, this means tailoring these controls to address the unique challenges and regulatory landscape of the sector, reinforcing the confidentiality, integrity, and availability of health information.

At BSI, our commitment extends to facilitating this integration, guiding healthcare organizations toward a unified ISMS that meets sector-specific requirements outlined in ISO 27799 and ISO/IEC 27701 but also incorporates the detailed controls from ISO/IEC 27002. This comprehensive approach aligns with global best practices, fostering resilience and trust in the healthcare ecosystem.

By implementing these standards concurrently, healthcare organizations establish a unified ISMS. This integrated approach promotes compliance with sector-specific requirements outlined in ISO 27799 and ISO/IEC 27701. It also incorporates the broader principles of ISO/IEC 27001, along with the detailed controls provided by ISO/IEC 27002. The combined effort results in a resilient and comprehensive information security framework, addressing the unique challenges of the healthcare sector while aligning with international best practices.

This integrated approach not only enhances the organization’s ability to adapt to evolving threats but also instills patient trust, demonstrating a commitment to the highest standards of information security and privacy management.

Benefits of the integrated approach

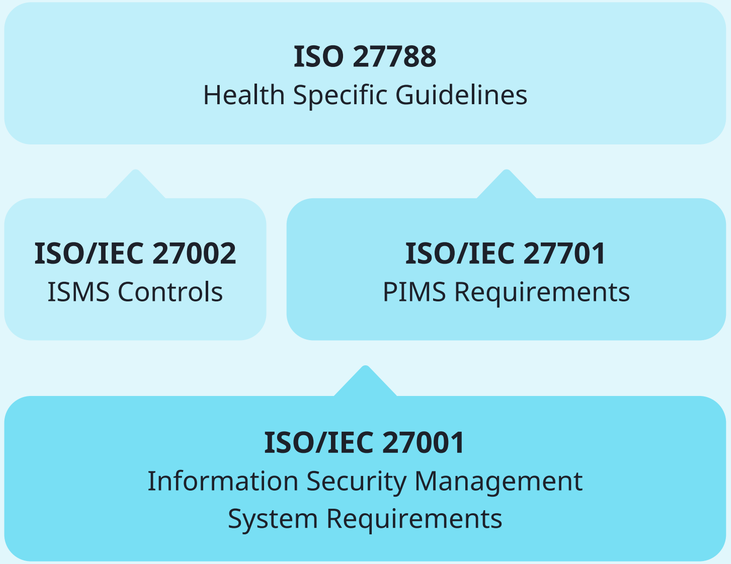
1 **Comprehensive risk management:**
The integrated approach allows organizations to comprehensively identify, assess, and manage risks specific to healthcare data, enhancing overall risk management effectiveness.

2 **Enhanced regulatory compliance:**
The dual implementation streamlines regulatory adherence, fostering a proactive and robust compliance strategy that meets both general information security requirements and healthcare-specific mandates.

3 **Strengthened confidentiality and integrity:**
The integrated controls reinforce the confidentiality of PHI and fortify data integrity, safeguarding a cohesive strategy that protecting sensitive health data.

4 **Unified information security culture:**
The integrated approach cultivates a culture of information security within the organization, resonating with both general principles and healthcare-specific nuances.

Information Security Management System (ISMS) & Privacy Information Management System (PIMS)



In the UK, failure to notify the Information Commissioner’s Office of a personal data breach within 72 hours can result in fines up to 2 percent of global turnover, as evidenced by Meta’s contestation of fine over $1 billion imposed by Ireland’s Data Protection Commission for mishandling data transfer.*

*Cost of a data breach (IBM data breach 2023)

7. Global implications of the ISO/IEC 27000 series:

An evolving healthcare data security landscape

The implications of these intertwined standards are vast; healthcare organizations can foster continued trust by demonstrating adherence to them, thus safeguarding the confidentiality and availability of health data. This adherence becomes particularly crucial considering global movements toward more stringent regulation of health data.

Associated standards related to data security and PHI

ISO/IEC 27701:
ISO/IEC 27701, an extension for privacy information management, integrates with ISO/IEC 27001, offering a tailored framework that includes privacy considerations, crucial in managing PHI.

PCI DSS:
PCI DSS (Payment Card Industry Data Security Standard) is a security standard crucial for organizations handling credit card information. Although not healthcare-specific, its emphasis on secure data handling aligns with broader principles applicable to safeguarding sensitive information.

SOC 2 Type 1 and Type 2 SOC 2:
These comprising type 1 and type 2 reports, establishes a framework for managing and securing data, frequently employed by service providers storing customer data in the cloud. The evaluation involves an independent assessment of the controls in place relevant to security, availability, processing integrity, confidentiality, and privacy.

NIST CSF:
NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) provides a comprehensive framework to manage and reduce cybersecurity risk. While not specific to healthcare, its principles contribute to a robust cybersecurity posture, essential for protecting health information systems.

NIST 800-53 and NIST 800-171:
NIST 800-53 outlines security controls and requirements for federal information systems, while NIST 800-171 focuses on non federal systems. These standards, although not healthcare-exclusive, contribute to establishing secure information systems across sectors.

CMMC 2.0:
CMMC (Cybersecurity Maturity Model Certification) is a framework specifically tailored for endorsing the cybersecurity readiness of defense contractors. While not healthcare-specific, the framework's focus on maturity levels and cybersecurity practices contributes to overall organizational resilience.

MVSP:
MVSP (Medical Vendor Security Program) is a security program specifically tailored for medical vendors. It addresses the unique security requirements and challenges faced by vendors operating in the healthcare industry, safeguarding the protection of sensitive health data.

NIST Privacy Framework:
NIST Privacy Framework is designed to improve privacy through enterprise risk management. While not specific to healthcare, its principles can be applied to enhance the privacy posture of organizations handling PHI.

Microsoft SSPA:
Microsoft SSPA (Microsoft Secure Software Development Standard) is Microsoft's framework for developing secure software. While not healthcare-exclusive, adhering to this framework is crucial when developing healthcare applications and systems to ensure robust security measures.

Across key global markets, there is a noticeable uptick in healthcare data protection legislation and evolving AI regulations. The US, with its impending HIPAA updates, heavily underscores risk assessment and data protection, both at the heart of ISO/IEC 27000 standards. Meanwhile, Asia-Pacific regions like Singapore, with its Personal Data Protection Act and other nations following the requirements of GDPR, signal an emphasis on the criticality of data security and privacy certifications.

In essence, the interplay of the ISO/IEC 27000 series is not merely a collection of standards but a synchronized mechanism delivering a more resilient future for PHI management. As the terrain of global health data protection evolves, these standards remain pivotal, shaping how healthcare entities build and maintain trustworthy digital fortresses around the sensitive data they are purposed to protect.

Looking ahead

The anticipated 2024 revision of ISO 27799 offers an advantageous opportunity for further input and refinement to this standard, with the opportunity to warrant its alignment with emergent technologies and continuously evolving regulatory requirements globally.

8. Deployment considerations and a look to the future

When determining the best standards for implementation, it's crucial to assess the geographical spread of healthcare entities seeking certification. This involves understanding the regional variations in healthcare practices, legal frameworks, and cultural nuances that may impact the implementation process. The assessment should identify specific regulatory obligations and assure that the deployment strategy aligns with these requirements. This includes addressing legal aspects, data breach notification requirements, and that the certification process is adaptable to changes in regulatory frameworks over time.

Different countries may have specific regulations and guidelines related to health information security. For instance, the European Union's GDPR places stringent requirements on the protection of personal data, including health information.

Understanding and aligning with these regional considerations during deployment permits that the ISO 27799 certification is effectively tailored to the specific needs of each location.

There is anticipation for an update to this health informatics standard expected in September 2024. Stakeholders engaged in regulatory practices and health informatics now have the opportunity to contribute insights to this update process. ISO WG 215 and IEC WG 4 will convene in March 2024 to further refine the draft.

Navigating the complexity of healthcare information security demands the consideration of regional dynamics and regulatory landscapes. Aligning strategies with specific obligations promotes the effective tailoring of standards like ISO 27799 to diverse frameworks.

BSI will continue to monitor and contribute to the refinement of ISO 27799, safeguarding its relevance and effectiveness in addressing the evolving challenges of health informatics.

Your partner
in progress

BSI Group
389 Chiswick High Road
London, W4 4AL
United Kingdom
+44 345 080 9000
bsigroup.com