Safeguarding privacy in the complex healthcare ecosystem

Leveraging privacy-specific processes such as PIA to protect privacy and uphold the rights of patients

Global healthcare industry is changing at a rapid pace with innovations in technology in a complex ecosystem. In particular, the rise of interconnected medical devices has transformed care delivery in ways that was unimaginable before.

WHO estimates that there are 2 million different kinds of medical devices in the world market, which are categorized into more than 7000 generic devices groups.

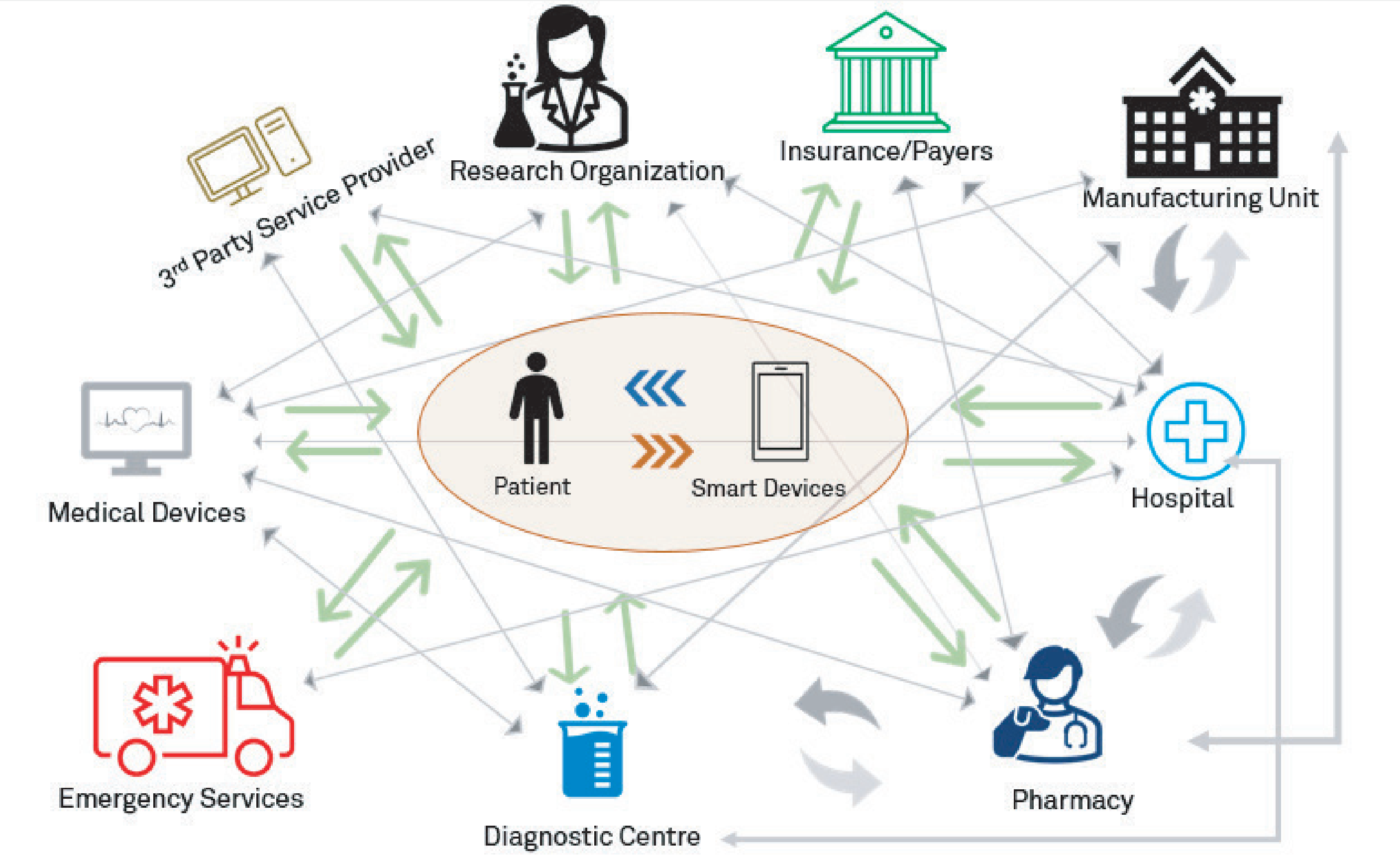


Fig 1: A representative view of complex interconnected healthcare ecosystem with patient data flowing across stakeholders

The accompanying digital ecosystem has expanded with this technological shift, creating a need for interconnectivity between different players including, but not limited to, diagnostic centers, healthcare providers, medical device manufacturers, insurers, data aggregators, technology service providers and pharmacies. Patient data is at the center of this expansion, integrating healthcare ecosystem and strengthening decision-making. Stakeholders leverage patient data to deliver safe, effective and secure services within the new technological paradigm.

The introduction of interconnected medical devices, however, has impacted the way patient data is processed, used and stored across the chain of care. Thus, while the story reads well so far, challenges are inevitable due to inherent complexities. The below table provides a view of security and privacy risks with new age technological changes within the complex ecosystem:

New Age Technology	Benefits	Security and Privacy
Big Data analytics	Aids in decision making, allows new business models, better manage population health	More Data, More Liabilities in the event of Breach
Cloud Adoption	Cost optimization and efficient processing of data	Cross Border Data Transfer Challenges
Usage of Social Media	From customer acquisition, to better engagement with patients	Lack of Control and possible compromise on security
Mobility	For continuous and real-time engagement with the customer & any-time availability of services	Target of Attack Due to App Vulnerability
Location Data	For location-based services & digital marketing	Intrusion of Privacy
Internet of Things (IoT)	Makes connected healthcare a possibility	Potentially Insecure Channel

Given this scenario, healthcare organizations including medical device manufacturers have become targets of cyberattack as the patient data traverses the vast network of managed and unmanaged medical devices, complex infrastructure across different stakeholders. These take advantage of vulnerabilities not just within medical devices but across the chain of care due to system or network weaknesses, and human error among others.

Some of the most common cyber-attacks to which the industry is vulnerable include the following:

- Phishing attacks
- Ransomware
- Denial of service (DDoS)
- Sniffing
- Insider Threats

These cyberattacks typically lead to unauthorized access or disclosure, loss or theft of patient data and at the same time such serious data breach results in privacy violations and compromise even leading to significant fines to be paid by the affected organization. According to Australian Cyber Security Centre (ACSC), ransomware is currently the most significant cybercrime threats in Australian health sector. In 2020, 166 cyber security breach incidents were reported which was significantly higher than 90 cyber security breach in 2019.

Privacy

While security measures such as malware protection, firewalls, access control, vulnerability assessment, data encryption, etc. address security risk, privacy requires a layer of trust to be established between the patient and the stakeholders. This is achieved by adopting privacy best practices including, but not limited to, consent management on usage or transfer of PHI data, data subject rights management, geo location for the storage of such data, and data retention time frames.

In the backdrop of the many privacy regulations across the globe, privacy has emerged as an important consideration in the healthcare ecosystem. It is compelling organizations to re-evaluate the methodology of dealing with their most critical asset – customer data including patient data, for safeguarding privacy. In this paper, our focus is to explore how some challenges to privacy in the interconnected medical IoT world can be addressed by leveraging PIA effectively.

It further explores how PIA as a part of the overall privacy program process safeguards privacy for patients in the complex healthcare ecosystem, in addition to cybersecurity to ensure medical device functionality and safety.

Need for PIA in Healthcare Ecosystem

Regulations view in the industry

With newer and widespread technological security threats affecting privacy and security of information, governments and regulatory bodies across geographies have enacted laws and regulations to govern the healthcare industry. For example, EU Commission, Australian Government's Department of Health, Therapeutic Goods Administration (TGA) have issued guidelines and regulations for medical device manufacturers towards cyber risk mitigation.

Regulations such as the European Union's General Data Protection Regulation (GDPR), Australia's Privacy Act and Health Insurance Portability and Accountability Act (HIPAA Privacy Rule), require organizations to have a purpose to collect and process personal information (patient data included), and limit processing to stated purpose.

The regulations apply to all who process, use, store or archive patient medical data and subsequently apply to medical device manufacturers and all the players in the healthcare ecosystem who handle personal information.

In it's 'medical device cyber security guidance', Australian Government's TGA states that the risk management for medical device cyber security requires assessment and corresponding action over the life-cycle of the device and it is manufacture's responsibility. One of the key considerations is, Personal health data, including data collected from medical devices, as it presents a lucrative target for malicious activity, requiring secure storage and transmission solutions.

Privacy Impact Assessment

PIA helps an organization to identify patient personal information processed by the organization and risks of processing such personal information, analyze the risks, and provide controls to manage risks.

Privacy regulations require organizations to conduct impact assessment of their processing activities dealing with personal information. Some of these laws such as GDPR mandate that the organizations implement security and privacy by design while manufacturing medical devices or developing health care information systems.

Planning

- Understand PI (& SPI) handled by organization, processes, systems and devices processing the PI
- Understand the Privacy and Security Policies of the organization

Access and Analyze

- Review the data flow lifecycle of PI data elements that are collected, processed, reported, shared and stored by the business assets in different locations.
- Analyse privacy policies and data management practices based applicable privacy principles and regulations.

Risk Assessment and Treatment

- Identify privacy risks from the PI flow.
- Define risk mitigation strategies based on criticality
- Review and refine Privacy Controls based on mitigation strategies

Document

- Develop Privacy Risk Register
- Residual Risk Sign Off by Business
- Monitor & Validate PIA Outcomes

Fig 2: Typically a PIA exercise involves 4 stages

PIA seeks answers to

- What PI and SPI is processed by a type of device or a health care application?
- How does PI flow from collection to processing to storage to archival/disposal?
- With whom is the PI shared and who can access the data?
- What safeguards – technical and organizational measures – are implemented to protect the PI?
- How long the personal information is retained and how is it disposed?
- What is the technology used to process the data at each stage? What is inherent threats and risks that the organization carries due to the technology used?
- Are all the risks identified, analyzed and have a treatment plan? Are the risks continuously monitored?
- Does the organization comply with the requirements of applicable privacy laws?
- How are the rights facilitated to individuals?

Key challenges in execution of PIA

Under regulations such as GDPR, it becomes the responsibility of device manufacturer to test and release the product and develop updates to avoid any breach. Manufacturers also have the responsibility of addressing the compliance requirements. Additionally, manufacturers are required to report certain adverse events or product problems to the regulatory authorities

In the integrated and connected digital world, it is a challenge for the manufacturers, clinical service providers and other health related service providers, to identify when they need to initiate PIA and what should be its scope. Another challenge is to ensure that the devices, equipment, applications and systems have the required level of security built to protect the privacy of information processed. We will address these in following sections.

Triggers for PIA

PIA should be initiated when there is new change planned in products or services, processes or policies of an organization PIA helps identify potential problems at an early stage when addressing them is often simpler and less costly. The primary triggers for conducting PIA are shown in the fig 3.

Besides the ones listed in fig 3, the organization should consider conducting the PIA of all existing products and services at least once annually. These will help identify new risks and effectiveness of the risk treatments done previously.

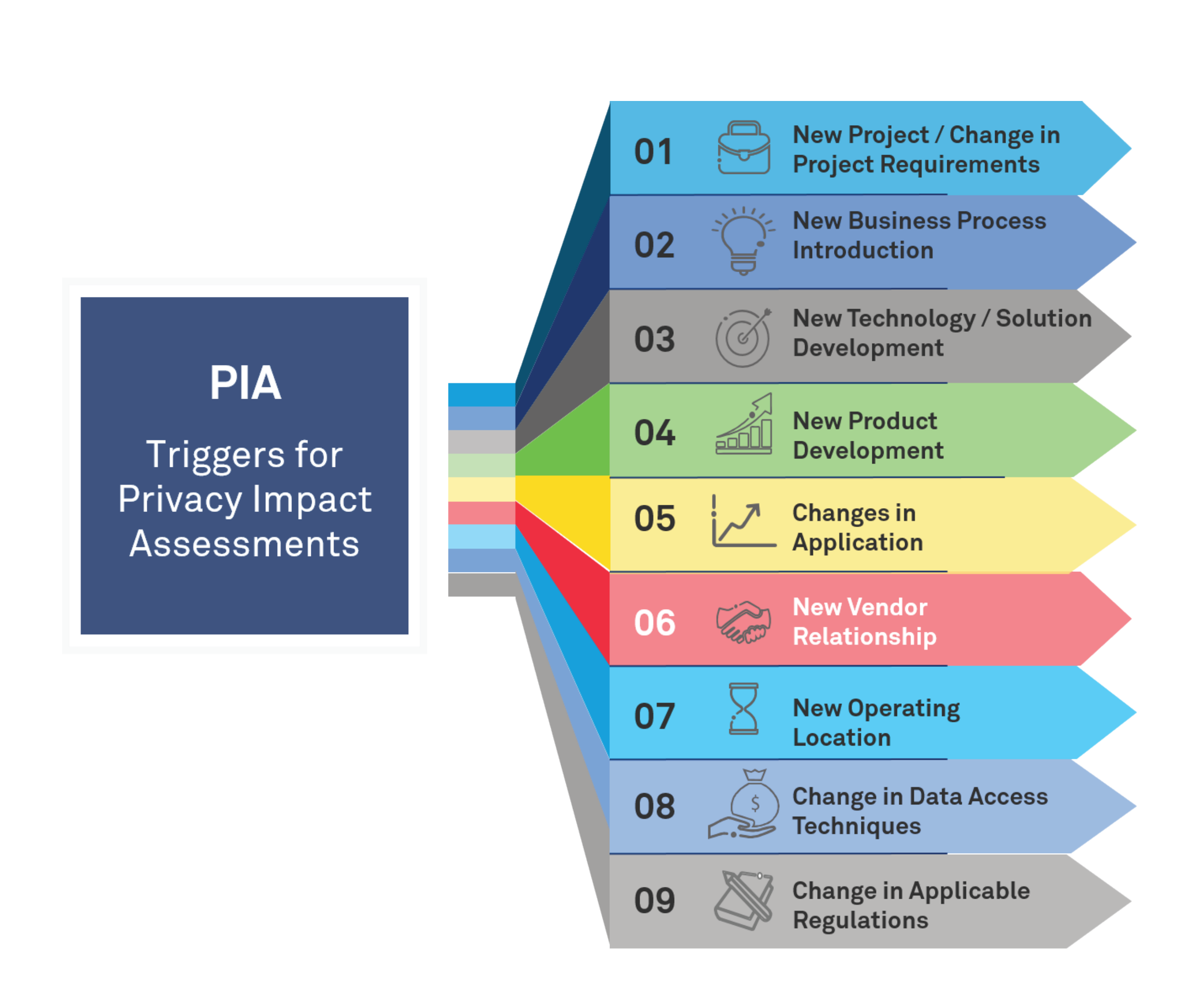

PIA
Triggers for Privacy Impact Assessments
01 New Project / Change in Project Requirements
02 New Business Process Introduction
03 New Technology / Solution Development
04 New Product Development
05 Changes in Application
06 New Vendor Relationship
07 New Operating Location
08 Change in Data Access Techniques
09 Change in Applicable Regulations

Fig 3: Triggers for PIA

Scope of PIA

The privacy regulations communicate that ensuring privacy and security of personal information is a shared responsibility of manufacturers, clinical service providers and other healthcare related service providers. Each player in the healthcare ecosystem needs to ensure privacy and security of the personal information processed by them.

We looked at two segments in this paper, the device manufacturers and the clinical service providers and identified key factors to consider while conducting PIA.

Device Manufacturers

The device manufacturer should conduct PIA of the devices at the new device ideation stage. This will help the organization to ensure that security and privacy requirements are included in the design itself (Privacy and Security by Design). Similarly for existing devices, the manufactures should conduct PIA when any change is proposed to the device. For example, upgrade of hardware or software of an existing device or new features or integration points are added to the device.

If any third party is involved in manufacture, like parts provider, software provider, the manufacturer should ask for documentation that help verify that appropriate technical measures are implemented to protect personal information. The manufacturer should also request PIA report if applicable and information on privacy and security risks and the effectiveness of risk treatments.

Besides the standard safety and security documents required under the applicable security and healthcare regulations, the manufacturers should also share with their customers a report on compliance with privacy regulation.

Use case of PIA for Medical Device

Below illustration captures the PIA process for medical devices by device manufacturer.

1. Planning

- Prepare list types of devices in scope.
- Identify applicable privacy laws and regulations, get the specific requirements.
- Identify resources, points of contact who can provide technical and business information on the device.
- Schedule and plan PIA activity for each device.

2. Assess and Analyze

- Understand the function of the device.
- If the device hardware has parts and software supplied by third parties. For each supplier, verify if supplier has shared PIA report if applicable and risks information.
- Understand consent management if applicable.
- Understand each unique data flow from collection to storage to processing/analysis to sharing and reporting of data. For each stage understand
  a. how the device/application is integrated with other systems.
  b. the internal and external parties who have access to the device. Identify the processing activities carried out by each party.
  c. the controls implemented to protect the data during each stage of the data flow and integration with the other.
- Identify how long the data is retained by the device for each data flow.
- Document how rights are provisioned to individuals, if applicable.

3. Risk Assessment & Treatment

- Identify and assess risks related to
  a. Each supplier.
  b. Each integration – technology, people and process
    i. Internal devices and systems
    ii. External devices and systems
- Assess risks related to service continuity
  a. Damage or theft of the device.
  b. Corruption of software running the device.
  c. Malware or Ransomware attack.
  d. Power failure, fire or natural calamities.
- Review existing privacy controls and identify gaps related to protection of personal information and rights of individuals.
- Discuss gaps and the risks identified with control owners.
- Define risk mitigation strategies based on criticality of the risks.
- Define/refine privacy controls based on mitigation strategies.

4. Risk Assessment & Treatment

- Prepare Privacy Risk Register.
- Get sign off on the residual risk.
- Prepare PIA Report.
- Document Risk monitoring, review and reporting process.
- Agree on date of next review cycle.

Fig 4: PIA for Medical Device

Clinical service and health related service providers

The clinical service providers like hospitals, need to ensure that for all the devices, healthcare equipment and applications that they purchase, the procurement department additionally requests for documentation that demonstrate compliance to applicable privacy laws, request for PIA report and risks information.

Each department or unit in the service provider's organization should be in the scope of PIA exercise. An inventory of personal information processed, processes and systems that deal with personal information should be the start point for conducting PIA exercise in each department or unit.

For applications and systems used across business processes like the Healthcare Information System, each device and application, which forms part of the Healthcare Information Systems should be assessed separately under PIA.

Use case of PIA by clinical service provider

Below illustration captures the PIA process for Healthcare Information System (HIS) by clinical service provider.

1. Planning

- Identify applicable privacy laws and regulations.
- Get list of all devices connected to the HIS.
- Get list of individual applications that make the HIS.
- Get names of all the application owners, the points of contact for device technical discussions.
- Plan PIA of each device and application in HIS.

2. Assess and Analyze

- Understand the functionality of the device/application.
- If the device/application is procured from a third party, verify if
  a. necessary security and privacy regulatory compliance documents have been reviewed by procurement team.
  b. third party has shared PIA report if applicable and risks information.
- Understand what PI is collected and for what purpose.
- Understand consent management if applicable.
- Understand each unique data flow from collection to storage to processing/analysis to sharing and reporting of data. For each stage understand
  a. how the device/application is integrated with other systems.
  b. the internal and external parties who have access to the device/application. Identify the processing activities are carried out by each party.
  c. the controls implemented to protect the data during each stage of the data flow and integration with the other.
- Identify how long the data is retained by the device/application for each data flow.
- Document how rights are provisioned to individuals, if applicable.

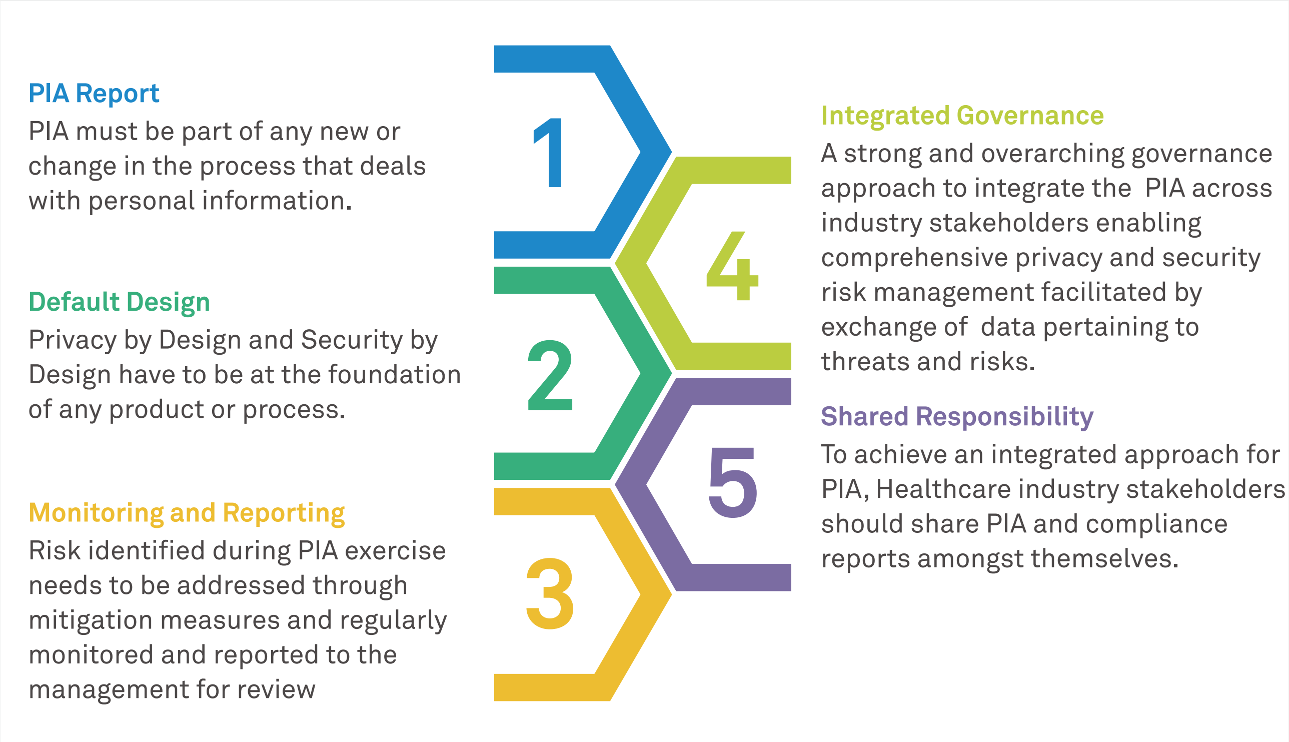
3. Risk Assessment & Treatment

- Identify and assess risks related to
  a. Each supplier.
  b. Each integration – technology, people and process
    i. Internal devices and systems
    ii. External devices and systems
- Assess risks related to service continuity
  a. Damage or theft of the device.
  b. Corruption of software running the device.
  c. Malware or Ransomware attack.
  d. Power failure, fire or natural calamities.
- Review existing privacy controls and identify gaps related to protection of personal information and rights of individuals.
- Discuss gaps and the risks identified with control owners.
- Define risk mitigation strategies based on criticality of the risks.
- Define/refine privacy controls based on mitigation strategies.

4. Risk Assessment & Treatment

- Prepare Privacy Risk Register.
- Get sign off on the residual risk.
- Prepare PIA Report.
- Document Risk monitoring, review and reporting process.
- Agree on date of next review cycle.

Fig 5: PIA for Clinical Service Provider



PIA Report
PIA must be part of any new or change in the process that deals with personal information.

Default Design
Privacy by Design and Security by Design have to be at the foundation of any product or process.

Monitoring and Reporting
Risk identified during PIA exercise needs to be addressed through mitigation measures and regularly monitored and reported to the management for review

Integrated Governance
A strong and overarching governance approach to integrate the PIA across industry stakeholders enabling comprehensive privacy and security risk management facilitated by exchange of data pertaining to threats and risks.

Shared Responsibility
To achieve an integrated approach for PIA, Healthcare industry stakeholders should share PIA and compliance reports amongst themselves.

Fig 6: Key takeaways for safeguarding privacy in the complex healthcare ecosystem

Conclusion

Given the nature of the Healthcare industry with its multiple stakeholders and extended complex ecosystem through which sensitive data navigates, the need of the hour is not to simply secure the information and protect privacy with stronger and effective controls, but for all the participants to work together building trust networks leveraging technology for focused collaboration so that the entire chain of care is by design addressing these critical requirements. This will help organizations strengthen their defense mechanisms and build more resilient systems.

In short, the medical device manufacturers are critical participants within the ecosystem to build privacy and security frameworks for compliance to regulations and protection of data. Specific to privacy, conducting a PIA is critical to align with and embed privacy requirements into the very fabric of the medical device and overall Healthcare ecosystem.

References

- **European Union Medical Device Regulation - Regulation (EU) 2017/745 (EU MDR) -** https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02017R0745-20170505&from=EN
- **General Data Protection Regulation - Regulation (EU) 2016/679 -** https://gdpr-info.eu/
- **Australian Cyber Security Centre published 2020 Health Sector Snapshot -** https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/2020-health-sector-snapshot
- https://www.who.int/health-topics/medical-devices#tab=tab_1
- https://www.medicaldevice-network.com/comment/cybersecurity-medical-changing-threats/

About the Authors

Shubham Shekhar

Shubham Shekhar is a presales consultant at Wipro in the Strategy & Risk Advisory Practice with Wipro Limited. A sales and marketing enthusiast, he has over 10 years of experience in sales, business development and consulting across domains - Fintech, IT, and PSUs. He is adept in developing and implementing business strategies for growth.

Rupa Parekh

Rupa Parekh is Practice Director with Wipro Limited, and has around 18 years of experience in various consulting, business and delivery roles in the information security domain. She is an accomplished risk and compliance leader with extensive experience in data privacy and protection. She is passionate about creating and delivering effective and efficient solutions to clients in their information security journey in the fast-paced digital world.

Vrinda Muzumdar

Lead Consultant – Cyber Security and Risk Practice

Vrinda Muzumdar has over 25 years of experience in IT industry, primarily in the area of application program management. For last six years she has been involved in Cyber Security and Data Privacy consultancy. She has worked extensively in this domain and has helped clients in Banking, Fintech, Retail and ITES industries to develop and implement privacy programs.

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful.
A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 220,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**