ICIC Express Letters
Volume **17**, Number **1**, January **2023**

ICIC International ©2023 ISSN 1881-803X
pp. **81–90**

A PROCESS MODEL FOR DATA PROTECTION IMPACT ASSESSMENT IN THAILAND'S HEALTHCARE SECTOR

Charnsak Srisawatsakul[1], Waransanang Boontarig[1,*]
and Gerald Quirchmayr[2]

[1]Faculty of Computer Science
Ubon Ratchathani Rajabhat University
2 Ratchathani Road, Naimueang, Mueang, Ubon Ratchathani 34000, Thailand
charnsak@researcher.in.th; *Corresponding author: waransanang.b@ubru.ac.th

[2]Faculty of Computer Science
The University of Vienna
Währinger Straße 29, A-1090, Vienna, Austria
gerald.quirchmayr@univie.ac.at

Received April 2022; accepted June 2022

Abstract. *The Data Protection Impact Assessment (DPIA) is a process or methodology that should assist an organization in ensuring the reasonable and trustworthy use of personal data throughout the process. In the healthcare sector, medical information is typically extremely sensitive personal data that must be protected by ensuring a high level of privacy. In Thailand, The Thai government has recently enacted a new Personal Data Protection Act (PDPA), which mandates that organizations protect personal data by law. Furthermore, if the healthcare industry collects, stores, or processes patients' data from the European Union (EU), the data processors are obligated to conduct a DPIA in accordance with the General Data Protection Regulation (GDPR). The DPIA should be implemented as soon as the new processing of personal data is designed, and it is a continuous improvement process. However, the DPIA process is still relatively new in Thailand's healthcare sector. Therefore, this study proposes a process model for conducting DPIA suitable for the Thai healthcare industry. The proposed process model was adapted from leading DPIA guidelines in EU countries and Thailand's PDPA. The findings of this study should assist data controllers and project managers in conducting an adequate DPIA, thereby boosting public trust in their organization's information systems and ensuring compliance with PDPA and GDPR.*

Keywords: PIA, DPIA, GDPR, PDPA, Privacy impact assessment, Healthcare privacy, Privacy

1. **Introduction.** The General Data Protection Regulation (GDPR) has a significant influence throughout all organizations worldwide that collect and process personal data on European Union (EU) citizens. The principle of GDPR is to protect personal data and any processing of it securely. In Thailand, the government published the Government Gazette of a new Personal Data Protection Act (PDPA) with a similar purpose to GDPR.

Healthcare organizations have implemented various information technologies to collect and handle patients' health information, such as the Electronic Medical Records (EMR). Hence, that information is extremely sensitive data. As a result, the privacy of healthcare information is an essential concern of the sector.

The Privacy Impact Assessment (PIA) is a tool that could help assess the impacts on the privacy of a project, policy, or service at the start of a new business or implements a new process [1]. Similar to PIA, the Data Protection Impact Assessment (DPIA) is a GDPR compliance activity. Therefore, organizations that rely on information systems to store,

DOI: 10.24507/icicel.17.01.81

process, and exchange personal information for various purposes, including healthcare, are required to conduct a DPIA if they wish to process the personal data of EU citizens.

However, Thailand did not have a personal data protection law before. This paper addresses this gap by providing practical guidelines for conducting DPIA based on a critical evaluation of existing DPIA methods in healthcare and identifying their most effective practices. Therefore, the objective of this paper is to propose the processes model of conducting DPIA in the Thailand healthcare sector. The following is the organization of the paper. First, it gives a critical evaluation of the recent related literature on the GDPR, PDPA, DPIA, and existing PIA framework of the healthcare sector. Second, the process for doing PIA is presented by analyzing relevant literature. Finally, the conclusion, discussion, and recommendations for further research are presented.

2. Literature Review.

2.1. **General data protection regulations.** The European Commission introduced GDPR in July 2016. Each organization, however, was given a two-year grace period to prepare. As a result, the GDPR became effective in all European Union member states on May 25, 2018 [2]. Following that, the GDPR contributed to increasing awareness of personal data protection throughout the European Union and the rest of the globe. The reason is that it expanded the scope of data protection to every collection and process of information related to EU citizens with no exception. Moreover, the GDPR has legislated new concepts to increase data protection, such as data protection by design and default.

2.2. **Personal Data Protection Act Thailand.** Thailand never had a law explicitly regarding personal data protection until 2019. Thailand legislated its first Personal Data Protection Act, published in the Government Gazette on May 27, 2019. The majority of the PDPA's sections have a one-year grace period scheduled to begin on May 27, 2020. However, the effective date was postponed twice more, in 2020 and 2021. Finally, the PDPA's effective date has been shifted to May 2022 at the time of publication of this article. The PDPA focuses on the collection, processing, disclosure, protection, and right of the data subject. In PDPA, it is not required that every organization undertakes a DPIA. The DPIA, on the other hand, will ensure that the organization does not violate the PDPA, which carries a hefty fine of 3 million Thai baht [3].

2.3. **Privacy impact assessment and data protection impact assessment.** The EU's PIA history begins with the Privacy Impact Assessment Framework (PIAF) in 2011 [1]. According to prior research on the PIAF, the first revision advises conducting PIA in Europe, Australia, Canada, Hong Kong, New Zealand, the United Kingdom, and the United States of America [1]. As a result, PIA has multiple definitions, but we define it following the GDPR. According to the GDPR, a data protection impact assessment is described as

> "a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them" [4].

2.4. **Guidelines on data protection impact assessment (Article 35 of GDPR).** It serves as the primary framework for conducting a DPIA compliance with GDPR [4]. It was published in conjunction with Regulation 2016/679, clarifying the EU GDPR's requirements. In October 2017, the DPIA was officially declared in Article 35 of GDPR [5]. Article 35 specifies that not all processes or activities are required to conduct a DPIA. DPIA is required only if the processing of data is "*likely to result in a high risk*". The GDPR establishes nine classification criteria for the term "likely to result in a high risk", as stated in Table 1.

Table 1. Nine criteria of the process that "likely to result in a high risk"

No	Criteria	Healthcare information
1	Evaluation or scoring	Yes
2	Automated decision making with legal or similarly significant effect	Possibly
3	Systematic monitoring	Possibly
4	Sensitive data or data of a highly personal nature	Yes
5	Data processed on a large scale	Yes
6	Matching or combining datasets	Possibly
7	Data concerning vulnerable data subjects (recital 75)	Yes
8	Innovative use or applying new technological or organizational solutions	Possibly
9	When the processing in itself "Prevent data subjects from exercising a right or using a server or a contract."	Possibly

According to Table 1, the nature of the collection and processing of health information may meet four criteria that indicate a high risk, implying that healthcare providers are required to conduct a PIA for their procedures.

The GDPR guideline serves as general guidance for conducting a DPIA. Nonetheless, there are numerous principles and recommendations for performing a DPIA in various contexts, for example, the PIA method from French's Commission Nationale de l'Informatique et des Libertés (CNIL) [6], and New Zealand PIA toolkit from Office of the Privacy Commissioner New Zealand [7]. Vemou and Karyda [8] provided a comprehensive analysis and discussion of the various PIA methodologies. They used 17 criteria to evaluate nine published PIA techniques in policy and academic contexts. The findings indicated that the majority of PIA procedures incorporate the following criteria: threshold analysis, risk assessment guidance, a responsible person, the involvement of external stakeholders, a sign-off function, the publication of the PIA report, periodic review, and a PIA report template. In addition, they concluded that the CNIL's PIA is the most comprehensive and up-to-date GDPR-based guideline.

2.5. **Existing DPIA guidelines in the healthcare sector.** Based on their legal framework, some organizations proposed guidelines and templates for doing DPIA, specifically in the healthcare sector.

2.5.1. *Privacy Impact Assessment toolkit for health and social care.* Ireland's Health Information and Quality Authority (HIQA) developed the Privacy Impact Assessment toolkit for health and social care [9]. HIQA is an independent agency created to promote safe, high-quality health and social care in Ireland. They have established standards, evaluated and reviewed health and social care services, and supported the improvement of service delivery. This guideline is divided into five stages: beginning with threshold assessment, identifying the privacy risks, addressing privacy risks and evaluating solutions, producing the PIA report, and incorporating the PIA outcomes into the project plan.

2.5.2. *Privacy Impact Assessment Policy.* The Privacy Impact Assessment Policy establishes guidelines for performing PIAs in accordance with the Personal Health Information Protection Act of Ontario (PHIPA). It is developed by Canadian Institute for Health Information (CIHI). The PHIPA contains guidelines and best practices for protecting health information in general [10]. However, this paper did not include a specific procedure for conducting a PIA in healthcare.

2.5.3. *The HIPAA Privacy Rule.* The HIPAA Privacy Rule was established following the United States of America's public law and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [11]. On the other hand, this privacy rule contains a set of national regulations designed to safeguard particular types of health information. It has no rules or guidelines regarding the PIA methodology.

2.5.4. *Managing Information Privacy and Security in Healthcare Privacy Impact Assessment Guide.* This is a comprehensive framework designed for the healthcare industry for conducting the PIA. It was published in the year 2008 [12]. This framework provides the step-by-step of the PIA process. There are eight steps to do the PIA in healthcare, including 1) Establish organizational imperative, 2) Oversee PIA process, 3) Initiate PIA, 4) Conduct PIA (collect data), 5) Compile findings review, 6) Findings and assess risks, 7) Define design requirements to address risks, and 8) Implement remediation.

TABLE 2. Studies on privacy impact assessment for healthcare

No	Name	Organization	Legal framework	Country	Template
1	Privacy Impact Assessment toolkit for health and social care	The Health Information and Quality Authority (HIQA) [9]	GDPR	Ireland	Yes
2	Privacy Impact Assessment Policy	Canadian Institute for Health Information [10]	PHIPA	Canada	No
3	The HIPAA Privacy Rule	HHS.gov U.S. Department of Health & Human Services [11]	HIPAA	USA	No
4	Managing Information Privacy & Security in Healthcare Privacy Impact Assessment Guide	Healthcare Information and Management Systems Society (HIMSS) [12]	–	Worldwide	No

In conclusion, the existing DPIA frameworks in the healthcare sector cannot accommodate all organizational requirements. It may be outdated, not based on the legal framework, and lag in detailed processes. On the opposite, the explicitly defined frameworks for each country's context and legal requirements make them incompatible with Thailand's PDPA. In this instance, the Thai healthcare industry's framework for conducting PIAs must be developed according to PDPA's requirements and compiled with GDPR.

3. A Process for Conducting DPIA of the Healthcare Sector in Thailand.

In this work, we developed a comprehensive process for performing DPIAs that is appropriate for the Thai healthcare business, based on EU regulations and PDPA instruments.

3.1. Roles in the DPIA.

Data Protection Officer (DPO) is the person within an organization who is responsible for ensuring that the personal data of its staff, customers, suppliers, as well as any other individuals (data subjects) complies with any data protection laws [13]. In this case, the healthcare providers need to appoint the DPO based on their knowledge of data protection. Depending on the organization's context, it can be appointed to a similar position such as risk management, and senior executive. Moreover, that person should have no conflict of interest between the duties he or she has been assigned. The DPO should be directly reported to the top management. During the DPIA, the DPO is the person who signs off the PIA report.

Data Controller refers to the juristic person who has the authority and responsibility to make decisions regarding the collection, use, or disclosure of data subjects' personal data [3]. In other words, the data controller is the person who determines the purpose and means of the personal data needed to be processed [14].

Data Processors are the persons who process personal data on behalf of the data controller. Sometimes the data controller and data processor are the same entity.

3.2. **Who should organize the DPIA?** The healthcare provider should initiate the DPIA by the person recognized as having the appropriate expertise and knowledge regarding the proposed project [9], such as the project manager. However, it depends on the context of the organization. For example, CNIL [15] suggests that the data controller should be the person who conducts the DPIA. Furthermore, the DPO also should provide guidance during the DPIA processes. Finally, in the end, the DPIA report should be signed off by the DPO or senior executive responsible for the organization [1].

3.3. **DPIA processes model.**

3.3.1. *Stage 1: Study of the context.* This is the initial stage of DPIA; it is used to ascertain the context in which data is processed. It should begin by outlining the new processing context's definition, scope, goal, and stake. Additionally, it is critical to identify the healthcare project's data controller and processor.

Study data flow, data processing, and support assets: In this process, the personal data required to be stored and storage duration should be described. In addition, the project's supporting assets, such as smartphones, tablets, body sensors, and Wi-Fi networks, should be fully explained.

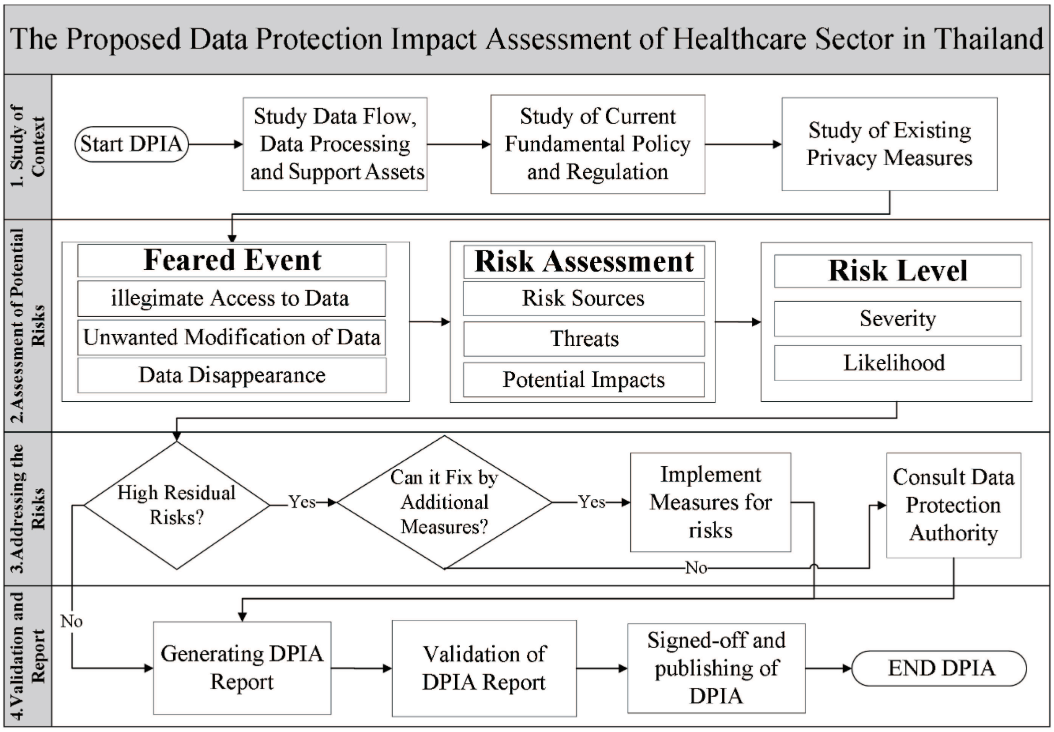
The Proposed Data Protection Impact Assessment of Healthcare Sector in Thailand
1. Study of Context
Start DPIA
Study Data Flow, Data Processing and Support Assets
Study of Current Fundamental Policy and Regulation
Study of Existing Privacy Measures
2.Assessment of Potential Risks
Feared Event
illegimate Access to Data
Unwanted Modification of Data
Data Disappearance
Risk Assessment
Risk Sources
Threats
Potential Impacts
Risk Level
Severity
Likelihood
3.Addressing the Risks
High Residual Risks?
Yes
Can it Fix by Additional Measures?
Yes
Implement Measures for risks
No
Consult Data Protection Authority
4.Validation and Report
No
Generating DPIA Report
Validation of DPIA Report
Signed-off and publishing of DPIA
END DPIA

FIGURE 1. The DPIA process adapted from EU [4], HiQA [9], Bieker et al. [16], and CNIL [6]

Study of current fundamental policy and regulation: Study the fundamental of relevant laws and policies that should help with privacy protection and avoid a fine if we fail to comply with them. Table 3 provides examples of fundamental policies and regulations that may apply to Thailand.

TABLE 3. Fundamentals policy and regulation for privacy protection

Criteria	Definitions	GDPR	PDPA
Consent given	The project should provide a clear statement for asking for the consent of data processing from data subjects such as the patients.	Art. 6	Sect. 19
Right of access	The data subject should have the right to obtain information about their personal data processing.	Art. 15	Sect. 30
Right to data portability	The data subject should have the right to receive personal data concerning him or her.	Art. 20	Sect. 31
Right to rectification	The data subject shall have the right to rectify his/her personal data.	Art. 16	Sect. 35
Right to erasure	The data subject should have the right to erase personal data concerning him or her.	Art. 17	Sect. 33
Right to restricting of processing	The data subject shall have the right to obtain from the controller restriction of processing, see Art. 18 of [GDPR].	Art. 18	Sect. 34
Right to object	The data subject shall have the right to object, on grounds related to his or her situation, at any time to the processing of personal data concerning him or her.	Art. 21	Sect. 32

Study of the privacy measures: The implementation of privacy measures could ensure the safeguard of personal data protection. However, the procedure for implementing the measure cannot be used as a universal checklist for all projects. Moreover, it needed to be tailored made for each project. Nevertheless, there are some recommended privacy measures suggested by CNIL [6], as shown in Table 4.

3.3.2. *Stage 2: Assessment of potential risks.* This is the most crucial step in the healthcare DPIA process. The DPO of the project should evaluate it. There are three distinct feared scenarios that could occur: illegitimate access to data, unwanted modification of data, and data disappearance. The assessment of potential risks should begin with the identification of the risk source, followed by a determination of how the risk source might pose a threat to the organization. What are the potential consequences if the threat occurs? Following that, outline the anticipated and planned privacy safeguards to prevent threats or mitigate the potential damage. Table 5 illustrates an example of a potential risk assessment. Finally, the level of risk associated with each feared event should be determined by analyzing its severity and likelihood. Table 6 summarizes the likelihood and severity of each scenario.

Severity: The magnitude of a risk is denoted by severity. It depends on the harmful nature of potential impacts.

Likelihood: It refers to the possibility that a risk will occur. It depends on the vulnerability level of the risk source or supporting assets.

3.3.3. *Stage 3: Addressing the risks.* This stage is designed to find the residual risk after assessing potential risks. If the residual is low, stage 4 should be commenced. Nonetheless, if the residual risks are still high, additional measures to prevent those risks should be added to the assessment and continue to stage 4. If there are no feasible measures, the DPIA conductor should seek consultation from the data protection authority.

Table 4. Recommended standard privacy measures by CNIL [6]

Categories	Privacy protection measures	
Data management	Logical access control	Data partitioning
	Anonymization	Data minimization
	Encryption	Backups
	Archiving	Integrity monitoring
Physical security	Physical access control	Operating security
	Hardware security	Paper document security
	Maintenance	Managing workstation and clamping down on malicious software
Network security	Website security	Security of computer channels (networks)
	Monitoring network activity	Avoiding sources of risk
	Traceability (Logging)	
Policy management	Protecting against non-human sources of risks	Risk management
	Privacy policy	Organization
	Supervision	Management of incident and data breaches
	Project management	Personnel management
	Relations with third parties	

Table 5. The assessment of potential risks

Feared event	Risk sources	Threats	Potential impact	Planned measures
1) Illegitimate access to data	• Human or non-human • Inside or outside • Accidentally?	The compromising of personal data or supporting assets. For example: • Patient record theft • Physical damage to devices • Hacked medical equipment	The consequence is threats occurring. • Phishing • Patient loss of medical record • Deterioration in the service quality	Choose from the planned measure that would prevent the threat or reduce the potential impact
2) Unwanted modification of data				
3) Data disappearance				

3.3.4. *Stage 4: Validations and reports.* The DPIA conductor should write a report summarizing the results from stages 1-3. The visual presentation of the data will aid the audience in understanding the DPIA. CNIL [6] recommended that the report contain a risk mapping assessment and action plan.

Risks mapping: It is the most common method for presenting the assessed overall and residual risks after assessment. It should show the risk of feared events before and after implementing planned measures in terms of severity and likelihood. The example of risk mapping is shown in Figure 2. The example objective after mapping the risks is shown in Table 7. For example, the risk of illegitimate access to data was at its maximum severity and likelihood. However, following the planned measure steps from stages 1-3, the risk was decreased to a limited level of severity and likelihood.

TABLE 6. The explanation of the level of likelihood and severity

Level	Severity	Likelihood
Undefined	• Cannot be defined	• Cannot be defined
Negligible	• No effect with data subjects • A few inconveniences with the project • Fix without any problem	• Not possible to occur
Limited	• Significant inconvenience with data subjects • Difficult to fix	• Rarely occuring
Significant	• Significant consequence problem with data subjects • Really hard to fix the problem	• Possibly occuring
Maximum	• Significant and irreversible problems with data subjects • It cannot be fixed without any problem.	• Frequently occuring

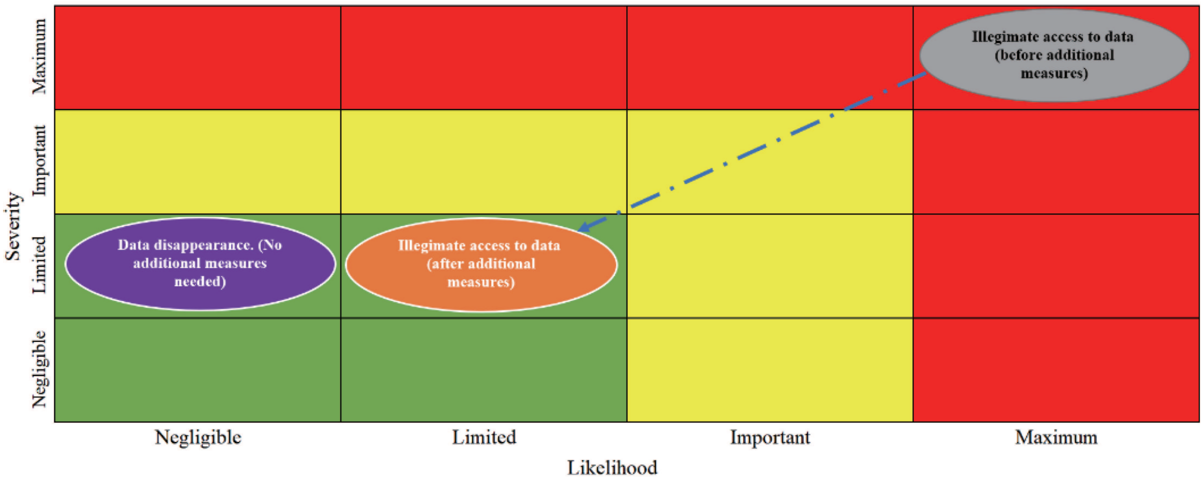

FIGURE 2. Example of risks mapping

TABLE 7. Risk mapping and example objectives

Risk mapping	Example objective
High severity and high likelihood	• Must absolutely be avoided • Must implement the measures to prevent or reduce severity and likelihood
High severity but low likelihood	• Must absolutely be avoided • Must implement the measures to prevent or reduce severity and likelihood
Low severity but high likelihood	• Must implement the measures to reduce the likelihood
Low severity and low likelihood	• Possible to take the risk

Action plan: This section of the report discusses any proposed future actions or extra measures that should be implemented. According to CNIL [6], it should contain the following details: required actions, manager, due date, difficulties, cost, and progress. Nonetheless, each action should be documented in a separate formal document and regularly monitored.

Two additional sections are required to produce a DPIA report that meets formal requirements. The first section must indicate that DPIA guidance was obtained from the DPO. In addition, it must include the DPO's signature and the date, as required by GDPR article 35(2) [5] and PDPA section 42(1) [3]. Another component must specify that the data controller consulted data subjects or their representatives regarding the intended processing of the data (GDPR Article 35(9) [5], PDPA does not include this requirement). Moreover, it requires the signatures of the data subject's authorized representatives. Nonetheless, if the data controller determines that collecting the opinions of data subjects is unnecessary, he or she must document this conclusion.

Publication of DPIA reports: A DPIA report of projects or processes should be published through the organization's public relations channel, such as its website or social media. It should help improve public transparency and confidence [1]. However, the GDPR does not require the publication of the DPIA report. It depends on the data controller and DPO to decide [4]. Therefore, the DPO should exercise caution when disclosing the system's vulnerabilities, as doing so would aid cybercriminals in attacking the system. Therefore, the DPO should consider publishing portions of the document, including an executive summary or conclusion.

4. **Summary and Outlook.** DPIA is a relatively new process for organizations in Thailand. Healthcare organizations store health information which is sensitive personal data. As a result, they must conduct a DPIA to ensure compliance with Thailand's PDPA or risk a penalty of up to 3 million baht. Furthermore, DPIA is a useful tool for identifying risks and mitigating the potential impact of data breaches. In this paper, we proposed a complete process for conducting the DPIA suitable for the healthcare industry in Thailand based on the tools from EU guidelines and PDPA.

The privacy protection literature in the EU and Thailand share a lot of familiar but still many differences in sections. Therefore, certain adaptations will become necessary when trying to apply the DPIA guideline and tools developed by the EU in Thailand, especially in the healthcare sector. The specific Thai registration has to strictly adhere because of the high sensitivity of medical data. Our paper has shown how the leading EU approach tool, DPIA, can be transformed in a way to make them useable for use in Thailand. We have also addressed the gaps which need to be covered from both sides when closely operating in the healthcare sector.

The vary benefited economic impact of ours is that whenever medical support is needed, the legal requirement from both Thailand and the EU will be met. Accordingly, technologies produced in one of those two areas can now be checked for compliance with the respective privacy registration. This will support the use of EU technologies in Thailand and Thai technologies in Europe. For companies working in both areas, a parallel check against both registrations is now considerably more accessible.

For the effectiveness of this model, our future research will also involve an experiment and evaluation of the model presented in this study in the Thai healthcare sector. Following the test, the results will be accumulated to help enhance the DPIA processes used in the healthcare industry. Additionally, we intend to apply the DPIA to various industries in Thailand. Particularly in industries without heavy use of information technology, such as agriculture and small businesses, this approach is expected to be vey helpful.

REFERENCES

[1] D. Wright, The state of the art in privacy impact assessment, *Computer Law and Security Review*, vol.28, no.1, pp.54-61, DOI: 10.1016/j.clsr.2011.11.007, 2012.

[2] European Commission, *EU Data Protection Rules*, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en, 2019.

[3] Thai Government, *Personal Data Protection Act*, http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF, 2019.

[4] WP29, *ARTICLE 29 – Data Protection Working Party*, https://ec.europa.eu/newsroom/document.cfm?doc_id=44137, 2016.

[5] EUR-Lex, Regulation (EU) 2016/679 of the European parliament and of the council, *Official Journal of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, 2019.

[6] Commission Nationale de l'Informatique et des Libertés, *Privacy Impact Assessment (PIA): Template*, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf, 2018.

[7] Office of the Privacy Commissioner New Zealand, *Privacy Impact Assessment Toolkit*, https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/, 2015.

[8] K. Vemou and M. Karyda, An evaluation framework for privacy impact assessment methods, *The 12th Mediterranean Conference on Information Systems (MCIS)*, Corfu, Greece, pp.1-5, 2018.

[9] Health Information and Quality Authority, *Privacy Impact Assessment Toolkit for Health and Social Care*, https://www.hiqa.ie/sites/default/files/2017-10/Privacy-Impact-Assessment-toolkit-A5.pdf, 2017.

[10] Canadian Institute for Health Information, *Privacy Impact Assessment Policy*, https://www.cihi.ca/sites/default/files/document/privacyimpactassessmentpolicy-en.pdf, 2019.

[11] U.S. Department of Health & Human Services, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html, 2013.

[12] Healthcare Information and Management Systems Society, *Managing Information Privacy & Security in Healthcare Privacy Impact Assessment Guide*, https://www.himss.org/files/HIMSSorg/content/files/D87_HIMSS_PIA_Guide_.pdf, 2008.

[13] European Union, *Data Protection Officer (DPO)*, https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en, 2019.

[14] European Union, *What Is a Data Controller or a Data Processor?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en, 2019.

[15] Commission Nationale de l'Informatique et des Libertés, *Privacy Impact Assessment (PIA) Methodology*, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf, 2018.

[16] F. Bieker, M. Friedewald, M. Hansen, H. Obsteller and M. Rost, A process for DPIA under the GDPR, in *Privacy Technologies and Policy. APF 2016. Lecture Notes in Computer Science*, S. Schiffner, J. Serna, D. Ikonomou and K. Rannenberg (eds.), Cham, Springer, 2016.