Health IT: A Framework for Managing Privacy Impact Assessment of Personally Identifiable Data

Cyril Onwubiko
Intelligence and Security Assurance, E-Security Group, Research Series Limited, London, UK

ABSTRACT
Health IT is the use of information technology (IT) in healthcare to improve patients' experience, enable quality care, efficiency, speed and security of the collection, exchange, sharing and storage of sensitive personal information. But Health IT faces a number of notable challenges ranging from privacy risks to trust and confidence in the use of EHRs. In this chapter, a framework for conducting privacy impact assessment (PIA) of Health IT projects is discussed. Privacy impact assessment is a process through which privacy risks are assessed and including recommendations for mitigating identified risks and ensuring compliance to policy and processes for handling and processing of highly sensitive and personally identifiable information (PII).

INTRODUCTION
In 2009 the US government signed the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act, 2009), a federal initiative that seeks to improve American health care delivery and patient care through an unprecedented investment in Health Information Technology (Health IT). Simply, Health IT is the use of IT in healthcare to improve patients' experience, enable quality care, efficiency, speed and security of personal information collection, exchange, sharing and storage. So Health IT encourages and incentivizes the use of electronic health records (EHRs) instead of paper medical records to maintain people's health information, the secure use and sharing of health information, and the use of IT to improve the quality and efficiency of care.

The goals of Health IT were pretty clear – to convince all physicians and hospitals to adopt EHRs, incentivize care service providers to adopt EHRs and to use them in ways that improves patients experience, quality and efficiency of care. But five years down the line, have these goals been realised? What have improved, and what haven't? What are perceived major drawbacks, and what could be done to improve?

The use of IT in Health to improve patients experience, improve quality of care, reduce delays in treatment, and improve healthcare standards as a whole is a welcome development and should be encouraged. Lessons learnt from other countries that currently use EHR information systems attest to impressive results, improvements in patient care experience, overall healthcare efficiency as seen with lower levels of drug error rates in Europe. For example, Denmark has the lowest rate of inappropriate medication in eight European countries (Denmark, the Netherlands, the UK, Iceland, Norway, Finland, Italy and the Czech Republic) – a 5.8 percent rate, compared to 19.8 percent in these countries on average (Lesk, 2013). Meanwhile, the US is still struggling to reduce errors. According to the 2000 National Research Council report (Grady, 2010) estimated that approximately 100,000 deaths resulted from medical errors each year; this figure has not improved over a decade later (Lesk, 2013).

Unfortunately, IT in Health comes with some challenges, especially, when use of IT in health is going to fundamentally and radically change existing healthcare practices such as use of EHRs for patient information record management, culture change in terms of electronic use, sharing and transmission of patients' information. As with any change, both patients and practitioners are going to react to this change one way or another. Similarly, the implementation and operation of Health IT in accordance to the HITECH Act are going to be challenging, too. These challenges are going to be multifaceted, including but not limited to technical, policy, interoperability, interface, privacy, security and data formatting and presentation issues. This thought is not radical, as the Office of the National Coordinator for Health Information Technology (ONC) itself had envisaged this, leading to the initiation of the Strategic Health IT Advanced Research Projects (SHARP), a program researching into, and addressing some of the perceived challenges in four specific areas – security and health information technology, patient-centered cognitive support, health care application and network design and secondary use of EHR information (Office of the National Coordinator for Health Information Technology, 2010).

According to the HITECH Act, Health IT includes hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information (HITECH Act, 2009). The adoption, building or 'migration' to EHR is going to be expensive, resource intensive, demanding and certainly challenging. Electronic health record as technology service is in itself complex, let alone policy, security, privacy and governance wrapper that are in them equally convoluted. For instance, Healthcare Trusts and Hospitals in the UK use a number of different electronic care record systems, such as EPR (Electronic Patients Record), PAS (Patient Administration System), CRS (Care Records System) etc. Compatibility between two EHR systems becomes an issue. Data format and data presentation from one system to another differs. How the same data is viewed or presented in one system is different to the other, nothing is seamless or straightforward between any two electronic health record systems. The same data is presented in different views making interpretation and understanding of health information a major concern.

The exchange, sharing and transmission of health information could span across enterprise boundaries, such as hospitals, care providers and could use technologies that traverse geographic boundaries, for example, cloud computing. This is likely to raise privacy concerns and could impact public trust and confidence, especially when it relates to personally identifiable information or personally identifiable data (PID), and when the sharing or exchange is not patient-consented. The use of networks, technologies and software that are inherently privacy-invasive, such as location-based technologies, smart cards, radio frequency identification (RFID) tags, and biometrics for health IT or for EHR systems can be a major concern.

Research surveys and polls consistently show that patients are enthusiastic about the adoption of EHRs but are equally concerned about the privacy of their digital health information. Nearly one in eight patients has withheld information from a healthcare provider due to privacy concerns (Agaku, Adisa, Ayo-Yusuf & Connolly, 2014). Failure to address these concerns could have real consequences for people's health (McGraw, 2013). Similar concerns resonate from privacy campaigners who believe patients should have a say in how their health information are shared, and who they are shared with. For example, currently in the UK, the National Health Service (NHS) initiated a Care.data project which supposed to compile a giant database of medical records showing how individuals have been cared for across the general practice (GP) and hospital sectors. According to the British Broadcasting Corporation (BBC), Care.data is believed will be shared with researchers for research purposes (BBC, 2014), and that records will be pseudo-anonymized, which means the identifiable data has been taken out. Instead, it will just contain the patient's age, gender and area they live in. Although there is provision for people to opt-out of the scheme should they wish to. The norm should have been for the initiative to have everyone

opted-out so that people can willingly opt-in should they choose to. Such canny approach does not seat well with the public, and hence erodes public trust and confidence, and could raise serious questions around the actual intents behind the NHS database programme. Is the intention really for research purposes or shared for underground citizens' surveillance? Again, with the recent episodes and revelations regarding mass citizen surveillance programmes in the US and cooperation by the UK, this is bound to raise eyebrows. No wonder it has been meant with stiff opposition and reluctance by the public. As at February 19, 2014, the NHS England Care.data project has been put on hold. The hesitation comes after polls suggested that less than half the population had heard of the scheme, concerns about the security of the data, the process for gaining consent, and data being available to commercial organisations.

To encourage public trust and confidence in Health IT, privacy risk assessment of all Heath IT components starting from HER systems and including data sharing and exchange policies and practices. This is in order that privacy risks relating to Health IT can be identified and mitigated appropriately.

Privacy impact assessment is used to assess privacy risks that may be associated with a project and to ensure that privacy legislations are not breached, and sensitive personally identifiable data are not compromised too. Privacy risk assessment is an assessment of risks associated with - failing to comply with state or federal privacy legislation - protecting personal information data of individuals, and satisfying privacy requirements of information systems, that may need to be redesigned or retro-fitted at considerable expense (Educause, 2010). This means that privacy risk assessment should be carried out on all projects, especially Health IT projects to ensure that:

1) they comply with privacy legislations or regulations;
2) they provide adequate safeguards to manage, handle, share, store or transport sensitive personal data or personally identifiable information (PII), and
3) Finally, they comply with Health IT-specific information systems' privacy requirements.

Managing privacy risks can be challenging, not because of the numerous issues of concern, but also because each project is unique and utilizes fundamentally different technologies and mechanisms to deliver its own service. While the steps involved in carrying out privacy impact assessment are the same for any project, but each assessment of privacy for any project is different. *A project* in this chapter refers to a system, programme, initiative or scheme. *A project* may involve a collection of systems that are used to deliver service for a specific purpose. For example, a census programme is a project whose aim is to count the number of lawful citizens, by checking and verifying their name, age, address and social or religious inclination, of a particular nation. This project may require the use of information communications technology (ICT) systems, people, electronic and manual processes. *An in-service* (existing) project is a programme of work that is already been delivered and in operational use. *A new project* is a programme of work that is in the initiation stage of the project lifecycle.

There are a good number of sources that provide guidelines for conducting PIAs such as (UK Information Commissioner's Office, 2009), (Educause, 2010), (Radack, 2010), (Gruteser & Grunwald, 2004), (Peirce, 2009), (Abu-Nimeh & Mead, 2001), (Privacy by Design, 2014). Unfortunately, organizations still face difficulty assessing privacy risks associated to new and existing projects. Some of the most common challenges faced by organizations include:

1) Appropriate assessment of privacy invasive technologies;
2) Justification for project;
3) Difficulty finding privacy experts within own organization;
4) Lack of appropriate guideline for tailored privacy risks assessment, and how to determine the level of privacy assessments required for a particular project.
5) Appropriate gathering and handling of personal information data and compliance to privacy regulations and legislations.

In this chapter, improvement to our contribution on managing privacy impact assessment of personally identifiable information (Onwubiko, 2011) is presented; offering guidance on how to assess privacy risks of both new and in-service projects. Further, lessons learned from managing privacy risks for new and existing projects, especially relating to Health IT, resulting from collection, aggregation, sharing, handling and transportation of sensitive personal information are discussed.

PRIVACY IMPACT ASSESSMENT

Privacy impact assessment is an assessment of privacy related risks comprising of four distinct assessments:

1. Assessment of the project's characteristics or features such as technologies or mechanisms deployed or intended of use. This assessment is to check if the technologies or mechanisms would be privacy invasive.
2. Assessment of the project's compliance with privacy regulations, state, federal, national, bilateral or multilateral privacy legislations. This relates to compliance with privacy regulations and legislations, especially those that operate where the project is located or situated. For example, the Data Protection Act 1998 in the UK or the 'the Privacy Act' in the US, or other privacy related pieces of legislations in other parts of the world, such as Canada, Australia and Germany.
3. Assessment of personal information data being processed, or to be processed by the project. For example, is personal information data collected identifiable or not; are they sensitive personal data; are they 'obsolete' personal identifiable data etc.
4. Finally, it is an assessment of the collection, sharing, distribution, storage and transportation of personal information data, and whether the processing of personal information is in line with privacy legislations. It is important to mention that PIA is not only applied to a project, but also applied to a workstream, programme, task, policy, procedure, platform or ICT System.

According to NIST's ITL Security Bulletin 2010 (Radack, 2010), PII or PID is any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (based on General Accountability Office and Office of Management and Budget definitions). A list of PII is as shown in *Table 1*.

Table 1: Personal Identifiers

S/N	Personal Identifiers	S/N	Personal Identifiers
1	Names (firstname, surname or lastname)	12	Biometric identifiers such as fingerprints, voice prints etc
2	Addresses (home, business or both)	13	Bank, Financial or Credit card details
3	Post code or Zip code	14	Mother's maiden name
4	Email address	15	Tax, Benefit or Pension records or Record numbers
5	Telephone numbers (Fax numbers)	16	Employment records
6	Driving license number	17	School attendance or records
7	Date of birth	18	Vehicle identifiers and serial numbers including license plate numbers
8	Social insurance number / National insurance number	19	Web universal resource locators (URLs)
9	Medical record numbers / Health records	20	Internet protocol (IP) address numbers
10	DNA data	21	Full face photographic images and any comparable images
11	Any other materials relating to social	22	Any other unique identifying number,

	services including child protection and housing		characteristic, or code.

> *Personal identifiers (shown in Table 1) comprise of both personal information that are in the public domain and sensitive personal data that when released is likely to cause harm or distress to the individual. These identifiers are derived from a couple of standards – HIPAA (*HIPAA (2006) *and HMG IA Standard No. 6 (*HMG IA Standard No. 6, 2009).

It is pertinent to mention that compliance with privacy legislation is dependent on where the project that is being assessed is located. For example, a project in the UK would have to comply with the UK privacy legislations and the wider European Union privacy legislations, and may comply with other privacy legislations of other countries if the organisation wishes to do so.

There are also bilateral and multilateral privacy legislations, such as the Safe Harbor Act (Directive 95/46/EC, 1995), which regulates the processing of personal data within the European Union in addition to Directive 2002/58/EC that protects privacy of electronic communications (Directive 2002/58/EC, 2002). Directive 95/46/EC is also available not only to EU member state (nations), but also, available to other countries outside the EU, which the United States (US) signed up to. Organization operating within bilateral or multilateral privacy legislation should comply with those pieces of privacy legislations. This means that a privacy impact assessment of a project operating in bilateral or multilateral privacy legislation must be equally assessed within the confinements of those bilateral or multilateral privacy agreements, and other specific privacy legislation of its own country. For example, privacy legislation compliance for a privacy impact assessment of a project in the UK would involve assessment of the project's compliance to both UK-specific privacy legislations and EU related privacy legislations.

Privacy impact assessment may seem onerous at times due to the numerous steps involved when carrying out PIA. Depending on the nature of the project, extensive privacy impact assessment maybe required. Some general purpose and useful guidelines exist such as handbook on PIA assessment (UK Information Commissioner's Office, 2009).

Our contribution in this chapter is rather unique and focused on providing a practical approach to conducting privacy impact assessment that is general-purpose and doctrinaire. The usefulness of our contribution can be seen in both the guidelines provided with respect to our Privacy Impact Suitability Assessment (PISA) Framework (see ***Figure 1***) and Privacy Screening Framework (see ***Table 4***).

In the private sector, for example, privacy impact assessments of projects are not as mandated as it is in the public or government sector. While, PIA may be conducted for certain projects based on best endeavours in the private sector, it is mandatory for all government and public sector projects as an essential risk management activity. For example, the Department of Homeland Security, National Cyber Security Division of the United States conducted privacy impact assessment of its EINSTEIN 2 Program in 2008 to examine its privacy implications with collecting, analyzing and sharing of Computer Security Information across the Federal Civilian Government (US-CERT, 2008). According to the United States Computer Emergency Readiness Team (US-CERT), the Department of Homeland Security (DHS) must provide this publicly available PIA prior to initiating a new collection of information that uses information technology to collect, maintain or disseminate information that is in an identifiable form or collects identifiable information through the use of information technology as mandated by the US, E-Government Act of 2002. Similarly, in the UK, the Information Commissioners Office (ICO), Cabinet Office has recommended privacy impact assessment for all projects, new and existing, whose functionality may require the collection, sharing or use of personal information. This was driven from the UK Data Handling Review of 2008 (Cabinet Office, 2008).

PRIVACY IMPACT SUITABILITY ASSESSMENT (PISA) FRAMEWORK

The privacy impact suitability assessment framework is our proposed framework for assessing a project's suitability for PIA assessment (see ***Figure 1***).

The PISA framework is an eight (8) step privacy assessment model, which aims to evaluate if a project is required to undergo PIA or not; and to determine the level of PIA required, where applicable. The first step (indicated by the small circle on each object) is the start of the PIA assessment. The second step is the scene setting assessment (a.k.a. stage 1 PIA). At this stage, the project is initially assessed as to whether personal information data will be processed by the project. For existing projects, the scene setting assessment will check if information being processed by the project involves personal information data. The third step is when a decision is reached whether the project should or should not undergo a stage 2 PIA assessment. If the outcome shows that personal information data is not being or will not be processed, then PIA is completed (step 8) and that concludes privacy impact assessment for that project. If otherwise, then the fourth step begins. The fourth step is the stage 2 PIA.

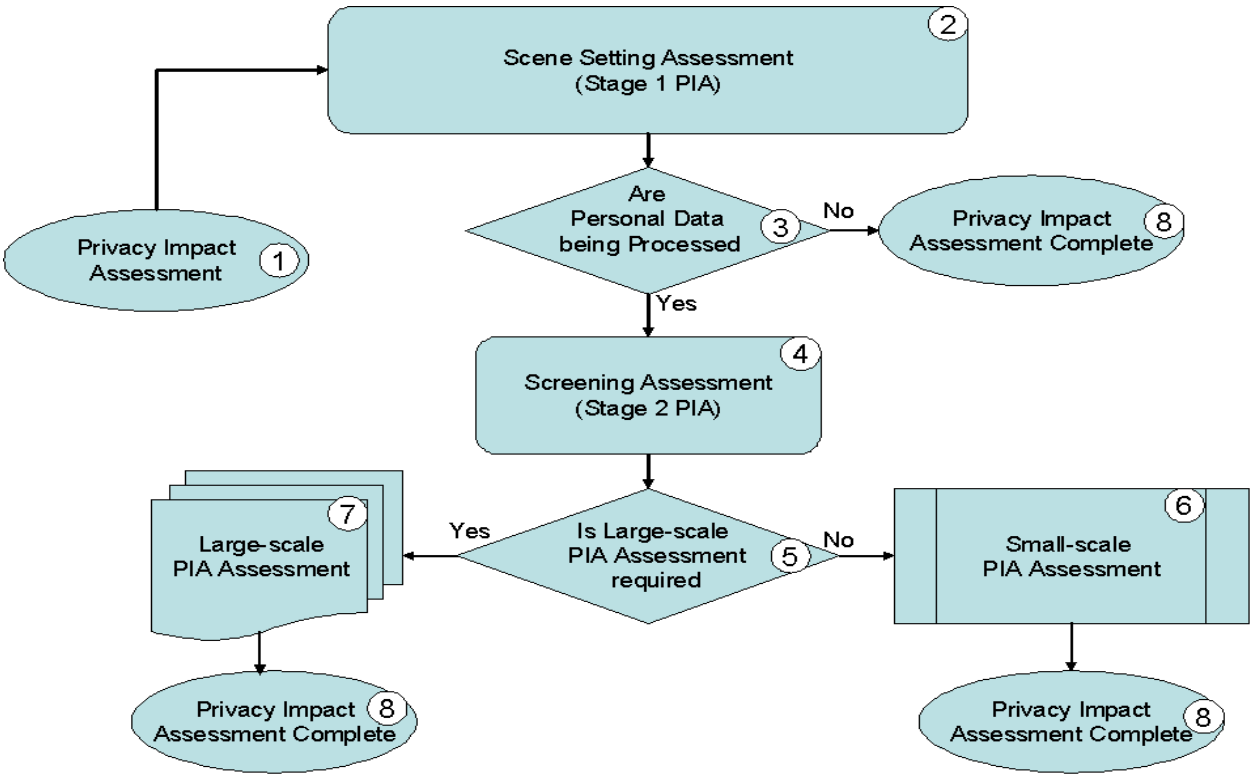

Figure 1: PISA Framework – Privacy Impact Suitability Assessment Framework (Onwubiko, 2011)

The second stage PIA (Stage 2 PIA) starts with the screening exercise when privacy risks of the project are assessed in much more detail than stage 1. This involves assessing the project's characteristics, such as technologies or mechanisms that will be deployed in the project, for example, checking if such technologies are privacy invasive. It also assesses the type of personal data that will be collected, and to ensure the people providing these data are aware and willing. In addition, it assesses if there is good justification for the project. The fifth step is when a decision is reached as to whether small-scale PIA or large-scale PIA is pertinent for the project. The sixth step involves carrying out large-scale or small-scale PIA, and finally, the seventh step completes the assessment. Since every project should be assessed of privacy risk, we thought the framework is a foundational contribution, which assist privacy experts and organization conduct, in a practical way, a privacy assessment of their projects.

Scene Setting Assessment (Stage 1 PIA)

The scene setting assessment (SSA) is the first stage PIA of a project. It is aimed to ascertain if the project will process personal information data, or already processes personal information data. This is applicable to existing project (see ***Figure 1***). To conduct a scene setting PIA assessment of a project, we have designed ten (10) fundamental scene setting questions to help with the assessment in order to deduce the suitability or appropriateness of privacy impact assessment of the project, as shown in ***Table 2***.

Table 2: Privacy Scene Setting Assessment

Privacy Scene-Setting Assessment		
PD	**Project Details**	**Response**
PD1	Project Name:	
PD2	Country of Project Location:	
PD3	Project Reference:	
PD4	Project Registration Type:	
PD5	Project Owner:	
PD6	Assessor Name:	
PD7	Assessor Email Address:	
PD8	Assessor Expertise:	
PD9	Assessment Date:	
SSA	**Scene Setting Assessment**	**Response**
SSA1	Would the project consume, process, transport or store personal information data?	
SSA2	What personal information data would the project process?	
SSA3	Why is personal information collected by the project?	
SSA4	What is the intended use of personal information data being collected by the project?	
SSA5	How would personal information data be processed, this includes sharing, transporting, exchanging, storing and disposing of personal information?	
SSA6	Is the organisation that owns the project an authorised Data Controller?	
SSA7	Is the organisation that owns the project an authorised Data Processor?	
SSA8	With whom will personal information be shared, or/and exchanged?	
SSA9	How are service consumers consent obtained?	
SSA10	How will service consumers informed of the justification for the project?	
SSA11	How will personal information data at rest secured?	
SSA12	How will personal information data secured on transit?	
SSA13	Select applicable legislation for the project	
SSA14	What privacy regulations apply or are required for the project?	

Based on the outcome of this assessment (answers to questions on ***Table 2***), a decision should be made, either to proceed, or stop further privacy impact assessment. If it is believed that the project will be used to process personal information data, then further PIA assessments are recommended, otherwise this concludes PIA assessment of the project. Suppose the outcome of the scene setting assessment turns out

that the project is handling personal information data. This implies that a second stage PIA (screening assessment), which is a much more thorough assessment than the scene setting assessment, will be required. It is pertinent to mention that, the first stage PIA is mandatory for all projects.

Screening Assessment (Stage 2 PIA)

The second stage PIA is referred to as the screening assessment, during which project stakeholders are interviewed to determine the level of personal data the project intends to process, or has been processing, this is applicable to existing projects (see ***Figure 1***).

The aim of the screening assessment is to determine whether a small-scale or large-scale PIA is deemed necessary for the project. A small-scale privacy impact assessment is an abridged privacy risks assessment of a project. It is recommended when a small percentage of the project characteristics underline some privacy concerns. For example, if one or two features of the project characteristics imply privacy concern, then it is justifiable to recommend a small-scale PIA assessment. If more than three aspects of the project characteristics underline privacy concerns, then a large-scale PIA is justifiable. Having said that, there are cases when a small-scale PIA is recommended even a number of a project features seems to underline privacy concerns.

For example, if it is perceived that personal data being processed are either none sensitive or the processing is infrequent. None sensitive personal data refers to personal data of a living individual that can only identify an individual when linked or combined with other personal data of that individual. For example, an email server project that collects only two sets of personal data during user registration such as name and email address of the user would justify a small-scale PIA, even though it aggregate significant volumes of personal information data. A large-scale PIA assessment is an extensive, thorough, and detailed privacy risks assessment. A large-scale PIA assessment is recommended when a good percentage of the project characteristics evaluated during a screening exercise underlines serious privacy concerns. For example, a data consolidation project of a health service that links data controllers or sources warrants large-scale privacy risks assessment. Both small-scale and large-scale privacy impact assessments require project stakeholders to be interviewed in order to determine the areas of the project that involve processing of personal information data, and the level of analysis or manipulation (source linkages) of personal data that are intended.

There is no empirical method of deciding which projects should undergo large-scale or small-scale privacy impact assessment. One approach that has been recommended to determining the level of assessment required for a project is the use of screening questions (Information Commissioner's Office 2009) developed by the ICO. The ICO's proposed screening process is extremely helpful; unfortunately, the screening process does not guarantee that the same project when assessed by two separate organisations would lead to the same level of PIA recommendations. For this reason, proposed the Privacy Screening Framework (see ***Table 4***), in addition, we designed a general purpose legal and privacy assessment questions (see ***Table 3***) to assist organizations assess legal and privacy compliance of projects during PIA assessments.

Table 3: Legal & Privacy Compliance Check

Legal & Compliance Assessment		
PD	Project Details	
PD1	Project Name:	
PD2	Country of Project Location:	
PD3	Project Reference:	
PD4	Project Registration Type:	

PD5	Project Owner:	
PD6	Assessor Name:	
PD7	Assessor Email Address:	
PD8	Assessor Expertise:	
PD9	Assessment Date:	
GPC	General Privacy Clauses	Response
GPC1	Is the project compliant with all relevant regulation/directives	
GPC2	Are the business processes to be used (or been used) for the project compliant with all relevant regulation/directives	
GPC3	Are there legal compliance that this project must satisfy?	
GPC4	Are there standards and law that this project must comply?	
GPC5	Are there privacy related compliances stemming from a code of connection or code of interconnection contract?	
GPC6	Are there privacy related compliance arising from corporate/statutory privacy policy?	
GPC7	Are there specific privacy requirements or compliance arising from service consumers that must be satisfied?	
GPC8	Are there privacy related mandates from the Public that this project must satisfy?	
GPC9	Is the project, the processes of the project or the personal data collected compliant with Public Health requirements?	
GPC10	Is this project compliant with the Health Insurance Portability and Accountability Act (HIPAA)	
GPC11	Will personal data be shared or transport outside the Country of Origin?	
GPC12	Will personal data be shared or transport outside the Province of Origin but consumed within the Country of Origin?	
UK	Country Specific Directives	Response
UK1	Is the project compliant with the Data Protection Act 1998?	
UK2	Is the project, the personal data that it handles, and its business activities compliant with the Data Protection Principles (1-8)?	
UK3	Freedom of Information Act, 2000	
UK4	Is the project compliant with the Privacy and Electronic Communications Regulations 2003?	
UK5	Is the project compliant with the Freedom of Information Act 2000?	
UK6	Is the project compliant with the Privacy Act 1974?	
UK7	Is the project compliant with the EU Directive 2002/58 EC on Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector?	
UK8	Is the project compliant with the EU Directive 95/46 EC on the processing of personal data and on the free movement of such data	
UK9	Freedom of Information and Protection of Privacy Act (FIPPA)	
UK10	Is the project compliant with the Human Rights Act 1998?	

Table 3 consists of twelve (12) questions comprising legal, regulatory and legislative assessment of personal data handling, processing and sharing. The idea behind the provision of the legal and privacy compliance check is to ensure that PIA assessments are consistently evaluated by each organization by

following the same prescriptive guideline. As seen in the table, there are ten (10) UK-specific directives that are also listed. The reason behind this is to include country-specific directive, so that dependent on where the project is located, assessment of country-specific directives are also assessed. In our future work, we hope to include country-specific privacy directives in the model.

After carrying out legal and privacy compliance checks of a project, the next activity in the PIA assessment is the privacy screening assessment.

PRIVACY SCREENING FRAMEWORK (PSF)

The privacy screening framework is our proposed framework that provides the required prescriptive guidance for carrying out large-scale PIA assessments. The PSF framework is flexible, adaptable and self-directing. It is flexible because the PIA assessor can choose to add or remove any non-applicable sections of the framework without influencing the end result of the assessment.

PSF is adaptable and self-directing because the PIA assessor is required to carry out the assessment, and can modify any sections of the framework that is deemed not applicable to the project's locality or operating environment (see Table 4). For example, when conducting a PIA assessment of a project in the UK, it may not be relevant to evaluate the project based on US-specific privacy legislations except where bilateral mandates are applicable. Similarly, privacy risk assessment of US-based projects should be evaluated against US-specific privacy legislations and applicable industry regulations, plus bilateral or multilateral privacy understandings, where applicable. Thus, it is equally the case with privacy risk assessment of project hosted in other EU countries such as Belgium, Germany or France.

The privacy screening framework is composed of eight (8) sections containing over 185 assessment questions. Each section contains over three subsections, and each subsection contains questions which are crafted to assessing in details the various aspects of the project privacy clauses, practices and policies, such as the data exchange policy, information sharing practices and data handling and storage requirements and principles.

Section 1 is about the project details, comprising project name, reference, organization, asset owner and name of PIA assessor. Section 2 is technology assessment, which focuses primarily on privacy risk assessment of three main areas – privacy-invasive technologies, event and information monitoring technologies, and data capturing and screening technologies. Section 3 is project justification assessment. It is aimed to ensure that the purpose and justification of the project are made known to the public or the users of the system. It has two subcategories – justification for data handling and justification for new data acquisition. Section 4 is identity assessment, which focuses on privacy risks associated to the use, combination and linkage of personal identifiers, such as username, date of birth, national insurance number etc. (see *Table 1*).

Section 5 is data assessment. This assesses the quantity and significance of personal data being processed (used, stored or transported). Section 6 is data handling assessment, which focuses on privacy risks associated with data collection policies, procedures and quality assurance. Section 7 is awareness assessment. It deals with privacy risks associated with the security of the information system processing personal information data for the project; in addition, it deals with secure disposal and destruction of the information system holding personal information data, when no longer in use. Finally, section 8 is miscellaneous, which affords the risk assessor the opportunity to profile other pertinent privacy risks particular to systems utilized for the project. For example, privacy concerns with legacy systems, bespoke design and customized solutions etc.

Table 4: Privacy Screening Framework (PSF)

High Level Privacy Impact Assessment		
1	Project Details	Response
PD1	Project Name:	
PD2	Project Reference:	
PD3	Country of Project Location:	
PD4	Project Registration Type:	
PD5	Project Owner:	
PD6	Assessor Name:	
PD7	Assessor Email Address:	
PD8	Assessor Expertise:	
PD9	Assessment Date:	
2	Technology Privacy Risk Assessment	
2a	Privacy-invasive technologies	Response
2a1	Please select technologies being deployed or in use by the project.	
2a2	Does the project use RFID or plan to deploy RFID (Radio frequency identification)?	
2a3	What is RFID used for? For example, tracking users, tracking people etc.	
2a4	Does the project use biometric technology (biometrics) or plan to deploy biometrics?	
2a5	What is biometrics used for in the project? For example, authentication, authorisation, tracking, gatekeeper etc.	
2a6	Are all technologies applied to the project well-understood by the organisation?	
2a7	Are all technologies applied to the project well-understood by the service consumers?	
2a8	Does the project use locator monitoring technologies or plan to deploy locator monitoring technologies, such as GIS, GPRS etc.?	
2a9	Which locator monitoring technology is in use or planned for use?	
2a10	What locator monitoring technologies used for in the project? For example, tracking users, tracking equipment, tracking both users and their actions	
2a11	Are there demonstrable concerns that the technologies used in the project may impact privacy	
2a12	Does the project use visual surveillance for its operation?	
2a13	Which visual surveillance tools are in use?	
2a14	What are the visual surveillance tools used for? For example, monitor people, monitor intruders, monitor both users and intruders, track object movement and interactions	
2a15	Are the privacy impacts (from the project) well-understood by the organisation, and by the service consumers	
2a16	Are there measures applied to avoid or mitigate negative privacy impacts, or at least reduce them to satisfactory levels of those whose privacy is affected	
2a17	What measure/controls are in place to address privacy concerns?	

2b	Event and information monitoring technologies	Response
2b1	Does the project involve the use of event and information monitoring technologies such as SEIM, SEM and SIM such that user traffic, user actions and user locations can be monitored	
2b2	Are SIEMS used to track user activities and interactions	
2b3	Are cookies being monitored and used in various ways users are not aware of, and their consent not sort?	
2b4	Are service consumers' activities logged?	
2b5	For what purpose are service consumers' activities logged?	
2b6	How long are logs retained?	
2b7	Are the organisation and service consumers aware that their traffic are being monitored	
2b8	Is the use of the SEIM/SEM/SIM due to regulatory compliance?	
2b9	What regulatory compliance does the use of SIEM/SEM/SIM fulfil?	
2b10	If service consumer data are collected, are they subject to reprocessing that could lead to the identification of individuals	
2c	Data capturing and screening technologies	Response
2c1	Does the project involve the use of data capturing, admission and screening technologies such as Biometrics, RFID, Blood sampling toolkit, Lab equipment, X-ray and digital imagery, data monitors (wireshark) such that user identifiable attributes, characteristics and features are monitored, captured or/and stored	
2c2	Which data capturing, admission, screening or registration technologies are in use?	
2c3	Are blood sampling toolkits used or will be used for the project?	
2c4	Are X-ray and digital imagery equipment in use?	
2c5	Is a medical monitor, such as heart monitors, pacemaker, or LCD implantation toolkits in use?	
2c6	Which traffic and data monitoring devices are in use?	
2c7	Which user registration equipment are in use?	
2c8	Is the use of the data capturing and screening tools due to regulatory compliance, if yes, please specify	
2c9	Which regulatory compliance mandates or recommends the use of data capturing and screening device?	
2c10	Are the organisation and service consumers aware that user traffic are monitored?	
2d	Cloud-based technologies	Response
2d1	Does the project use or intend to use Cloud-based services?	
2d2	What type of Cloud is used or will be used?	
2d3	Which Cloud delivery model is in use or may be used?	
2d4	Who is the Cloud Provider?	
2d5	Is the Cloud Provider Local, Provincial or International?	
2d6	What controls are offered to assets in the Cloud by Provider?	
2d7	Is the Cloud Provider an authorised Data Processor?	
2d8	Is the Cloud Provider an authorised Data Controller?	
2d9	Is the Cloud Provider compliant to DPA, Privacy Act or EU Directives 95/46 EC or EU Directive 2002/58 EC?	
2d10	Is the Cloud Provider's Data Centres local, overseas or both?	

3	Project Privacy Risk Justification	
3a	Privacy notices	Response
3a1	Is there an appropriate privacy notice outlining the legitimate reasons/intention for processing of personal information?	
3a2	What does the privacy notice include?	
3a3	Are service consumers aware or informed as to why their personal data are being collected?	
3a4	Is there a process in place to ensure privacy notice is provided prior to data collection to all intended service consumers?	
3a5	Is personal data/information collected through a 3rd-party for the project. That is, is data collection process outsourced via a 3rd-party?	
3a6	Is privacy notice communicated to service consumers about the use of 3rd-party data collector/processors?	
3a7	Is the 3rd-party collecting the data local, offshore, near offshore	
3a8	Where is the 3rd-party organisation located?	
3a9	Is the 3rd-party organisation a registered and authorised data collector or data processor?	
3a10	How is privacy notice communicated to service consumers?	
3a11	If user consent is required, how does the project seek to obtain this?	
3a12	Is personal data collected being used for the purposes outlined in the original privacy notice?	
3b	Justification for data handling	Response
3b1	Is there justification to why personal data are collected or processed?	
3b2	What justification exists for the collection and further processing of each type of personal information?	
3b3	Are service consumers aware or informed as to why their personal data are being collected?	
3b4	How did service consumers get to know about the benefits of the project for them or society?	
3b5	Is the project a government project, such as a national census project	
3b6	Do service consumers understand the benefits of the project to them or society?	
3c	Justification for new data acquisition	Response
3c1	Is the acquisition of new personal data required?	
3c2	Why is new data required?	
3c3	Will the new pieces of data collected be combined with existing data	
3c4	What new set of data or identify are or will be acquired?	
3c5	Do service consumers understand the benefits of the extra data supplied in the overall assessment of the project	
4	Identity Privacy Risk Assessment	
4a	Intrusive or onerous use of new or substantially changed identity authentication requirements	Response
4a1	Will the enrolment or registration process require new identifiers to existing ones?	
4a2	Will the registration or enrolment process of the service requires three or more personal identifiable information such as (Name, Address, NI, DoB, SIN, email, Mother's Maiden name etc.)	

4a3	Will the authentication process of the service requires the use of new identifiers?	
4a4	Please, select the identifiers used?	
4a5	Will the project cache or store personal identifiable information of the service consumer during registration	
4a6	Does the enrolment or registration process require two or more processes (for example, collection of basic personal details and onerous PII details)	
4b	Use of a new identifier for multiple purposes	Response
4b1	Will the project require a new ID (such as, username, DoB, eye colour, address, NI etc.) and would this new ID be combined with existing IDs	
4b2	Will the new ID be combined with existing IDs?	
4b3	Will an ID be used for multiple purposes such as used for registration, authentication and identification or service improvement contact	
4b4	How many identifiers are used in total for registration or authentication of service consumers?	
4c	Additional use of an existing identifier	Response
4c1	Will the project make use of a combination of existing IDs (example, username, DoB, year, address etc.) in its processing or analysis	
4c2	How many identifiers are required?	
4c3	How many identifiers are combined?	
4c4	Please, select the identifiers used?	
4c5	Please, select identifiers that are combined?	
5	Data Privacy Risk Assessment	
5a	Sensitive and personally identifiable data (PID/PII)	Response
5a1	Will sensitive or personally identifiable data be collected and further processed?	
5a2	Please, select sensitive or personally identifiable data that would be collected and processed by the project	
5a3	What are the reasons for collection and further processing of sensitive personal information?	
5a4	Will data collected for other purposes used in this project?	
5a5	Will the project use or combine personal data collected for other uses with those collected during service registration/enrolment?	
5a6	Will the project involve significant change in data linkages / data sources	
5b	Linkage of personal data with data in other collections, or significant change in data linkages	Response
5b1	How many data linkages or data sources (transfer, consolidation or storage) of personal data are in use	
5b2	Will data collected for other purposes be used in this project	
5b3	Will the project use or combine personal data collected for other uses with those collected during service registration/enrolment or privacy notice?	
5b4	Will the project involve significant change in data linkages / data sources	
5b5	Will the project involve significant change in data linkages / data sources	

5c	Handling of a significant amount of new data about each person, or significant change in existing data-holdings	Response
5c1	What is the estimated number of users who may use this system?	
5c2	What set or combination of user data are required during user registration/enrolment?	
5c3	Will the project result in the handling of a significant amount of new data about people such as Name, address, DoB, NI, Mother's maiden name etc.	
5c4	Will the project result in the handling of a significant change in existing data-holdings	
5c5	Will the project combine both new and existing personal data	
5d	Handling of new data about a significant number of people, or a significant change in the population coverage	Response
5d1	Will the project result in the handling of new data about a significant number of service consumers	
5d2	What is the number of service consumers required to use the service?	
5d3	Will the project result in a significant change in the population coverage	
5d4	What population coverage is anticipated	
6	Data Handling, Processing, Protection & Mobility Privacy Risk Assessment	
6a	Compliance	Response
6a1	Is the project or organisation a registered Data Controller?	
6a2	Is the project or organisation a registered Data Processor?	
6a3	Is the project, programme or organisation register as data controller or data custodians in accordance with prevailing laws/directives?	
6a4	Does the project or the organisation have a privacy policy?	
6a5	Does the project have privacy policy statement?	
6a6	Does the project have a privacy notice statement for services offered by the project?	
6a7	Does the project or organisation have a data protection policy?	
6a8	Will the project have a privacy impact assessment policy or procedure?	
6b	Data collection policies or practices	Response
6a1	Does the project involve new data collection policies that may be unclear or intrusive to service consumers	
6a2	Does the project require the modification of existing data collection policies that may be unclear or intrusive to service consumers	
6a3	Does the project involve new data collection practices or procedures that nay be unclear or intrusive to service consumers	
6a4	Does the project require the modification of existing data collection processes or procedures that may be unclear or intrusive to service consumers	
6a5	Are there mandatory learning and training courses for service providers and developers that are tailored for data protection and privacy controls and guidelines	
6c	Data quality assurance processes or standards	Response
6c1	Does the project have a data quality process or procedure?	

6c2	Are users aware of the quality assurance procedures of the project?	
6c3	Will the project use a new data quality processes or procedures that may be fundamentally different from existing data quality procedures?	
6c4	Will service consumers or users be notified of the new, or changes in data quality procedure?	
6c5	When was the data quality procedure changed?	
6c6	When will the new data quality procedure be implemented /deployed?	
6d	Data security arrangements, practices and processes	Response
6d1	Does the project have a data security process or procedure?	
6d2	Are service consumers/users aware of the security assurance procedure of the project?	
6d3	Will the project use a new data security processes or procedures that may be fundamentally different from existing data quality procedures?	
6d4	What data security controls are in place for the project?	
6d5	Does the project use changed data security arrangement processes or procedures that may be unclear or intrusive to service consumers?	
6d6	When was the data security procedure changed?	
6d7	When will the new data security procedure be implemented /deployed?	
6e	Data access or disclosure arrangements, processes and practices	Response
6e1	Does the project or organisation have a data access and disclosure policy or process?	
6e2	Is there a subject access request policy?	
6e3	Does the project comply or will comply with subject access request?	
6e4	Does the project use existing data access or disclosure process that may be unclear or intrusive to service consumers?	
6e5	How often is existing data access or disclosure process reviewed?	
6e6	Does the project use new data access or disclosure process that may be unclear or intrusive to service consumers?	
6e7	When was the new data access or disclosure process deployed or signed-off?	
6e8	Are service consumers aware of, and agreed to, the new data access or disclosure process?	
6f	Data retention arrangements, practices and processes	Response
6f1	Does the project or organisation have a data retention policy?	
6f2	When was the data retention process or policy signed-off?	
6f3	Does the data retention periods stipulated in the policy compliant with data protection principles?	
6f4	Is the existing data retention policy unclear or noncompliant with the Data Protection Principles?	
6f5	Is there an aspiration to change the existing data retention policy or process?	
6f6	Why would the existing data retention policy/process been changed?	
6f7	When will the new data retention process/policy be signed-off?	
6f8	Who signs off the data retention policy?	
6g	Disclosure for publicly available information	Response
6g1	Does the project have a publicly accessible portal	
6g2	What sort of information would the portal hold about service	Name

	consumers?	
6g3	Does the portal correlate or collate a set of personal information data, such as name, address, and user activities?	
6g4	Will the project make publicly available piece of personal information data readily accessible. For example, use of public Internet website that organize and aggregate personal information data, such as data mining?	
6g5	Who will have access to publicly available personal data from the portal?	
6h	Data Sharing	Response
6h1	Does the project share personal data with another organisation, institution or 3rd parties?	
6h2	Is personal data shared for commercial gain? For example marketing?	
6h3	Are service consumers aware of, and agreed to, the sharing of data with another entity?	
6h4	How is the data shared?	
6i	Data mobility	Response
6i1	Does the project plan to send personal data to jurisdictions outside the EEA (EU, Iceland, Norway, and Liechtenstein)?	
6i2	Has the jurisdiction that the project is transferring the information to been assessed as "Adequate"	
6i3	Is personal data transferred to America to a company that signs up the Safe Harbor act?	
6i4	Which jurisdiction or country is data sent to?	
6i5	Is the project using any Cloud delivery mechanism or cloud type to transfer personal data?	
6i6	Which mechanisms are used to share or move personal data around?	
6j	Hosting	Response
6j1	Is the project outsourced to a provider outside of the organisation?	
6j2	Is any component of the project hosted overseas, offshore or near offshore?	
6j3	Is the outsourcee or 3rd-party organisation a Cloud Provider?	
6j4	Which jurisdiction or country is the outsourcee located?	
6j5	Is the project using any Cloud delivery mechanism or cloud type?	
6j6	Which Cloud delivery type is used?	
7	Data Archive Privacy Risk Assessment	
7a	Data archival policies, practices and processes	Response
7a1	Does the project have a data archive policy or process?	
7a2	How long is personal data being archived	
7a3	Are data archived online or offline	
7a4	Will archived data be used for other purposes except for its original intentions	
7a5	What additional purposes would archived data serve?	
8	Assessing Privacy Risk resulting from Decommissioning	
8a	Secure sanitisation	Response
8a1	Does the project or organisation have a decommissioning and secure disposal policy?	
8a2	Has any system components of the project been decommissioned, re-	

	used or destroyed?	
8a3	Which system components of the project have ben decommissioned either for re-use, upgrade or destruction?	
8a4	Are systems sanitized before re-use?	
8a6	For systems re-use, have personal data stored on the system being securely destroyed such that their re-construction is impossible?	
8a5	How are the systems/components sanitised?	
8a7	How are paper-based assets containing personal data destroyed?	
9	Privacy Risks Business Impact Assessment	
9a	Vulnerability	Response
9a1	Are the public aware of the project?	
9a2	Is the project under any competition?	
9a3	Are the system components of the project located in vulnerable sites? For example, offshore premises, near offshore locations	
9a4	Will the project (portal) be accessible from vulnerable environment?	
10	Others	
	Please provide any comments you think may assist with the privacy risk assessment of the project or platform being evaluated.	

Privacy Impact Assessment of an In-Service Project

A project is said to be in-service when it is already being used to delivery a type of service or another. In every aspect, it means the project has gone live. There are five phases to any project lifecycle: initiation phase, development phase, test phase, in-service phase, and decommission phase. Privacy impact assessment of an in-service project is the retrospective privacy risk assessment of a project that is already being used to deliver a service. This means that risk assessment of the project was previously completed only on the basis of business and security requirements, without prior assessment of privacy risks associated with the project.

Privacy impact assessment of an existing project is the retrospective assessment of privacy risks associated to that project. First, privacy assessment suitability of the project should be established as shown in ***Figure 1***. Second, privacy risks relating to technologies or mechanisms deployed in the project, data collection and handling procedures applied (see Privacy Screening Framework - ***Table 4***), and compliance to privacy legislations and regulations (see ***Table 3***) should be evaluated. Finally, specific project privacy requirements should be addressed.

Assessing privacy risks of an existing (in-service) project can be challenging, while the outcome is often astonishing and expensive, because of the following:

1. Asset owners and senior information risk owners do not have a clue how damaging results from such assessments may turn up.
2. Outcome could imply privacy violation or breach.
3. Outcome could show that certain technologies are privacy intrusive or that the data collection and handling procedures contravene privacy regulations or legislations. This may lead to such technologies being decommissioned from the project, consequently resulting to significant financial losses to the organization.
4. Outcome could be costly because the result may mean that certain assets in the project may have to be decommissioned, withdrawn or destroyed. It could also result in significant financial penalties such as fines due to breach of privacy. For example, in August 2010, the UK Government's Financial Services Authority (FSA) fined Zurich Insurance record data loss fine of

£2.3M due to a breach on privacy (Shane, 2010). There are a number of cases of huge financial penalties being hit on organisations due to privacy breaches, and such breaches are now starting to be publicly disclosed as Government takes new stances to ensure organisations take privacy seriously.

To conduct privacy impact assessment of an existing project we recommend a quick assessment using our privacy impact assessment questionnaire (see ***Table 2***). This assessment is meant to show if PIA is indeed relevant to the project or not. Based on the outcome of this assessment, further privacy assessments of the project will be decided. It is pertinent to mention that privacy impact assessment of in-service projects follow the same methodology as new projects (see ***Figure 1***). This means that, first, privacy suitability assessment of the project (Stage 1 PIA). Second, based on the outcome of the Stage 1 PIA assessment, Stage 2 PIA will commence; otherwise the assessment is concluded. Following the second stage PIA, two sets of assessment is envisaged, either a small-scale or a large scale PIA assessment.

It is pertinent to re-iterate that the outcome of privacy impact assessment of an existing project can be insightful and expensive. We recommended organisations to consider conducting PIA as early as possible in the project lifecycle to minimize the consequences associated with in-service PIA. For example, PIA of an existing project could reveal that an organisation is in breach of privacy because of the use of technologies that are intrusive in the processing of personal information data. In another case, it may reveal that an organization does not comply with certain privacy regulations or legislations. Either case, the impact it will have on the organization is huge. For instance, it could lead to significant financial penalties, withdrawn accreditation, or/and subsequent termination of the project. In a normal circumstance, breach of privacy attracts a fine and requires fresh risk assessment of the project, which costs both time and money. In an extreme case, it will lead to significant financial penalty (as a result of breach of customer service agreement and resultant fine from the government), affects the organisation brand (negative media publicity), and especially in situations where disclosure of security or privacy breaches are required due to regional or provincial legislation. Finally, it may lead to termination of the project.

Privacy Impact Assessment of a New Project

With new projects it is recommended that privacy requirements are assessed from the outset and consideration to these requirements are made prior to implementation. This does not mean that privacy impact assessment of new projects is a panacea to all privacy concerns. As shown in ***Table 5***, the difficulty to carrying out privacy impact assessment of new projects are that at the early stages of a project, very little is known of the various components of the project. For example, the entire design of the project may not have been fully developed. Stakeholders may not fully understand all the requirements of the project and detailed functional features of all the technological mechanisms to be deployed in the project may not have been known. Hence, privacy assessment of all the various components of the project, at this stage, is not feasible.

New projects afford an organization the opportunity to consider privacy requirements from the outset. As set out by local, national and international privacy agencies, privacy impact assessment is one way of ensuring that privacy concerns are addressed from the start of project initiation to the entire lifecycle risk management of the project. The fact that a project is new does not make privacy impact assessment of that project any easier compared to PIA assessment of an in-service project. As shown in ***Figure 1***, the same framework is utilized to assess both new and existing projects.

A major concern observed with most privacy impact assessments is that organisations do not often have the right mix of privacy skilled experts to carry out privacy impact assessments. Often, people with limited privacy expertise from varying but related disciplines such as information assurance, information security or information technology are asked to carryout privacy impact assessments. Our

recommendation for organisations is to enlist the service of privacy experts to assist with PIA exercise, especially when large-scale PIA is recommended. A lesson learned from carrying out privacy impact assessments is that interpretation of privacy requirements does so often differ among stakeholders.

Table 5 provides some comparisons between PIA of new and existing projects. It is evident that there are issues that are common to both new and existing projects, such as compliance to privacy legislations and regulations. Nevertheless, there are issues that fall under one category but not the other. For example, privacy impact assessment of existing projects may require retrofitting of privacy, or risk acceptance of privacy non-compliant practices; whereas, for new projects, privacy considerations are recommended from the outset, hence retrofitting of privacy requirements are not applicable.

Table 5: A Comparison of Privacy Impact Assessment of Existing and New Projects

Specific Issues to New and Existing Projects		
S/N	**New Project**	**Existing Project**
1	At the early stages of the project initiation phase, functional requirements of the different components of the project may not be known and well understood, hence privacy impact assessment of the project at this stage may be inconclusive.	Functional requirements are known, but the realisation that the project maybe combining multiple personal information identifiers may not have been considered.
2	Often, all the technologies, or mechanisms to be used in the project may not be properly identified, hence privacy assessment relating to technology or mechanism, or even the design cannot be properly evaluated.	Because the project is already in-service, even when privacy risks are identified, addressing all the identified risks may impact service, hence business needs often override privacy requirements.
3	Ownership of risk may become an issue, especially when information security roles and responsibilities have not been defined and agreed on.	Ownership of risk is also an issue with existing projects, especially when prior privacy risks have not been conducted.
4	Expertise in conducting privacy impact assessment for new projects within a single organisation (for example, small to medium-size organisation) is a challenge.	Expertise in conducting privacy impact assessment is also a challenge for existing projects, because: a) Skills to do so may not exist within one organisation, and, b) Expertise to assess existing projects, and manage relationships and interfaces that exist with in-service project can be onerous.
5	The scope or extent to which personal information to be collected will be processed (shared, stored, combined, exchanged) may not be known and well understood.	Where privacy impact assessment may reveal a high likelihood of privacy violation, business needs may override privacy requirements, especially if addressing privacy issues may result to service impacting consequences or significant financial expense.
6	The extent to which different personal information identifiers may be combined, processed or analysed may not be fully determined.	There may be a bias to suppress privacy risk in relation to business needs since privacy impact assessment was carried out retrospectively.
7	The justification of the project to service	The justification for existing projects are known,

	consumers (users of the systems, public or citizen) may not have been discussed or communicated to the public or wider service consumers.	but the use of additional personal identifiers may have not been justified for existing projects, and when there is a scope change to existing project, this is not often communicated to the service consumers.

Risk relating to Aggregation of Personal Identifiable Data

Personally identifiable information (PII) requires special handling/processing procedures in accordance to the Data Protection Act (DPA) Principles 1-8, the Privacy Act and other national and international privacy legislations. This is because the impact of privacy breaches to an individual, which could vary from prolonged personal distress to significant personal financial losses. Unfortunately, privacy breach of a project collecting PII data of citizens will impact a larger population of individuals, resulting to prolong distress to a population of individuals. The cumulative and interdependent risks resulting from the collection of significant number of aligned sensitive personal information data require proportionate risk mitigation procedures, and additional controls may seem plausible to address risk resulting from aggregation of these PII data. When carrying privacy impact assessment of a project, it is worth taking into consideration (at stage 2 of the PIA assessment) whether personal data from numerous data collectors or sources will be aggregated. That is when a significant number of personally identifiable information is collected or combined proportionate privacy-assurance controls should be required. For example, additional storage, processing and handling requirements may be needed.

Personally identifiable information requires special handling, sharing, storage and retention procedures. While these procedures are essential to protecting PIIs, additional handling and sharing procedures may be required if a significant amount of personal data is required. Further, if these information would be handled in new ways or ways that involved new linkages of personal data, additional controls should be used to address risks resulting from this new practice.

Solutions and Recommendations

In this chapter guidance to conducting privacy impact assessment of both new and in-service projects are provided. Fundamentally, the Privacy Impact Suitability Assessment (PISA) framework is provided to enable organisations successfully carry out privacy impact assessment, knowing that every project should be assessed for privacy risks. The PISA framework is useful and straightforward to use and apply to any project with respect to privacy risks assessments.

To ensure PIA assessments are consistent and straightforward, we proposed the Privacy Screening Framework, which assists privacy assessors to assess projects prescriptively against all the seven categories of privacy risks. The PSF framework is flexible, adaptive and self-directing; which means that the person undertaking the assessment (assessor) can choose to adapt the framework to suit the needs of a particular project. The framework can be utilized and applied by any person. The framework is straightforward and derived based on lessons learned in carrying out PIA assessments for a number of organisations on a number of projects. Further to the frameworks provided, we provided the legal and privacy compliance check (see ***Table 3***) to ensure consistency when assessing privacy regulations and directives compliance.

With the understanding that the earlier privacy assessment is planned in the project initiation programme the better the organization will be in addressing privacy requirements, issues or concerns. We recommend that privacy impact assessment should become an essential part of the risk management process of every project. We hope that this will help organisations plan PIA from the outset of the project, knowing that retrofitting of privacy assessment can be costly as we have seen with PIA assessment of in-service projects.

When planning privacy impact assessment, considerations should be made of risks resulting due to the sheer volume of personally identifiable information the project would process. And when data from different sources will be used, the impact of aggregation of these data should be considered. This should serve as an indicator as to when additional privacy controls may be required due to aggregation effect. Finally, we recommend that privacy impact assessment should be carried out by privacy experts within an organization, and where people with the right skills cannot be found, the services of external privacy agencies should be enlisted. There is new privacy legislation in the UK that empowers the UK Information Commissioner's Office to exact financial penalty to any organization in breach of privacy. This will, and has ushered a reawakening of privacy consciousness in organizations, especially, governmental organizations and agencies.

FUTURE RESEARCH DIRECTIONS

We plan to automate the PIA frameworks proposed in this chapter into a toolkit that will assist organizations when carrying out privacy risk assessments. The proposed toolkit will be available for download, or used from www.research-series.com. The provision of automated toolkits to assist with conducting PIA can be helpful, but the challenge will be on the coverage of relevant privacy legislations. This is because local or provincial privacy legislations are different among countries; hence, it will be challenging to cover all applicable privacy legislations in the toolkit.

CONCLUSION

In this chapter, we discussed the overriding benefits of Health IT, especially adoption of the electronic health records, providing very useful insights to Europe where EHRs are fully operational and functional. To assist with Health IT adoption in the US, especially encouraging public trust and confidence in EHR, we proposed a privacy impact assessment framework for managing privacy risks associated to the exchange, sharing and transmission of personally identifiable information. The privacy assessment framework aids to identifying and remedying privacy risks in Health IT. It provides assessments questions that can be tailored to any Health IT project in order to fully understand associated privacy risks and remediation plan.

The different issues relating to privacy impact assessment of new and in-service projects are demonstrated and discussed. It was found that in-service projects were challenging to be privacy assessed, and the outcome of privacy impact assessment to an in-service project could be insightful and expensive; and consequently could result to significant financial losses to the organization when found in breach of privacy. Privacy impact assessment frameworks were proposed, discussed and utilized to demonstrate their usefulness when conducting PIA assessments. Each aspect of the privacy framework was described such as the privacy impact suitability framework, legal and privacy compliance check and privacy screening framework. Finally, issues surrounding aggregation of personally identifiable information were discussed with the view to highlighting associated risks while recommending essential privacy controls to addressing these risks.

ADDITIONAL READING SECTION

Onwubiko, C. (2011). Challenges to Managing Privacy Impact Assessment of Personal Identifiable Data. *Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances*, (Eds.) Te-Shun Chou. Pennsylvania: IGI Global.

Onwubiko, C. (2008). Security Framework for Attack Detection in Computer Networks. Germany: VDM Publishing.

KEY TERMS & DEFINITIONS

Personal Data: Personal data is data that relates to a living person who can be identified by those data, or from those data plus other information which is in the possession of, or is likely to come into the possession of, the data controller. For example, first name, last name or/and date of birth of a living person.

Sensitive Personal Data: These are identifiable personal data whose release would put those persons at significant risk of harm or distress, unless otherwise disclosed by the persons. For example, a person's medical records, bank details, social insurance number (national insurance) or tax records etc.

Personal Identifiable Data (PID): These are sensitive and personal data that can be used to identify an individual. Personal identifiable data is the same as Personally Identifiable Information (PII), while the former is associated to Europe; the latter is associated with America. Examples of PII include a combination of one or more personal identifiers such as full face photographic images and any comparable images plus name, or date of birth plus address and health records. A full list of personal identifiers is shown in *Table 1*.

Data Protection Act (DPA): This is a piece of legislation that governs how personal information of living individuals is processed. Processing of personal information means, how personal information are obtained, shared, recorded or stored (held). This piece of legislation was enacted in 1998 in the United Kingdom (UK).

REFERENCE

Abu-Nimeh, S. & Mead, N. R. (2009). Privacy Risk Assessment in Privacy Requirements Engineering. *2nd International Workshop on Requirements Engineering and Law*, 11, 7-15.

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A. & Connolly, G. N. (2014). Concern about Security and Privacy, and perceived control over collection and use of health information are related to withholding of health information from health care providers. *PubMed, US National Library of Medicine, National Institutes of Health*. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/23975624/

British Broadcasting Corporation, (2014). Care.data: How did it go so wrong? Retrieved February 21, 2014 from http://www.bbc.co.uk/news/health-26259101

Cabinet Office (2008). The Data Handling Procedure in Government: Final Report, June 2008. Retrieved from http://www.cesg.gov.uk/products_services/iatp/documents/data_handling_review.pdf

Directive 95/46/EC (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Directive 2002/58/EC (2002). Protection of Privacy to Electronic Communications. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

Educause (2010). Privacy Risks Assessment. Retrieved from http://www.educause.edu/node/645/tid/30444?time=1281348515

Grady, D. (2010). Study finds no progress in safety at Hospitals. Retrieved from http://www.nytimes.com/2010/11/25/health/research/25patient.html?_r=0

Gruteser, M. & Grunwald, D. (2004). A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks in Security in Pervasive Computing. *Lecture Notes in Computer Science*, 2004(2802), 113-142

HIPAA (2006). Saint Louis University Institutional Review Board. HIPPA TIP Sheet, 31st March 2006. Retrieved from www.slu.edu/Documents/provost/irb/hipaa_tip_sheet.doc

HITECH Act (2010). Health Information Technology for Economic and Clinical Health Act. Subtitle A, SEC 3000, Definitions, 2009. Retrieved from http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf

HMG IA Standard No. 6 (2009). Protecting Personal Data and Managing Information Risk. Cabinet Office, CESG National Technical Authority for Information Assurance, Issue 1.2.

Information Commissioner's Office (2009). Privacy Impact Assessment. Handbook Version 2.0. Appendix 1 – PIA Screening Process. Retrieved from http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app1.html

Lesk, M. (2013). Electronic Medical Records: Confidential, Care and Epidemiology. *IEEE Security & Privacy, Building Dependability, Reliability and Trust*, 6(11)

McGraw, D. (2013). Privacy and Security as Enabler, Not Barrier, to Responsible Health Data Uses. *IEEE Security & Privacy, Building Dependability, Reliability, and Trust*, 6(11)

NHS Database (2014). NHS Bosses Accused of 'Climate of Fear' over Care Data. Retrieved from http://www.telegraph.co.uk/journalists/laura-donnelly/10628950/NHS-bosses-accused-of-climate-of-fear-over-care.data.html

Office of the National Coordinator for Health Information Technology (2010). Strategic Health IT Advanced Research Projects (SHARP). Retrieved from http://www.healthit.gov/policy-researchers-implementers/strategic-health-it-advanced-research-projects-sharp

Onwubiko, C. (2011). Challenges to Managing Privacy Impact Assessment of Personal Identifiable Data. Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances, (Eds) Te-Shun Chou, Pennsylvania: IGI Global.

Peirce, T. (2009). RFID Privacy & Security. *IEEE International Conference on Communications, ICC*, 24, 11-15

Privacy by Design (2014). We Must Strongly Protect Privacy in Electronic Health Records. Retrieved from http://www.privacybydesign.ca/index.php/must-strongly-protect-privacy-electronic-health-records/

Radack, S. (2010). Guide To Protecting Personally Identifiable Information (PII). *NIST ITL Security Bulletin*. Retrieved from http://csrc.nist.gov/publications/nistbul/april-2010_guide-protecting-pii.pdf

Shane, D. (2010). Zurich Insurance hit with Record Data Loss Fine. Retrieved from http://www.information-age.com/channels/security-and-continuity/news/1277718/zurich-insurance-hit-with-record-data-loss-fine.thtml

US-CERT (2008). Privacy Impact Assessment EINSTEIN Program. *Department of Homeland Security, National Cyber Security Division, United States*. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf