



Managing Information Privacy & Security in Healthcare

Privacy Impact Assessment Guide

By the Privacy Impact Assessment Work Group

TABLE OF CONTENTS

HIMSS Privacy Impact Assessment Guide..... 1

TABLE OF CONTENTS..... 1

I. Introduction..... 3

II. Background ..... 3

    A. What is a PIA? ..... 3

    B. Who Should Conduct a PIA?..... 4

    C. Information Covered in a PIA ..... 4

    D. When to Conduct a PIA..... 5

    E. The Role of a PIA throughout System Lifecycle ..... 6

III. PIA Process..... 7

    A. Organizing a PIA ..... 7

        1. Securing Organizational Support ..... 7

        2. Roles and Responsibilities..... 8

    B. Preparing for a PIA..... 8

        1. Information Needed for the PIA ..... 8

        2. Understanding the System Architecture ..... 9

        3. Understanding Privacy Requirements ..... 9

IV. Conducting the PIA ..... 9

    A. Approaches ..... 9

        1. Automated Tool Approach ..... 9

        2. Questionnaire Approach ..... 10

        3. PIA and Risk Analysis Approach ..... 11

    B. Components of the PIA ..... 12

- C. Documenting PIA Findings: The Report..... 14
- V. The PIA Results ..... 15
  - A. Communicating the Results..... 15
  - B. Using PIA Results ..... 16
  - C. Maintaining the PIA ..... 17
- VI. Glossary of Terms..... 18
- APPENDIX A – PIA Model Questions..... 20
- CONTRIBUTION ACKNOWLEDGEMENT ..... 22

## I. Introduction

This guidance document serves as an educational resource best practices guide for the healthcare industry to help providers and related organizations efficiently and properly perform Privacy Impact Assessments (PIA). HIMSS created this guide to provide a framework for understanding PIAs and to assist organizations in PIA preparation and implementation activities. Tools and processes mentioned in this document are included as examples. HIMSS does not endorse any particular PIA tool or assessment methodology.

HIMSS and its volunteers have reviewed and relied on various industries' PIA resources and standards. The authors of this paper discovered a plethora of government and non-healthcare related resources and have selected those most applicable and transferable to the healthcare industry for inclusion in this guide. The intent was to broadly examine the use of the PIA as it exists independent of specific application or industry.

Nevertheless, the information presented here has been interpreted and adapted to reflect healthcare best practices<sup>1</sup> and, where possible draws from the actual experiences healthcare and related organizations have encountered in conducting PIA efforts.

## II. Background

### A. What is a PIA?

A PIA is a tool used to assess the impact and risks to the privacy of personally identifiable information (PII) stored, used and exchanged by information systems. The Office of Management and Budget (OMB) defines the PIA as:

*an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.<sup>2</sup>*

A PIA has increasing importance in electronic healthcare initiatives as PII is captured, processed, stored, and transmitted by healthcare organizations. Significant privacy risks are often introduced in these scenarios. Additionally, privacy risks are inherent in many information management practices that seek to anonymize personal information and in instances where additional PII augments an existing data set.

---

<sup>1</sup> The concepts provided in this document were primarily derived from two sources:  
 - HHS Privacy Impact Assessment activities in response to Privacy Act Requirements; and  
 - ISO Financial Services Industry – Privacy Impact Assessment (ISO/WD NP 22307, dated 2005-12-12). ISO 22307:2008 available at: [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=40897](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40897)

<sup>2</sup> Office of Management and Budget (OMB), *Memorandum for Heads of Executive Departments and Agencies*, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Memo M-03-22 (September 26, 2003), <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

PIAs supported and employed on a systematic basis provide numerous benefits to an organization:

- A PIA can be used to evaluate whether appropriate privacy protections are in place and to reveal necessary mitigations aimed at reducing potential privacy risks.
- A PIA serves as a tool to address privacy requirements, complimenting organization-wide compliance activities (e.g. HIPAA privacy, etc.).
- A PIA supports auditing best practices and provides important evidence of compliance activities.
- A PIA compliments other risk assessment activities by providing data on safeguards currently employed to protect information, cataloging the type of information gathered, used, stored and exchanged by systems.

### ***B. Who Should Conduct a PIA?***

Organizations that rely on information systems to store, process or exchange personal information should consider incorporating PIAs into their compliance efforts and information system management processes. The following are among the many types of organizations that benefit from such practices:

- Larger providers, including hospitals
- Vendors
- Service providers
- Device manufacturers
- Any organization that functions as a business associate
- Employers
- US Government agencies covered under the E-Government Act OMB guidance (M-03-22).
- Organizations required to respond to external requests for (personal) data.

An organization should contemplate the benefits of PIAs when: 1) there is a real or perceived risk to the confidentiality of personal information, and/or 2) an organization invests in information technology and maintains data in electronic form. Increased use of and reliance on electronic records (and the resulting accessibility and availability of volumes of personal information) increases the business impact and potential privacy risk on an organization. PIAs provide an objective means to evaluate the various uses and disclosures of personal information, and the related risks to information privacy. The PIA process, in turn, allows the organization to proactively plan appropriate risk mitigations.

### ***C. Information Covered in a PIA***

A PIA may focus on different types of information collected, used, stored and exchanged by systems. The concept of "privacy," however, is derived of an individual's right to have control over their information and to selectively divulge aspects of that information, at their discretion. Therefore, the PIA is intended to assess risks to that individual right, in an environment (such as a healthcare facility) where controls and processes are outside of the individual's immediate control. Various nomenclatures are used to describe the types or aspects of information subject to this privacy right, including:

- Protected Health Information (PHI)<sup>3</sup>
- Personally Identifiable Information (PII)<sup>4</sup>

---

<sup>3</sup> Protected Health Information is defined by the Health Insurance Portability and Accountability Act as individually identifiable health information that is transmitted or maintained in any form or medium. See [45 CFR 160.103](#) (2007).

- Information in Identifiable Form (IIF)<sup>5</sup>
- Personal Data<sup>6</sup>

PIAs generally focus on identifiable information of the individual. Organizational confidential, secret or proprietary information is therefore considered outside the scope of the PIA. For the purpose of this guide, we have used the term Personally Identifiable Information (PII) as a generic term for the type of data covered in a PIA. The type of data covered in a PIA may depend upon the context or environment in which a PIA is conducted. At a minimum, both PHI and Personal Data are assumed to be included in PII.

#### ***D. When to Conduct a PIA***

A PIA may be conducted to evaluate information privacy and security throughout the life cycle of a system, product or project, or when a risk assessment is required in light of activities such as information sharing or exchanging with other organizations or agencies.

Examples of *types* of systems and situations that would benefit from a PIA:

- Systems with access to a database, file or document that may update, share, or create duplicates in soft/hard copy of PII data;
- Systems or host websites that collect, maintain, archive records with PII;
- Systems with multiple application and/or interoperability processes – exchanging data with other systems;
- Systems that transmit PII to other applications or systems;
- Systems have interfaces with multiple applications or other systems where PII is exchanged;
- Systems with the ability to download files or records containing PII to other local, remote or removable storage devices;
- Systems containing PII that can be accessed by the public;
- Systems supporting different levels and types of authorized users with access to PII data;
- System requirements are defined for a new/existing system, product or project involving PII; and
- Systems involving the physical transfer or archiving of PII data.

PIAs can be especially helpful when defining requirements for a system. The PIA serves as a tool to assess information privacy risks associated with a system. This is accomplished through the definition of

---

<sup>4</sup> Personally Identifiable Information is information that an organization may have or maintain (e.g. financial information, e-mail addresses, employment information, disability information, etc.) and other categories of confidential information.

<sup>5</sup> IIF is “information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).” *Supra* note 2.

<sup>6</sup> Personal Data is defined as: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. See Directive 95/46/EC of the European Parliament and of the Council, *Official Journal of the European Communities*, No. L 281, 31–50 (November 23, 1995), [http://www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html#HD\\_NM\\_28](http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_28).

appropriate privacy (and security) controls. These controls are defined through the answers to key questions such as:

- Who are the target users for this system?
- To what degree will these users comply with privacy and security requirements?
- What is the purpose for providing access to PII (e.g. providing a service, customer service activities, viewed by another organization, or viewed by public)?
- How is access granted to a user and how is it authenticated to permit a user's access: (e.g., as an administrator or a user, to read, edit, or copy)?
- Are appropriate audit mechanisms employed to ensure that when data is created, accessed, modified, processed, or exchanged (transmitted to other systems, applications, users) effective audit records are generated?

### ***E. The Role of a PIA throughout System Lifecycle***

PIAs play an important part throughout a product, system, or project lifecycle, allowing organizations to assess risks to information privacy and security.<sup>7</sup> The following suggested questions and observations reveal various privacy considerations applicable to a system from the design stage through the system's retirement.

#### **For design and development stages:**

- What steps must be taken to secure access to PII data for the technology/environment the system uses (e.g., Internet, network)?
- Are there interfaces, links or transmission points where PII data is exchanged?
- Do different users require different levels of authentication to access the system? If so, who will be able to access and view PII?
- Are effective audit records being produced and appropriately managed; and do those records capture personal data?

#### **For active systems:**

- How does your organization handle suspected PIII disclosures?
- How many - privacy/security issues were reported as violation or technical errors that involve PII?

#### **For system enhancement:**

- Is the enhancement involved in a new process that uses PII data?
- Is there any impact on existing processes caused by the system enhancement, potentially introducing new hazards to the integrity of the PII? If so, then a PIA and a risk assessment should be conducted to determine if additional privacy/security requirements are needed.

---

<sup>7</sup> Project life-cycle refers to the process of defining requirements, design and development—launched and active—enhancements and the end of life cycle (sunset).

### For the sunset/end of life cycle of a system:

- Will PII data be deleted, archived or used by another system?
- Will all PII data be used in whole or as a subset?
- The reuse of PII data will require a new PIA assessment for use in a new or existing system.
- When sharing/exchanging PII data between organizations, a PIA will assess the use of PII in the new host, if it is new or existing system.
- PIA response evaluation can be graded by any of the following response measures: low/medium/high, percentage: 0 – 100%, or with a point value.

## III. PIA Process

### A. Organizing a PIA

This section addresses the measures an organization should consider when preparing for a PIA.

#### 1. Securing Organizational Support

To be successful and valuable to the organization, the PIA process should have an executive sponsor and steering committee to facilitate broad support throughout the organization and provide guidance to the effort. While the business and technical drivers behind the initiative may differ, the process for obtaining organizational support and acquiring the resources necessary to support the PIA program are much like other privacy, security and related compliance efforts.

The following are proposed steps for securing organizational support:

- **Identify an executive sponsor to support the effort.**
  - The appropriate executive may vary depending upon the approach employed. (See Section IV *infra* for details).
  - Executive sponsors might include a CIO or CISO, since the system owners are likely affiliated with these offices.
  - Key stakeholders to the effort include the Privacy Officer and Chief Compliance Officer (if they are not one in the same).
- **Organize a Steering Committee to oversee the PIA program efforts and provide support and guidance to the effort.**
  - This cross-representative group should include representatives from IT, security, privacy, key system owners and legal.
  - Define a policy that describes the purpose, objectives and expectations for PIAs.
  - Define roles and responsibilities for system owners, developers, security and privacy.
  - Educate the organization on the PIA objectives, process and expectations.
  - Train system owners and developers on how to conduct a PIA.
- **Launch the program.**
  - Communicate a commitment statement from the executive sponsor so that the organization supports the PIA process.
  - Provide a resource center (e.g. intranet site, network drive, etc.) where information regarding the PIA process can be found.

## 2. Roles and Responsibilities

Roles and responsibilities in the PIA process may vary depending upon the organizational structure, size and the PIA approach employed (as described in Section IV below). The following table illustrates some of the common roles and responsibilities in supporting PIAs.

Role	Establish Organizational Imperative	Oversee PIA Process	Initiate PIA	Conduct PIA (collect data)	Compile Findings	Review Findings and Assess Risks	Define Design Requirements to Address Risks	Implement Remediation
Executive Sponsor	X	X						
Governance Committee		X						
System Owner / Developer			X	X	X		X	X
CIO			X				X	
CISO			X				X	
Privacy Officer						X	X	

Despite the various approaches, roles and responsibilities tend to follow similar function alignments. PIAs are generally conducted by system owners and developers since they are most familiar with the use and function of the systems and the information involved. While Privacy Officers may not directly drive the PIA process, they are important stakeholders in reviewing the findings, assessing risks and helping to facilitate a remediation plan, including maintenance of documentation required for privacy compliance.

### *B. Preparing for a PIA*

#### 1. Information Needed for the PIA

As users prepare to fill out the PIA, they may gather documentation already created for the system, particularly previous PIAs and security documentation, such as risk assessments or certification and accreditation packages. These documents can contain information about the system that will make completing the PIA documents more efficient.

In general, any documentation about the system, including architecture designs, business process data, system of record notices (SORN's), system analysis reports, and other data is useful in completing a PIA. For many organizations, only a system design document or user instruction manual will exist. Business and system architecture information can still be gleaned from these sources.

There are specific sources of information that can be used to conduct a PIA. Two of the most important sources to review are the system architecture information and the organizational privacy requirements.

## 2. Understanding the System Architecture

An important source to review for the PIA is the system architecture itself. The system architecture outlines the specific relationships between the system and other entities within the organization. System architecture review may entail reviewing system documents and conducting interviews to obtain the information.

For example, if the system shares sensitive data with other systems, or if the system exchanges information internally that is classified as sensitive, then the underlying metadata surrounding these particular transactions (as shown in architecture diagrams, if available) would be useful to have during the PIA. This will help the PIA respondent answer many of the underlying questions regarding data access and data attributes.

## 3. Understanding Privacy Requirements

An important facet of preparing for a PIA is to understand the organization's privacy requirements. The privacy requirements dictate the type and relevance of questions included in the PIA. Because a PIA is used for analysis and recommendations related to privacy, there should be alignment between the questions asked in the PIA and the privacy goals of the organization.

For example, healthcare organizations that have non-external facing systems may wish to conduct a PIA, but the PIA template can be structured to not focus on the exchange of private data but on the storage of private data, to provide a more accurate measurement to management of the compliance or status of the organization.

## IV. Conducting the PIA

### A. Approaches

As a starting point, healthcare organizations may assess internal systems. However, over time and as volume and complexity of information exchange increases, it may be necessary to expand the use of the PIA.

PIAs are generally collected by either using a document template or using a worksheet to capture the information. In some cases, the process is automated using an application designed to store and process the information collected in an organized and accessible manner. Listed below, are three separate approaches largely used by various government agencies in building their PIA assessment process. Each approach differs based on roles and based on the steps taken to complete the PIA, but could easily apply to healthcare organizations.

### 1. Automated Tool Approach

One approach considered in this guide involves the use of an automated PIA tool that stores the information collected for the PIA. For this approach, a risk analysis that considers the risks and remediation necessary to protect PII is conducted separately. The Department of Health and Human Services (HHS) employs this method as a standard approach for conducting PIAs required by the Privacy Act.<sup>8</sup>

---

<sup>8</sup> HHS Information Security Program, *Privacy Impact Assessment Guide*, 2007, available at: [http://oma.od.nih.gov/ms/privacy/PIA\\_Guide.doc](http://oma.od.nih.gov/ms/privacy/PIA_Guide.doc)

Step	Roles	Process
1	System owner, developer, and CISO	Determine when a PIA must be conducted
2	CIO and CISO	Assign Roles and Responsibilities
3	System owner and developer	Prepare for the PIA
4	System owner and developer	Compose a PIA
5	System owner, developer, and CISO	Characterize the System
6	System owner and developer	Complete the PIA
7	CIO and CISO	Approve or Demote the PIA
8	System owner and developer	Maintain the PIA

Automated PIA tools may provide the following type of features, including but not limited to:

- A central location to maintain PIA information and documentation
- Reporting structured to support specific requirements such as FISMA reporting
- Central location a to carry out all PIA functions associated with an IT system's lifecycle
- Enterprise-wide collaboration
- Role-based authorization within the tool

Benefits of using automated tools include:

- Standard and consistent questions (will not change from year to year).
- Once initial training is complete there will be no need to retrain every year.
- Standard questions will allow an organization to develop an effective user manual and provide example responses to PIA questions.
- Standard questions allow reviewer/coordinator to focus on answers and not just the questions.

Potential challenges:

- Some questions will not apply and may alienate a system or responder.
- In some organizations limitations present in the questions may pose a problem in accurately reflecting the system's attributes.

## 2. Questionnaire Approach

Another approach involves the use of questionnaires to collect the information pertaining to a large number of systems and a large number of potential system changes. This method anticipates the need to quickly assess and document the privacy impact. This approach, like the method using an automated PIA tool,

considers the risks and mitigations necessary to protect PII separately. The Department of Defense (DOD) employs this approach given the large number of systems and potential changes<sup>9</sup>. This method involves fewer steps and is designed to be a quicker process.

Step	Roles	Process
1	Owner and Developer	Obtain a copy of the assessment from your privacy officer. Request briefings on organizational privacy requirements.
2	Owner and Developer	Complete questions on the PIA, and consult with necessary parties
3	Owner, Developer, CIO, Privacy Officer, CISO	All parties should reach an agreement on design requirements and resolve any identified privacy or security risks. Ensure that all appropriate surnames are obtained.
4	Owner, CISO	Review PIA for IT Security C&A purposes. Provide completed PIA to the IT Security Officer and Privacy Officer.

### 3. PIA and Risk Analysis Approach

A third approach considered in this guide is employed by the Internal Revenue Service (IRS) and is recognized by the OMB as the model approach to use for building a PIA process.<sup>10</sup> This approach is focuses on conducting the PIA as well as resolving and mitigating risks identified in the PIA. This method ties the PIA process to the risk analysis to incorporate the PIA findings into risk-based decisions. While this is the most desirable method since it identifies risks and uses the PIA information to affect decisions, this method can also take more planning and coordination.

Step	Roles	Process
1	System Owner and Developer	Request and complete PIA (PIA) Training.
2	System Owner and Developer	Answer the privacy questions

<sup>9</sup> Department of Defense (DOD), *Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance*, 2005, available at: [http://www.dla.mil/public\\_info/efoia/DODPIAGuidance.pdf](http://www.dla.mil/public_info/efoia/DODPIAGuidance.pdf)

<sup>10</sup> Internal Revenue Service (IRS), *Model Information Technology Privacy Impact Assessment*, 1996, available at: [http://www.cio.gov/Documents/pia\\_for\\_it\\_irs\\_model.pdf](http://www.cio.gov/Documents/pia_for_it_irs_model.pdf)

3	System Owner and Developer	Submit the PIA document to the Privacy Officer
4	Privacy Officer	Review the PIA document to identify privacy risks from the information provided. The Privacy Officer will get clarification from the owner and developer as needed.
5	System Owner, Developer, Privacy Officer and CIO	The System Owner, Developer and the Privacy Advocate should reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached then issues will be raised to the CIO for resolution.
6	System Owner and Developer	The System Owner and Developer will incorporate the agreed upon design requirements and resolve the identified risks.
7	System Owner, Developer, and Privacy Officer	Participate in required reviews to ensure satisfactory resolution of risk

### ***B. Components of the PIA***

PIA components lead the assessor or analyst to a determination of the compliance or risk level of the system, process, etc. as well as revealing any necessary mitigations. The PIA should elicit responses that are 1) clear and unambiguous; 2) provide specific information that will aid in the evaluation (avoid redundancy, or seeking irrelevant information); and 3) will provide a vehicle to identify appropriate follow-up, remedial, or mitigating actions.

One approach to determining what questions should be asked is to outline the relevant requirements, and identify what specific information is needed to address each requirement. Understanding the impact of varying answers to the questions asked, and evaluating how some responses might change the outcome of the assessment (impact of answers on next steps, need for additional information, etc.), can assist in developing the PIA components and the wording of the questions. Anticipating various types of responses may help identify the best way to ask the questions.

The PIA tool chosen should integrate the following key sections to ensure that the PIA is effective. The following table outlines specific sections that should be included in the PIA, representing high-level categorizations of “privacy principles” that drive the specific questions asked within the PIA.

It is important to note that the PIA tool is attempting to determine the relative alignment between the privacy principles of the organization and the system being assessed. This intent is consistent regardless of the delivery method for the PIA questions.

<b>PIA Tool Sections</b>	<b>Description</b>
Information and Privacy	The use of information must be controlled. Information may be used only for a necessary and lawful purpose. Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them. Information collected for a particular purpose should not be used for another purpose without the data subjects consent unless such other uses

	<p>are specifically authorized or mandated by law.</p> <p>Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual.</p>
Data in the System	<p>The sources of the information in the system are an important privacy consideration if the data is gathered from other data sources.</p> <p>Information collected from external sources should be verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. This is especially important if the information will be used to make determinations about individual's care</p>
Access to the Data	<p>Who has access to the data in a system must be defined and documented.</p> <p>Users of the data can be individuals, other systems, and other organizations. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data.</p>
Attributes of the Data	<p>When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data.</p> <p>First, the data must be <i>relevant</i> and <i>necessary</i> to accomplish the purpose of the system. Second, the data must be <i>complete</i>, <i>accurate</i> and <i>timely</i>. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.</p>
Maintenance of Administrative Controls	<p>Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.</p> <p>Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory requirements. Precise rules must be established for the length of time information is kept and for assuring that it is properly eliminated at the end of that time.</p> <p>The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure the privacy of individuals and prevent unnecessary intrusion. The use of monitoring capabilities should be limited, at a minimum, to some ascertainable standard of reasonableness.</p>

Because much of the required information is already known or available to the system or program manager, the template/worksheet focuses on asking questions specific to assessing privacy of the system. The template should be structured to capture the following points:

- What information is to be collected?
- Why the information is being collected?
- What is the intended use of information by the organization?
- With whom the information will be shared?
- What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared?
- How will the information be secured?
- Will a system of records notice be created (public announcement that the system exists)?

The PIA Tool should also ensure that the following style rules are part of the assessment:

- Open-ended questions should be written concisely and in a way that is easily understood by the general public.
- Expand each acronym the first time it is used: the acronym should be used in all subsequent references.
- Technical terms and references should be defined.
- References to governmental publications and other documents should include the complete name of the reference the first time it is used.

**Appendix A** contains a set of model questions to include in the PIA. This set of questions is intended to assist healthcare organizations in establishing their own PIA template for use in their organization, and to serve as a reference point as an organization begins developing their PIA. Other questions should be added or these questions tailored to meet the needs of the individual organization.

### ***C. Documenting PIA Findings: The Report***

A PIA report should generally cover the following points:

- The scope of the PIA;
- The summary description of the system and any other components aligned to the system;
- The team that performed the PIA and developed the PIA Report;
- The governance structure surrounding the PIA process;
- The decision-making processes for system development based on the PIA Report;
- The relevant Privacy Policies, privacy laws and standards for the processing of personal information relevant for the system;
- Assessment findings as to the privacy risks of the system and whether it is able to comply with relevant privacy policies and laws, the significance of those risks to both complying with privacy regulations and the meeting of business objectives and any other risks to personal information discovered during the assessment;
- Recommended alternatives to both mitigate the risks and achieve the stated business objectives of the system; and

- Identification of the executive who is the recipient of the PIA report and who is responsible for acting on findings and recommendations.

One approach commonly used in PIA reporting is to provide a set of privacy principles aligned to the PIA. If an organization has established a set of privacy principles, the PIA template components can be grouped into categories that are then aligned to these principles. This type of analysis can be included in an executive summary to senior management in order to increase understanding of how effectively relevant systems and processes are aligning to the organization's privacy goals.

## V. The PIA Results

### *A. Communicating the Results*

The PIA Assessment process fails to add value unless the results are communicated to the stakeholders who participated in the assessment. If the results of the assessment are not disclosed to the participants, no improvement in the privacy practices of the organization will result. The following communication plan is suggested for effective communication.

#### **Step 1: Consolidate the findings**

The various pieces of the PIA need to be consolidated into an assessment report. For each part of the organization that provided input to the assessment, a report on the results of that input should be communicated back to the participants. This report should include:

- The information provided by the organization, and the responsible point of contact;
- The criteria used to assess the information;
- The sufficiency of the information to fulfill the criteria;
- Deficiencies if noted; and
- Recommendations for corrections/improvements.

#### **Step 2: Summary Report to the PIA sponsor**

The organization responsible for the PIA should be provided with an executive summary report of the PIA results. Depending upon the organization, this information may be a briefing or a written report. The executive summary should include:

- Description of the work effort and any key approaches, the resources used, and the systems assessed;
- Summary of the findings describing the areas of greatest concern, as well as highlighting successes in how information is currently being managed;
- Summary of any significant improvement plans, their timelines and budget;
- Implications, as well as specific outcomes in terms of reducing risk, including quantitative measure, if known;
- Summary of any key learning from the process and any follow-up steps pertinent to future assessments; and
- Progress made to date, if this is a follow-up to a previous assessment.

This report is crucial to the success or failure of the impact assessment. If management does not concur with the findings of the PIA, it will be difficult for an organization to expend resources for

improvement. The PIA summary also serves as evidence that the assessment process was carried out by the organization.

### **Step 3: Reporting to the cognizant IT and Compliance organizations.**

The summary should also be reported to an organization's:

- Chief Compliance Officer,
- Chief Privacy Officer, and
- Chief Information Security Officer.

This reporting provides an opportunity for the organization to monitor potential trends in the Privacy posture of the organization. When necessary, centralized solutions or task forces can be formed to address common privacy issues among several areas of the organization.

### **Step 4: Communication of Remedial Action Plans**

Based on the results of the PIA, remedial actions may need to be undertaken by the organization. If this is the case, the remedial action plan, including schedule and budget, needs to be communicated to the appropriate organizations. Potential remedial actions can include:

- Additional privacy awareness training for the organization;
- Changes to existing records management policies; and
- Posting of privacy policies in conspicuous locations.

The objective is to execute on the remedial action plan to correct deficiencies noted by the PIA. Efforts to correct deficiencies need to be documented for compliance purposes, as they provide a measurement instrument for subsequent PIAs and evidence that the organization is addressing shortcomings in its privacy policies.

The objective of the communication process is to note organizational strengths and weaknesses, and to correct deficient privacy practices proactively within the organization.

## ***B. Using PIA Results***

The primary purpose of a PIA is to allow the organization building or operating a personal information system to decide whether it is in compliance with relevant data protection legislation at any particular stage in time. An important secondary goal is to meet the privacy expectations of the public with respect to moral and ethical considerations. PIAs provide a foundation for the development of a stronger and more robust privacy framework for an organization.

Additionally, a PIA will serve as an educational and negotiating tool for the system owners to use for purposes of compliance reviews by senior management and by the external data protection agent or agency. The PIA should make it relatively easy for executives and the privacy commissioner and his or her staff to understand how the system works and what the privacy issues and risks are, if indeed there are any.

A PIA will continue to evolve over time with the continued development of a particular system. This is one of its most important characteristics, since the PIA can be used to monitor important changes in any system—especially those with potentially negative implications for the privacy of individuals.

### ***C. Maintaining the PIA***

In addition to maintaining a hard copy of the PIA, an organization will periodically need to review the PIA to ensure they comply with current system practices. A PIA is a living document that must be updated when a major change in the system occurs. The following table outlines what some of these triggers for initiating a PIA update:

Type of Change	Description
Conversions	Converting paper-based records to electronic systems
Anonymous to Non-Anonymous	Functions applied to an existing information collection change anonymous information into information in identifiable form
Significant System Management Changes	New uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system
Significant Merging	<p>Organization adopts or alters business processes so that databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated</p> <p>For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously at issue</p>
New Public Access	User-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public
Commercial Sources	Organization systematically incorporates into existing information systems databases of information in identifiable form, purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement)
New Interoperability Uses	Organizations work together on shared functions involving significant new uses or exchanges of information in identifiable form

Internal Flow or Collection	Alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form
Alteration in Character of Data	New information in identifiable form added to a collection raises the risks to personal privacy. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise

Periodic reviews of the PIA will ensure that these triggers—or any other changes in a system's management, operational, or technical environment that may impact the organization—will be captured. Once a system expires or is retired and no longer in operation, the system's PIA may also be retired.

## VI. Glossary of Terms

### Information in Identifiable Form (IIF)

Information in Identifiable Form in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

### Personal Data

Personal Data is any information relating to an identified or identifiable human being.

### Personally Identifiable Information (PII)

Personally Identifiable Information is information that an organization may have or maintain (e.g. financial information, e-mail addresses, employment information, disability information, etc.) and other categories of confidential information.

### Processing

Processing is any operation which is performed on Personal Data, such as collection, recording, storage, organization, alteration, use, disclosure, transmission, or deletion wholly or partially by automated means, as well as any operation performed on Personal Data stored or intended to be stored in a systematically accessible (paper-

based) filing system.

**Protected Health Information**

Protected Health Information is defined by the Health Insurance Portability and Accountability Act as individually identifiable health information that is transmitted or maintained in any form or medium.

**Sensitive Data**

Sensitive data is a sub-set of personal data which reveal an individual's racial or ethnic origin, political opinions or membership of political parties or similar movements, religious or philosophical beliefs, membership of a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offences, criminal records, proceedings with regard to criminal or unlawful behavior, or personal identification numbers issued by the government

**System**

A System contains a structured set of data that can be accessed according to specific criteria, and is systematically accessible

## APPENDIX A – PIA Model Questions

System Information	<ul style="list-style-type: none"> <li>• What information is to be collected?</li> <li>• From whom is the information collected?</li> <li>• Why is the information being collected?</li> <li>• What specific legal authorities, arrangements, and/or agreements defined the collection of information?</li> </ul>
Uses of the System	<ul style="list-style-type: none"> <li>• Describe all uses of the information.</li> <li>• Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)</li> <li>• How will the information collected from individuals or derived by the system, including the system itself be checked for accuracy?</li> </ul>
Retention	<ul style="list-style-type: none"> <li>• What is the retention period for the data in the system?</li> <li>• Has the retention schedule been approved?</li> </ul>
Internal Sharing and Disclosure	<ul style="list-style-type: none"> <li>• With which internal organization(s) is the information shared?</li> <li>• For each organization, what information is shared and for what purpose?</li> <li>• How is the information transmitted or disclosed?</li> </ul>
External Sharing and Disclosure	<ul style="list-style-type: none"> <li>• With which external organization(s) is the information shared?</li> <li>• What information is shared and for what purpose?</li> <li>• How is the information transmitted or disclosed?</li> <li>• Is a Memorandum of Understanding (MOU), contract, or agreement in place with any external organization(s) with whom information is shared, and does the MOU reflect the scope of the information currently shared?</li> <li>• How is the shared information secured by the recipient?</li> <li>• What type of training is required for users from agencies outside the organization prior to receiving access to the information?</li> </ul>
Notice	<ul style="list-style-type: none"> <li>• Was notice provided to the individual prior to the collection of information?</li> <li>• Do individuals have the opportunity and/or right to decline to provide information?</li> <li>• Do individuals have the right to consent to particular uses of the information?</li> <li>• If so, how does the individual exercise the right?</li> </ul>
Individual Access, Redress, and Correction	<ul style="list-style-type: none"> <li>• What are the procedures that allow individuals to gain access to their own information?</li> <li>• What are the procedures for correcting inaccurate or erroneous information?</li> <li>• How are individuals notified of the procedures for correcting</li> </ul>

	<p>their information?</p> <ul style="list-style-type: none"> <li>• If no formal redress is provided, what alternatives are available to the individual?</li> </ul>
Technical Access and Security	<ul style="list-style-type: none"> <li>• Which user group(s) will have access to the system?</li> <li>• Will contractors to the organization have access to the system?</li> <li>• Does the system use "roles" to assign privileges to users of the system?</li> <li>• What procedures are in place to determine which users may access the system and are they documented?</li> <li>• How are the actual assignments of roles and rules verified according to established security and auditing procedures?</li> <li>• What auditing measures and technical safeguards are in place to prevent misuse of data?</li> <li>• Describe what privacy training is provided to users either generally or specifically relevant to the program or system?</li> <li>• Is the data secured in accordance with organizational Certification &amp; Accreditation requirements?</li> <li>• If yes, when was Certification &amp; Accreditation last completed?</li> </ul>
Technology	<ul style="list-style-type: none"> <li>• Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?</li> <li>• Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.</li> <li>• What design choices were made to enhance privacy?</li> </ul>
Conclusion	<p>The concluding section should inform the reader, in a summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.</p>

## CONTRIBUTION ACKNOWLEDGEMENT

This PIA Guide was developed by the HIMSS Privacy & Security PIA Work Group.

**Mariann Yeager MBA, Work Group Chair**  
Principal  
HIT Professionals Inc

**Kristen (Kris) Knight, JD**  
Director, Privacy Compliance  
Philips Healthcare

**Jonathan D. Bogen MS MBA CIPP**  
President  
HealthCIO Inc

**Nicholas Mankovich PhD**  
Director, Product Security  
Philips Medical Systems

**Katherine Brewer**  
Division of Privacy Compliance  
Office of Information Services  
Centers for Medicare & Medicaid Services

**Erik Pupo MBA**  
Practice Leader  
PPC

**Alan R. Constantian Lt Col, USAF, MSC, CPHIMS**  
Director  
Information Services Design & Development Group  
Centers for Medicare & Medicaid Services

**Hisham Takyeldin**  
Siemens

**Ronda R. Henning**  
Sr. Scientist  
Information Assurance Capability Owner  
Harris Corporation

**Lisa Gallagher**  
Senior Director Privacy & Security  
HIMSS  
Email: [lgallager@himss.org](mailto:lgallager@himss.org)