Common Privacy Framework – Version 2

April 30, 2015

Contents

1 Background

The "Common Privacy Framework (CPF)" was originally developed for the Community Care Information Management (CCIM) Assessment Projects, and was subsequently applied to the Integrated Assessment Record (IAR). The Common Privacy Framework is used by all Health Service Providers (HSPs) who are completing a set of assessments and/or submitting those assessments for sharing in the Integrated Assessment Record (IAR) tool. The CPF provides a framework for the collection, use and disclosure of Personal Health Information (PHI) relating to these assessments. The CPF focuses on the minimum baseline that needs to be achieved when HSPs share a client's PHI to aid the delivery of care or services to that client. HSPs are encouraged to explore ways to continually improve their privacy practices beyond this baseline. Please note that the term "client" will be used throughout this document to refer to clients, consumers, residents and/or patients.

The Common Privacy Framework was originally created based on:

- The experiences of, and feedback from, representative sectors regarding how to address identified privacy operation challenges. Details regarding how this was captured is described in Appendix C – Methodology;
- The analysis of privacy practices in Community Care HSPs, gathered through surveys, focus groups and interviews;
- A review of existing Privacy toolkits and documentation such as Long-Term Care (LTC) and Community Support Services (CSS) Privacy and Security toolkits;
- An in-depth analysis of assessment project documentation and lessons learned from pilot implementations of Assessment Projects, and information gathered through analysis of the privacy practices in community care sectors.

The analysis of privacy practices was conducted with selected volunteer HSPs and the participation for the original version of this framework was limited to representations from various:

- CSS HSPs;
- Community Mental Health (CMH) HSPs;
- LTCH HSPs who are also CSS HSPs, and were thus able to participate in the survey and focus groups with both perspectives in mind.

The following sectors later adopted the Common Privacy Framework to meet their mandatory requirements to participate in IAR.

- LTCH
- Community Care Access Centre (CCAC)

The requirements are analyzed based on current scope and mandate of the projects, which may change with time.

Table 1 below reflects the CPF adoption status based on individual sector and the respective shared assessment types as of December 31st 2014.

CPF Document Version	Sector	Assessments
Version 1	Community Mental Health	Ontario Common Assessment of Need (OCAN)
	Inpatient Mental Health	Resident Assessment Instrument – Mental Health (RAI-MH)
	Long-Term Care homes	Resident Assessment Instrument – Minimum Data Set (RAI-MDS)
	Community Support Services	interRAI Preliminary Screener for Primary and Community Care Settings (interRAI-PS)
	Community Support Services	interRAI Community Health Assessment (interRAI-CHA)
	Community Care Access Centres	interRAI Contact Assessment (interRAI-CA)

Table 1

In March 2015, the IAR Provincial Steering Committee approved a motion to include Coordinated Care Plans (CCP) as another type of assessment, as per Schedule C section I(2)(h) of the IAR Data Sharing Agreement.

This current version of the document is extended to:

- the use of the CPF in Primary and Acute Care Sector's Health Service Providers (HSPs) and the inclusion of CCP as a shared assessment type and;
- provide these HSP's with the necessary information to support the implementation of the CPF and;
- HSPs that have previously implemented IAR and will be participating in the CCT Project. These HSP's have the additional benefit of experience, knowledge and application of the CPF that will be extended for the inclusion of the CCP.

A summary of these changes is reflected in Table 2 below:

CPF Document Version	Sector	Assessments
Version 2	Primary Acute	Coordinated Care Plan (CCP)

Table 2

For more information on the methodology used to build the CPF, please refer to Appendix C.

Moving forward, all HSP's leveraging the CPF should refer to the Common Privacy Framework – Version 2.

2 Why Have a Common Privacy Framework?

"How can I control who sees the information I'm giving you?"

"How do I know my privacy is being respected?"

"Where does my information go?"

Addressing clients' privacy concerns with practical, effective and consistent privacy practices, and ensuring privacy practices align with the expectations of the Information Privacy Commissioner of Ontario (IPC), was identified by health service providers (HSPs) as critical requirements when successfully implementing the creation and sharing of assessments via an electronic tool. Privacy is also vital in ensuring the quality and completeness of the data contained in the various assessments. Research suggests that the more clients are able to trust an HSP to respect their expressed privacy preferences, the more likely they are to provide complete information about themselves.

In this context, privacy is the ability of the assessment systems and processes to enable the client to control how information about themselves is collected, used and disclosed, and feel that he/she is able to exercise that control freely.

Privacy Challenges

Challenges involved in ensuring consistent privacy practices across the community sectors include:

- Multiple assessment projects can serve the same client base yet implement privacy at different times with similar intent but with different tools
- Duplicate and occasionally diverging privacy and security requirements and frameworks from multiple projects can lead to confusion in how to implement privacy protections
- High staff and volunteer turnover rates at HSPs create challenges regarding maintaining awareness and a strong culture of privacy and privacy practices
- HSPs are not always clear if their privacy processes serve their client needs and are appropriate and in alignment with PHIPA and the expectations of IPC. This lack of clarity sometimes results in unbalanced/less than optimal privacy restrictions that negatively impact clinical outcomes
- Diverse client sensitivity about how their information is being used and the privacy implications around information sharing
- Lack of consistent technology to support privacy

In light of these challenges, the Common Privacy Framework was developed to leverage existing processes and tools to better support meeting both clients' privacy expectations and the HSPs' privacy and regulatory requirements.

It is also expected that many of these privacy challenges apply to primary and acute care sectors.

3 What is the Common Privacy Framework?

The Common Privacy Framework (CPF) is a comprehensive framework that was developed in response to HSPs requesting in-depth privacy guidance, especially when sharing assessment personal health information. It was created to support the implementation of Assessment Projects throughout the Community Care Sector including the Integrated Assessment Record (IAR); and later extended for use by Primary and Acute Care sectors for implementation of the Care Coordination Tool (CCT) by the Health Links. It aligns with and supplements other resources, such as the Privacy and Security Toolkits that were developed to support the framework.

Development of the Common Privacy Framework began with identifying the current privacy practices and requirements of community care HSPs as well as the privacy requirements identified in assessment projects. This Common Privacy Framework document addresses those requirements at a high level. Additional support is provided in the form of toolkits which contain implementation guidance and detailed samples and templates.

This approach will benefit clients as they will now be able to confidently receive a consistent level of privacy regardless of where/when services are sought. HSPs will also benefit from this framework as it will provide clear privacy guidelines.

Objectives

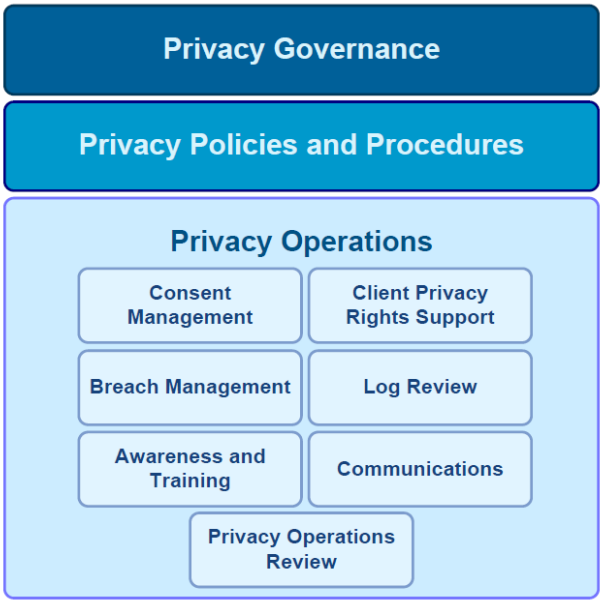
The Common Privacy Framework over-arching objectives are to:

- Understand, identify and address privacy challenges and requirements faced by care sectors
- Facilitate HSP compliance with PHIPA
- Establish a minimum baseline of privacy practices to instill trust that upholds client privacy rights when and where the client seeks care
- Establish a consistent privacy framework across all sectors that are sharing assessments, that is simple, easy to understand and leverages existing tools and processes
- Assist client HSPs in the successful implementation of Assessment Projects

Ultimately the Common Privacy Framework will balance the needs of HSPs to:

- Meet legislative requirements for privacy
- Respect their clients' rights and
- Enable cooperative care planning and service coordination to clients.

4 Common Privacy Framework



Overview

The Common Privacy Framework provides a guideline for the toolkits that will assist HSPs with the implementation of the Common Privacy Framework.

The Common Privacy Framework presents each component of privacy at a high level and is organized into three layers:

- Privacy Governance: Provides privacy strategy and direction, and documents decisions on key privacy issues
- Privacy Policies and Procedures: Defines the specifications for privacy operations according to the direction and decisions from the Privacy Governance layer
- Privacy Operations: Addresses day-to-day privacy issues with processes established by Privacy Policies and Procedures

Each component is in turn divided into three sections:

- *Requirements (what it is)*: A list of the parameters or key elements that must be agreed upon in order for the component to be consistent across HSPs
- *Design (what it looks like)*: A list of the key processes or activities that make up the component
- *Implementation (how to do it)*: A set of the integration steps required to establish the privacy component in an HSP – the steps are divided into those relating to people, processes, and technology. These high-level implementation considerations guide the training, process integration and technology suggestions provided in the supporting toolkits.

Components

5.1 Privacy Governance

Privacy Governance provides privacy strategy and direction, and makes decisions on key privacy issues. Privacy Governance within an HSP should clearly define the structure and processes to establish privacy strategies and directions as well as making strategic decisions on privacy issues.

The HSP senior executive or the HSP board of directors are ultimately responsible for the privacy governance within their organization. The Privacy Officer should be appointed by executive management, report to the executive, and be responsible for managing all privacy related requirements within the HSP.

Framework	Description
Requirements	Governance Structure The privacy officer should be officially appointed by senior management. The privacy officer should be part of senior management or report to senior management. The privacy officer is authorized to and accountable for addressing all privacy related issues within the HSP. Governance Process Senior management sets privacy strategy and direction with recommendations from the privacy officer. Commitment from senior management is critical to the success of the privacy strategy. Example: The goal of the governance process is to make decisions about how privacy should be handled, such as deciding on what kind of consent model is the best one for the HSP and its clients.
Design	The governance process is composed of, but not limited to, the following key activities: Establish privacy governance Privacy governance is established to manage privacy effectively. This includes formalizing the appointment of the privacy officer and assigning the privacy officer as the contact person for privacy issues, as specified by PHIPA s. 15. The privacy officer's reporting structure needs to be clearly defined; and roles and responsibilities must be clearly specified. Example: Inform HSP leadership of any privacy activities, decisions and/or updates by including it as a standard agenda item at regular HSP leadership committee meetings Set privacy strategy Privacy strategy sets direction on overall privacy management and guides the development of the privacy policy and procedures. Privacy strategy should be established based on legislative requirements, business objectives, organizational culture, etc. High-level strategy example: Implement all privacy processes outlined in the Common Privacy Framework in order to achieve compliance with PHIPA.

Framework	Description
	Develop privacy policies and procedures Privacy policies and procedures define the specifications for privacy management and operational activities. Privacy policies and procedures should be aligned with the privacy strategy. Oversee privacy management program Privacy governance should oversee/monitor the privacy management program including program management and operational activities and take action if the privacy program deviates from the privacy strategy, making improvements as appropriate.

Framework	Description
Implementation	People Senior management should officially appoint the privacy officer and ensure all staff within the HSP is appropriately made aware of this role and function. Example: The privacy officer's job description should clearly define the roles and responsibilities of the position. A memo should be sent to HSP staff members announcing the privacy officer, and should include the privacy officer's roles and responsibilities. Process Privacy governance should be integrated with, and be part of, the HSP's overall governance. Technology Technology is not required for the implementation of privacy governance.

5.2 Privacy Policies and Procedures

Privacy policies and procedures define the specifications for privacy operations according to the directions and decisions from the Privacy Governance layer.

Framework	Description
Requirements	Policy A privacy policy should be developed to provide clear direction on privacy practices. Privacy procedures are created based on what is established in one or more policies. Example: A small HSP may need to have one broad privacy policy that identifies the privacy requirements and associated procedures, whereas a larger HSP may need to have separate policies to address privacy issues to deal with the complexity of the HSP's working environment. Procedures

	The following minimum baseline privacy procedures, which are described in subsequent sections of this document, should be established: • Consent Management • Client Privacy Rights Support • Breach Management • Log Review • Awareness and Training • Privacy Communications • Privacy Operations Review Approval • All privacy policies and procedures should be approved by senior management.

Framework	Description
Design	Policy and Procedure development is composed of, but not limited to, three key activities: Develop privacy policy Privacy policy should be developed in accordance with privacy strategy, and clearly describe the direction from senior management regarding key privacy requirements. Establish privacy procedures Privacy procedures provide guidance on both privacy management and operations, and specify the activities and workflow that deal with specific privacy issues. Example: HSPs should leverage existing procedures where appropriate or develop new ones to address new privacy requirements identified in this framework. Review and approve policy and procedures The privacy policy and procedures must be reviewed and approved by senior management and updated. Examples of when an update would be required include changes to legislation, operational changes, changes in organizational culture, etc.
Implementation	People Privacy awareness training should be provided to all staff and any third party who may have access to PHI in the HSP. The training should include information on new policy and procedure elements, and provide examples of expected behaviour as well as unacceptable practices. Specific training on the privacy procedures should be provided to any staff involved in these procedures. Example: Only staff involved in breach management procedures should be trained on breach management procedures, whereas all staff should be trained in consent and client privacy rights procedures. Process The privacy policy and procedure development should be consistent with the HSP's existing policies and procedures. Any changes to pre-existing policies and procedures must be incorporated. Technology Technology is not required to implement the privacy policy and procedures.

5.3 Privacy Operations

Privacy Operations are the set of ongoing activities that address all day-to-day privacy issues. For example, privacy operations include consent management to manage the client's consent for the collection, use and disclosure of personal health information. The privacy officer will be able to successfully provide consistent and continuous support to business operations if privacy operations are well established and managed.

Operations should be defined and documented to standardize the workflow, activities, and roles and responsibilities in accordance with the direction of the privacy policy and procedures. Privacy Operations include the following components:

- Consent management
- Client privacy rights support
- Breach management
- Privacy operations review
- Log review
- Awareness and training
- Privacy communications

Consent Management

HSPs must implement a consent management process to manage consent and consent directives in compliance with the Personal Health Information Protection Act (2004).

The consent management framework adopted by the HSP should be based on the legislative requirements. It should also take into consideration the HSP's culture, business practices and processes, technical capabilities, administrative landscape, and the specific needs of its client base. To enable PHI sharing across HSPs, a baseline consent management framework must also be established. The baseline consent management framework helps to establish the trust between participating HSPs that a client's privacy is being respected and shared appropriately. An optimal consent framework baseline is comprised of the following:

Framework	Description
Requirements	Consent Type Informed Consent (either implied or express) Consent can be either implied or express, but in order to be valid the consent must be knowledgeable and for the purposes of this framework, informed. Knowledgeable consent is defined under PHIPA (see appendix B for more details) as requiring the client to know: (a) the purposes of the collection, use or disclosure, as the case may be; and (b) that the individuals may give or withhold consent. In this framework, we define informed consent as knowledgeable consent as well as: • The client should be aware of the information that is collected, used and disclosed • Clients should be aware of the positive and negative consequences of giving, withholding or withdrawing consent • The HSP must be reasonably certain that the client understands the information provided to them • The person is well informed enough to ask any clarifying questions, and has received responses to his or her requests for additional information Example: The client may be informed verbally, in writing through posters or brochures, or through any means deemed necessary for them to understand. Whether the client is asked directly to provide consent or is not explicitly asked for their consent to the collection, use and disclosure of their PHI is up to the HSP's discretion as long as the client is informed. Scope of Consent Directives

	Each HSP should determine the scope of consent directive that they are able to support. HSPs should communicate this with all clients so that clients can make informed decisions on consent. At minimum an HSP's privacy policy and practice should support a Client's consent directive applied to their entire PHI. HSP's are encouraged to explore ways of refining the scope of the consent directive. Example: If an HSP's electronic health record software is not able to hide a specific section of the client's health records, then the HSP must inform the clients that their consent will be applied to the whole health record so their consent will either be "share all" or "share nothing". Consent Directive Override Express consent is required to override the consent directive. Example: If the client has withdrawn their consent and the client has been referred for treatment to another HSP, the HSP must expressly ask the client to see their PHI since the client previously withdrew their consent. The Client's PHI cannot be assumed to be shared, even though a referral would normally include PHI. Disclosure without Consent As per PHIPA Section 40(1), "Health information custodians may disclose a patient's PHI without consent where the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons", clients should be informed that disclosures may occur in situations where the HSP staff believe that it is necessary to avoid serious bodily harm.

Framework	Description
Design	The consent management process is comprised of, but not limited to, three key activities: Inform the Client Regardless of whether the HSP uses implied or express consent, the client must be informed of the purpose for the collection/use/disclosure of their PHI, as well as their privacy rights. The HSP can take a different approach to inform the client depending on their business process, the client's preference, etc. Obtain Consent Once the client is informed of the purpose of PHI collection/use/disclosure and their privacy rights, the HSP can use their existing consent practices to assume implied consent or obtain express consent. Manage Consent The consent must be properly documented for tracking purposes. Appropriate actions should be taken to ensure that the consent is registered in an electronic system or recorded on physical media along with PHI. Examples of physical media might include hard copy documents, spreadsheets, lists, reports, etc. Example: Maintaining a log book, or excel spreadsheet of when consent was obtained or withdrawn will make maintaining traceability of consent directives across programs, paper files and software files easier.
Implementation	People All staff must receive proper training on the consent management process. Partner HSPs must be informed of the changes to the consent management process, should they occur or be required. The public, including clients, must be informed of the HSP's privacy practices, including the consent process. Process The HSP's consent management process must be integrated with the HSP's clinical and/or assessment process. When PHI is shared externally with other HSPs, consent management processes must be established between organizations to ensure effective collaboration and cooperation occurs. Example: If a HSP's standard consent process is to inform clients verbally, the discussion should be integrated into the HSP's intake or assessment process. Technology If HSPs have current technology that registers and enforces the consent directive but use a manual procedure to obtain express consent, a process needs to be in place to ensure that the manual procedure aligns with the technology functions regarding consent. Example: When a client withdraws consent and that consent directive is captured manually, there needs to be some way for the electronic system to register that the client does not want their information shared, and for the electronic system to enforce and not show that information to anyone.

Client Privacy Rights Support

HSPs have an obligation to:

- Provide access to a client's PHI to the client upon the client's request
- Respond to a client's request for a correction to their PHI
- Address a client's challenge or complaint concerning compliance with privacy legislation

The client privacy rights support component of the Common Privacy Framework fulfills these obligations.

Under the Personal Health Information Protection Act, individuals have certain rights to their PHI. Specifically, they have a right to:

1. Access their record.
   Sections 52 through 54 states that an individual has a "right of access" to their record of personal health information. These sections also state that the HSP must provide a response within 30 days and if the individual believes that the HSP has refused or is thought to have refused the request, they have the right to file a complaint with the Information and Privacy Commissioner.

2. Change/correct information within their record.
   Section 55 states that an individual may request that the custodian correct their record, if the individual believes the record is inaccurate or incomplete. In this case as well, the custodian must grant or refuse the request within 30 days, and if the individual believes that the HSP has refused or is thought to have refused the request, they have the right to file a complaint with the Information and Privacy Commissioner.

3. File a complaint with the Privacy Commissioner regarding an HSP's privacy practices.
   Section 56 of PHIPA states that an individual has the right to file a complaint with the Information and Privacy Commissioner if they have "reasonable grounds" to believe that someone has contravened or is about to contravene a provision of the Act. Applying this right to these circumstances, an individual has the right to file a complaint if they believe that the Custodian has sub-standard privacy practices or they have failed in someway to protect their privacy.

Client privacy rights support identifies responsibilities and clearly delineates the tasks that should be put in place within any given HSP and the tasks which are introduced when HSPs begin to share PHI with other HSPs.

Framework	Description
Requirements	Access Personal Health Information

	A client can request access to their PHI from an HSP. The HSP must provide a response to the client within 30 days of the request or ask for an extension of 30 days (within 30 days from the original request). Change Personal Health Information A client can request change or correction to their PHI from a Health Information Custodian. The HSP must provide a response to the client within 30 days of the request to change PHI or ask for an extension of 30 days (within 30 days from the original request). Correction of Personal Health Information The HSP, if satisfied with the client's demonstration that the record is incomplete or inaccurate, will take appropriate action to correct it. The HSP, if not satisfied with the client's demonstration that the record is incomplete or inaccurate, must create a "statement of disagreement" (describing the client's request as well as the HSP's opinion) and add it to the client's health record. File a Privacy Complaint A client can file a complaint about the privacy practice of a HSP, if the client believes that the HSP has sub-standard privacy practices or they have failed in some way to protect their privacy.
Framework	Description
Design	The client privacy rights support process is comprised of, but not limited to, four key activities: Request/Complaint Under PHIPA, the client can make a request to an HSP to access or change their PHI. The client also has a right to file a complaint regarding the privacy practice of the HSP. The client must make the request or complaint in writing. Escalation If the request to access or change PHI involves other HSPs, the HSP should identify the other HSPs involved. Then the HSP should either provide the list of HSPs to the client so the client can make his/her request, or facilitate the request on behalf of the client. Handling If the request to access or change the PHI or the complaint relates solely to information in the custody or control of a single HSP, local privacy process at the HSP will be used to respond to the client. Reporting In a shared environment, a participating party such asa Health Information Network Provider (HINP) will coordinate the activities among all involved HSPs when a client's privacy request/complaint involves multiple HSPs.
Implementation	People

	In both an electronic and manually sharing environment, changes to any participating HSP both at the human resource and business process level must be communicated among members to ensure the response to client privacy request/complaint is properly coordinated and managed. Process If the request to access or change the PHI or the complaint relates solely to information in the custody or control of a single HSP, local processes are leveraged. When a client's request/complaint involves multiple HSPs, the HSPs in the sharing environment need to coordinate and communicate prior to their response to the client. Integrated processes must be put in place for the HSPs to work together on a unified response. Technology The technology to collect, use and disclose PHI should provide the functionality to facilitate the response to a client's request or complaint. Example: Assessment software should permit the user to print out or show the client their assessment upon request. Adopting technology to maintain the client's request/compliance registry is a priority. Example: Maintaining a spreadsheet of client requests and complaints, how they are resolved, at what date, and by whom.

Breach Management

Breach management is the end-to-end management of a privacy breach or security incident that affects the privacy of personal health information.

An incident is the contravention of a policy, procedure, duty or contract, or a situation that results in the potential exposure of sensitive personal information and/or personal health information to unauthorized parties.

Examples of privacy breach and security incidents that may occur in a shared environment:

- A printed assessment record is left in a public area (e.g. a coffee shop or restaurant)
- Theft, loss, damage, unauthorized destruction or modification of assessment records
- Inappropriate access to assessment records by unauthorized users
- A large number of health records are accessed by a single individual in a short period of time (out of the ordinary)
- A user account and password is compromised which results in unauthorized access to PI/PHI
- Violation of privacy policies or procedures

A privacy breach can be identified and/or reported from inside the HSP or outside the HSP by, for example, the client, the organization in its role of HINP who hosts the sharing system, or any other individual.

The Information and Privacy Commissioner (IPC) of Ontario recommends that HSPs develop a privacy breach protocol to handle any potential privacy breach (for more information, see the IPC breach guidelines brochure at http://www.ipc.on.ca/images/Resources/hprivbreach-e.pdf). The protocol enables the HSP and their partners in the same sharing environment to respond quickly and in a coordinated way during a privacy breach. The protocol also defines the roles and responsibilities of each party in the sharing environment, so that investigation and containment of a breach are more effective and efficient, and remediation will be easier to implement.

Framework	Description
Requirements	Breach Detection Breaches can be detected and reported by internal staff, Service Providers, clients, partner HSPs, and other third parties. *Example: A clerk from a retail store calls to ask the HSP to: "Please stop faxing us", identifying that PHI has been faxed to an incorrect telephone number instead of the intended HSP. This alert constitutes a breach which should immediately initiate the breach handling protocol.* Breach Notification The following parties should be notified in the event of a breach: • Client • Originating HSP who shared the PHI • Service Providers who provides the electronic system for hosting and/or sharing PHI, where applicable • Information and Privacy Commissioner of Ontario (IPC) or the HSP's board as appropriate Breach Reporting All breaches should be recorded and logged once detected and a report developed to document the resolutions, corrective actions and lessons learned. The report or the summary of the report should be distributed to the affected parties. *Example: The privacy officer should maintain a file or spreadsheet that indicates when a breach was identified, who was notified, what was done to resolve the breach, and any other changes made to the HSP's procedures in order to avoid other breaches.*

Framework	Description
Design	The breach or incident management process is comprised of the following activities: Detection Each participating HSP and HINP should have a defined means of incident detection and monitoring process. This mechanism should allow their staff, clients or third parties to report incidents or breaches to the HSP. Escalation When an incident or a breach is detected or reported to a participating HSP in a sharing environment, the HSP should conduct initial triage to determine the impact to the HSP or the HINP. If the incident or the breach affects more than one HSP in the sharing environment, the incident needs to be escalated to all other affected HSPs. The HINP should also be involved to coordinate investigation and response. Breach Handling Each participating HSP should have their own internal incident management process to investigate, contain and recover from the breach. When an incident is escalated to the most responsible HSP, that HSP will activate its internal incident management process to handle the incident. Breach Notification Once the breach is contained, each HSP should notify all affected parties, including the clients as required by PHIPA. Reporting Once an incident is resolved, resolution details should be kept in a centralized incident registry. This will help the HSP to learn from past experience by gathering information for management reporting.
Implementation	People In environments where information is shared - both electronic as well as 'paper-based', changes to any participating HSP both at the human resource and business process level must be communicated to their members. This ensures the integrated breach management process is kept up-to-date and can give quick, accurate access to information regarding any potential incident and breach. Regular gathering among the privacy officers (or roles of similar capacity) should help to cultivate an environment that encourages information sharing and process improvement. Process The breach management process should focus primarily on collaboration and cooperation with the other affected parties in the same sharing environment, whether PHI is shared physically via fax or hand delivery, or an electronic sharing system.

	In an electronic sharing system, the HINP is in the best position to establish the process to coordinate the breach management activities among participating HSPs. Individual HSPs must interface internal breach management processes with the HINP breach management process. For the sharing via fax or hand delivery, the party who receives PHI from or sends PHI to, your HSP should be the central interface in the breach management process. Technology Any manual procedure, such as completing an incident or breach report, gathering information, communicating with other affect parties by phone, must be able to integrate with technology whenever possible for both electronic and manual sharing environments. The HSPs and HINP need to consider adapting their integrated breach/incident management process with their electronically sharing system environment and any computer network technology.

Privacy Operations Review

Privacy Review seeks to provide reasonable assurance that the privacy operations are performed effectively and consistently according to the defined procedure.

Depending on the HSP environment and resource availability, there are many different approaches to perform a privacy operations review, from HSP self-assessment with a simple checklist to sophisticated control testing.

Privacy officers can also engage various resources to perform a review, including but not limited to:

- Assigning privacy resources
- Engaging internal review departments
- Contracting to a third party consulting firm

Framework	Description
Requirements	Objective The objective of the privacy operations review is to ensure the privacy operations are carried out consistently with the defined processes. Approach The privacy operations review should include, but is not limited to, the following activities: • Interview with personnel involved in privacy operations • Identifying, collecting and verifying samples of privacy practices Frequency Privacy review should be performed at least on an annual basis or whenever violation of the privacy policy is detected or privacy breach occurs.

Framework	Description
Design	The privacy operations review is comprised of, but not limited to, three key activities: Develop a privacy operations review plan A privacy operations review plan should be developed to specify the scope, objectives and approach for the review. The privacy operations review plan should be approved by senior management and shared with the affected parties prior to the review. Example: A checklist that lists all the HSP's privacy policies and procedures could be used to verify if those policies and procedures are being followed. The checklist could include a checkbox that includes: "Has every staff member been trained as per the scheduled outlined in the awareness and training procedure?" Execute the review The privacy operations review should be performed based on the approved review plan. All findings have to be validated with the affected parties. Report the findings All findings must be clearly documented in a report, including the impact, risk rating and recommendation. The review report should be presented to senior management and affected parties. Monitor the corrective actions All issues identified in the review must be assigned to an owner who is responsible to take corrective actions to resolve the issues. All issues should be closely monitored and tracked until they are closed.
Implementation	People Affected parties should be informed on the privacy operations review requirements and processes. Process Privacy operations review may be performed by the privacy officer. However, if the HSP has an independent performance review department, it may be more effective for the review department to perform the privacy operations review with the assistance from the privacy officer. The privacy operations review process should be integrated with the HSP's audit processes. Technology Technology is not required.

Log Review

The Personal Health Information Protection Act (PHIPA) requires that access to health information be on a need-to-know basis. To meet this requirement, HSPs are required to have controls in place that regulate

access and log activity as well as procedures to regularly review the logs and user access activity. Access logs play an important role in this access review process and during breach investigations.

Different HSPs will have logs of varying technology and complexity, and the privacy officer should identify which logs may be useful when identifying a privacy breach, and develop a plan to review those logs. The privacy officer is accountable for ensuring that the log review is performed. If required, the privacy officer may choose to involve IT support or other staff to help perform this review in order to adhere to HSPs internal operation requirements and procedures.

Framework	Description
Requirements	Inventory Logs The Privacy Officer should make a list identifying: • What logs are already kept that may indicate access to personal health information • What additional procedures are necessary to monitor access to personal health information *Example: Even if no software is used, client sign-in sheets when cross-referenced with staff schedules can provide useful information. When software is used to collect, use or disclose PHI, the software should have the ability to log user activity.* Determine Approach The HSP should determine what the best approach to reviewing should be, including which logs should be reviewed as well as what to look for. The approach to reviewing logs should be based on the risk level of the HSP's environment. *Example: The following may be considerations for how often to do a log review:* • *The complexity of the HSP's environment. i.e.: The more clients, staff or PHI, the more opportunities for breaches.* • *Frequency of breaches. Few breaches can be an indication of lower risk of breaches. However, HSPs should use caution in using low frequency of breaches as the sole basis for determining how often to do log review since lower frequency may also be an indication that breaches are going undetected.* Determine Frequency The HSP should determine how often logs should be reviewed. *Example: Depending on size and volume of logs as well as available resources, logs should be reviewed on a daily, weekly or monthly basis.*

Framework	Description
Design	Log review planning is comprised of, but not limited to, three key activities: Define the Log Review Plan The HSP should create a plan to inventory and determine the approach and frequency for log review including identifying key roles within the HSP that will be responsible for log review. In order to develop the log review plan, the HSP should analyze the level of risk of breaches, i.e.: what is the sensitivity of the PHI that is being accessed, how many staff and other people have access to it, how aware of privacy those individuals are, etc. *Example: HSPs who have a process for signing confidentiality agreements and providing regular privacy training may have a plan that reviews the log less frequently than an HSP who does not have these processes established.* Institute Log Review Plan The HSP should roll out their log review plan and institute any new procedure, and identify all necessary touch points and escalation procedures for when routine review of logs identifies an issue or breach. Determine Log Review Improvement Plan After log review has been implemented for a few months, the HSP should consider whether the log review plan is meeting objectives and if there is any way to improve the procedure.
Implementation	People All staff involved in log review must be trained in when and how to review logs, which logs to review, and what to look for. Process Log review activities should be closely integrated with the breach management process, thus when an event that has potential of misuse or a breach is detected, the proper breach or incident management process can be triggered and the appropriate personnel can be notified. Technology The main consideration of implementing logging is to ensure the log has the capability to capture the widest range of events, and the information it captures provides comprehensive details about the events. This is essential when conducting effective security, compliance and breach investigation.

Awareness and Training

Privacy awareness and training raises the privacy awareness of all staff, volunteers and anyone else that handles or accesses PHI. It provides the knowledge and skills required to manage client privacy.

The purpose of awareness and training is to ensure that:

- All staff understand and practice the appropriate collection, use and disclosure of PHI
- All staff understand and acknowledge individual user roles and responsibilities relating to privacy
- The HSP is in compliance with applicable legislation and standards (e.g. Personal Health Information Protection Act 2004)
- Staff, volunteers, and other applicable parties understand the importance of privacy and how to protect it.

Framework	Description
Requirements	Audience All internal staff including senior management, clinicians/physicians, third party staff, volunteers and anyone else who handles or accesses PHI. Mechanism In-classroom training, online training, quizzes, posters, brochures, newsletters, emails. Content Privacy legislation and principles, organizational privacy policies and procedures, changes to the privacy practices.
Design	Awareness and training is comprised of, but not limited to, three key activities: Develop an awareness and training plan An awareness and training plan should be developed to promote the awareness of privacy within the HSP. The awareness and training plan should cover various audience groups, delivery mechanisms for different audiences and contents specific to each audience. Develop contents Content should be developed for different audiences. In general, the awareness and training should communicate the privacy principles, privacy legislations, organizational policy and procedures and requirements specific to the HSPs. Deliver the awareness and training Awareness and training should be delivered via appropriate channels that maximize the impact of the message. *Example: Use posters and brochures for all staff and volunteers, and use additional classroom based training for specific staff who interact with clients on a daily basis.*
Implementation	People All staff should, at a minimum, receive privacy awareness training annually. Customized training should be provided to the staff involved in privacy processes. Process Privacy awareness and training should be consistent with the HSP's general training strategy and following the existing training management processes, including development, approval, delivery, etc. Privacy awareness and training should be integrated with the HSP's training management process. The privacy officer should work with the HSP's training department if there is one, to integrate the privacy awareness and training into the HSP's training management process. Example: If you have an orientation for all new staff and volunteers, include privacy awareness as part of that orientation. When you refresh the orientation once or twice a year, refresh the privacy training as well. Technology

	Technologies such as public websites, e-learning platforms and email can be utilized to deliver the privacy awareness and training to the right audience. Existing technologies in the HSP should be considered when establishing the awareness and training strategy.

Privacy Communications

The success of a privacy program depends on the positive perception and confidence that personal information and personal health information of clients is well protected. Privacy communications plays a major role in establishing the confidence and trust with the HSPs and clients. Privacy communications is the set of activities involved in managing and orchestrating all internal and external privacy communications with the goal of informing the stakeholders of privacy practices, building a reputation for privacy management, and establishing trust with stakeholders and clients.

The objectives of privacy communications are to:

- Establish broad awareness among stakeholders and clients of the HSP's privacy practices
- Communicate clear, concise and timely communications using multiple channels
- Maintain a forum for ongoing communication with key HSPs including support for current initiatives
- Work collaboratively with all key stakeholders to communicate and improve the understanding of HSP's goals, value and benefits from privacy perspective
- Communicate the benefits of sharing information and exchanging data
- Identify and publicize best practices and success stories in the privacy practices
- Ensure timely, consistent, clear and coordinated messages.

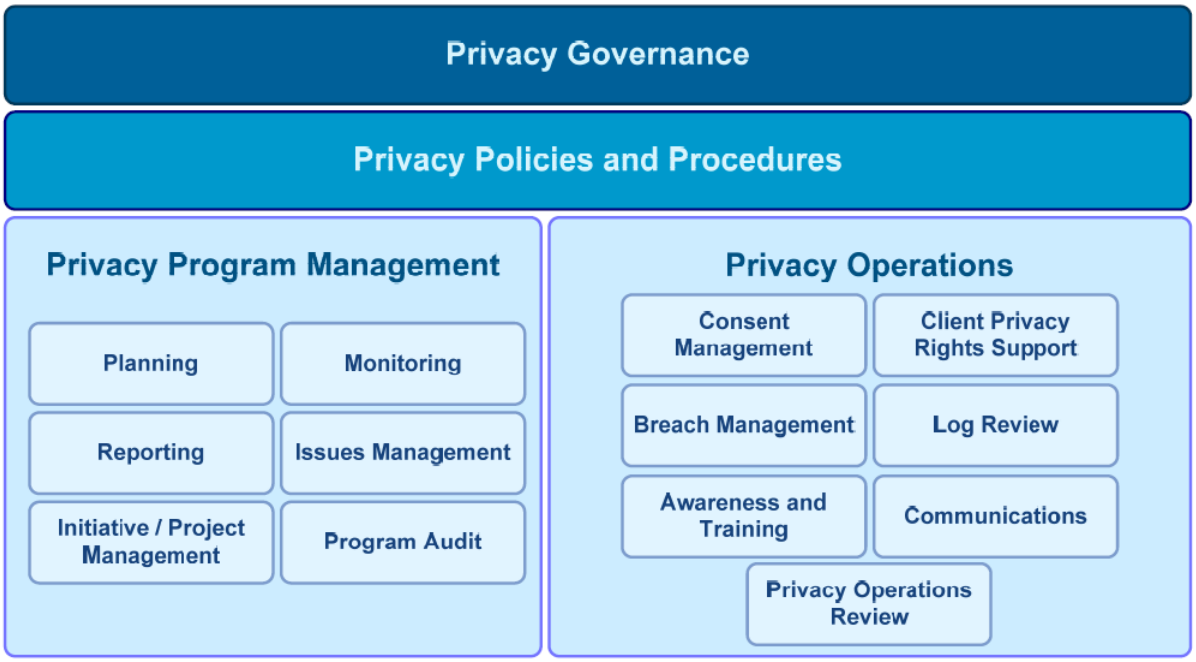
Framework	Description
Requirements	Audience General public, clients, partners, internal staff, families as defined by the client. Mechanism HSP's website, poster, brochure, newsletter, emails. Content Organizational privacy practices, informed consent, changes to the privacy practices. *Example: The HSP should publish a description of their privacy practices on their website or on a poster in their facility, as required by PHIPA.*
Design	Privacy Communications is comprised of, but not limited to, three key activities: Establish a communications plan A privacy communications plan should be developed to communicate privacy practices with clients and the general public. In the communications plan, targeted audiences must be clearly identified; delivery mechanisms for different audiences group should be determined; contents for different audience have to be specified. Develop content Content should be developed for different audiences. In general, the content should cover the HSP's privacy practices, consent management and changes to the privacy management.

	Deliver the message Key messages should be delivered via the most appropriate means to maximize impact. For example, a message to the general public should be published on the HSP's website and messages to clients should be delivered via posters and brochures or in person.

Framework	Description
Implementation	People General privacy messages should be communicated with all internal staff on a regular basis. Process Privacy communications should be consistent with the HSP's general communications strategy and follow the existing communication processes, including review, approval, publishing, etc. Privacy communications should be integrated with the HSP's communications process. Privacy officer should work with Communications to integrate the privacy communications into the HSP communication process. Technology Technologies such as a public website and email can be utilized to deliver privacy communications to a broad audience. Technologies in the HSP should be considered when establishing communication strategy.

Appendix A — Common Privacy Framework

An example of a comprehensive privacy framework based on industry best practices is included below for reference purposes. The Common Privacy Framework described in this document has leveraged the reference framework below according to the priorities identified during requirements gathering.



Appendix B —Glossary of Acronyms and Definitions

CAP	Common Assessment Projects, a term sometimes used by CCIM to refer to the assessment projects ongoing in the CCAC, CSS, CMH&A and LTCH Sectors.

CCAC Community Care Access Centres.

CCP Coordinated Care Plan

CCT Project A term used to refer to the Coordinated Care Tool project that is implementing to select Health Links and HSPs in community, primary and acute care sectors.

CMH / CMH&A Community Mental Health / Community Mental Health & Addictions.

CPF Common Privacy Framework, a term that applies both to this document as well as to the overall initiative that includes this document and the supporting toolkits.

CSS Community Support Services.

Client As noted earlier, the word "Client" is used throughout this document to refer to clients, consumers, residents and/or patients.

Consent Consent is defined in PHIPA PART III, under sections 18 – 28.

Under PHIPA section 18(1)(b) in order for consent to be valid; consent must be knowledgeable. Knowledgeable consent is defined in section 18(5) as: A consent to the collection, use or disclosure of personal health information about an individual is knowledgeable if it is reasonable in the circumstances to believe that the individual knows,

(a) the purposes of the collection, use or disclosure, as the case may be; and

(b) that the individual may give or withhold consent. 2004, c. 3, Sched. A, s. 18 (5).

For the purposes of the Common Privacy Framework, we define informed consent based on the above definition of knowledgeable consent as well as specifying that:

- The client should be aware of the information that is collected, used and disclosed
- Clients should be aware of the positive and negative consequences of giving, withholding or withdrawing consent
- The HSP must be reasonably certain that the client understands the information provided to them
- The person is well informed enough to ask any clarifying questions, and has received responses to his or her requests for additional information.

Consent can be either implied or express, but in order to be valid the consent must be knowledgeable and for the purposes of this framework, informed. Once the client has been informed, here are two explanations of Implied Consent and Express Consent:

- Implied Consent – Implied consent refers to situations in which it is reasonable to infer that the client is consenting by the action that they have taken, and it is not necessary to specifically (or expressly) ask for the client's consent. For example, when a client allows their blood to be drawn at a medical laboratory, it is implied that they consent to the results of their blood work to be disclosed to the ordering clinician. Similarly in community care, when a client fills out an intake form that clearly identifies the purposes of the form and what it will be used and who it will be shared with.
- Express consent – to the collection, use or disclosure of personal health information by a health information custodian is explicit and direct. It may be given verbally, in writing or by electronic means.

HSP	Health Service Provider – A person or entity that meets the criteria set out in the Local Health System Integration Act, 2006. CCIM uses health service provider (HSP) in the context of organization. The Act is online at: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_06l04_e.htm
HINP	A Health Information Network Provider – Under PHIPA, HINP is defined as "a person [or organization] who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians." O. Reg. 329/04, s. 6 (2).
HIC	Health Information Custodian: A health information custodian is a listed individual or organization under PHIPA that, as a result of his or its power or duties, has custody or control of personal health information.
IAR	Integrated Assessment Record - The IAR is a viewer that enables HSPs to access common assessment data from participating care sectors in a secure and accurate manner. It allows information to be viewed electronically using a single source of assessment data, improve information management and enable collaborative care planning.
LHIN	Local Health Integration Network.
Log Review	PHIPA requires that access to PHI be on a need to know basis. To meet this requirement, organizations are required to have controls in place that regulate access and log activities, as well as procedures to regularly review the logs and user access activities. Audit Logs play an important role in this access review process and during breach investigations.

PHI — Personal health information – Information, in oral or recorded form, which identifies an individual. Under PHIPA, Personal Health Information is defined as information that:

- Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
- Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual;
- A plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;
- Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;
- Relates to the donation by the individual of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily substance;
- Is the individual's health number; or
- Identifies an individual's substitute decision-maker.

PHIPA — The Personal Health Information Protection Act, 2004 sets out rules to protect a patient's personal health record across the health system.

Privacy — The right of an individual to control the collection, use and disclosure of his/her Personal Information; freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.

Privacy breach — Includes the theft or loss of PHI as well as the access or modification of PHI by unauthorized persons.

Stakeholders — Stakeholders include participating health service providers who perform or are involved in assessments, particularly in the sectors Community Support Services, Community Mental Health and Long-Term Care Homes.

Appendix C — Methodology and Requirements Used to Build the CPF

Common Privacy Framework Methodology

The methodology used to develop the Common Privacy Framework is detailed below.

Oversight Model

A model to provide oversight for the Common Privacy Framework was established in order to gather feedback from participating sectors from both a sector-specific and province-wide perspective.

The objectives of the oversight model was:

- To incorporate feedback on the framework and supporting toolkits from participating sectors, and
- To ensure that the framework and supporting toolkits were implementable across all sectors.

Sector Current Privacy Practices Analysis

An analysis of Current Privacy Practices in community care sectors was conducted using an on online privacy survey with follow up in the form of in-person focus groups.

The objectives of the current privacy practices analysis were to:

- Identify the diverse existing privacy practices within participating Community Care HSPs
- Understand the challenges that HSPs encounter in implementing privacy protection
- Identify the existing tools, resources and lessons learned within the sectors, and Gather privacy requirements for the Common Privacy Framework.
- Gather privacy requirements for the Common Privacy Framework.

Assessment Project Requirements Gathering

In addition to gathering requirements directly from HSP stakeholders, a thorough analysis of Assessment projects to date was conducted through a detailed review of project documentation and lessons learned.

The objectives of the project requirements gathering were to identify and leverage:

- Lessons learned from Assessment projects with regards to privacy
- Existing privacy tools and resources provided to Assessment projects
- Privacy implementation challenges from cross-HSP perspective and
- Privacy requirements for the Common Privacy Framework from a project perspective.

CPF Development

Once key requirements were identified from the information gathering activities, the Common Privacy Framework was developed and focused to meet those requirements.

A key objective of the Common Privacy Framework was to establish a baseline that is acceptable to all stakeholders by prioritizing and focusing on the requirements needed across projects and sectors rather than trying to address all potential privacy issues.

Review Common Privacy Framework

Once the Common Privacy Framework draft was developed, it was reviewed for comment by participating sector HSPs as per the oversight model. Specifically, the Common Privacy Framework was:

- Reviewed in detail by sector-specific working groups, and their feedback documented; then
- Presented, along with the sector-specific feedback, to the sector steering committees for further guidance; then
- Discussed at the Provincial Working Group with representatives from participating sectors as well as LHIN and eHealth representation to ensure that changes made based on feedback was acceptable to all sectors

The objectives of this review were to:

- Get cross-sector consensus on the Common Privacy Framework
- Provide an agreed upon framework, that is PHIPA compliant, for the supporting toolkits that were subsequently developed

Develop Toolkits

Once the framework was reviewed and agreed upon, supporting toolkits were created to:

- Assist the implementation of the framework
- Minimize the effort required by HSPs to implement the framework

The toolkits included:

- Implementation guides
- Training materials
- Sample policies, procedures, forms, scripts as well as other materials

and:

- Leveraged existing privacy processes and tools where possible, including building upon and supplementing existing privacy toolkits
- Introduced minimal change to existing processes where possible

- Recognized the change management considerations HSPs undergo as they adopt the Common Privacy Framework
- Provided simple, easy to use, easy to understand templates and materials to make the integration of a common privacy framework as simple and seamless as possible

Review Toolkits

Once toolkits were developed they were reviewed and/or used by participating sector HSPs to ensure that:

- Tools met the stated requirements and
- Tools were straightforward and could be readily implemented and maintained

Leveraging Toolkits

An extensive Privacy & Security toolkit was developed and used for the implementation of the IAR to over 1,200 HSPs. The toolkit will be leveraged by subsequent projects and care sectors in the context of creating and sharing assessment information amongst HSP's for the purposes of providing care.

Common Privacy Framework Requirements

The requirements for the Common Privacy Framework were based on the analysis of privacy practices of Community Care HSPs which were gathered through surveys, focus groups and interviews as well as an n-depth analysis of assessment project documentation and lessons learned. Privacy toolkits and documentation were reviewed to identify other key requirements.

The requirements presented in this report are summarized specifically for the Common Privacy Framework. The requirements specific to the tools that support the framework are presented in the supporting toolkits documentation.

HSP Requirements

Here is a high level summary of requirements identified from the HSPs' perspective for the development of the Common Privacy Framework.

Ref #	Requirement
HSP-01	Should use simple, clear, and straightforward language.
HSP-02	Should be sufficiently high-level and flexible that it can be readily adapted to local processes.
HSP-03	Must address privacy awareness and training of various audience groups, broad privacy topics and different delivery channels.
HSP-04	Should address the need for privacy policies and procedures.
HSP-05	Should include consent management that covers the lifecycle of the consent directive as one of the key components.
HSP-06	Should accommodate HSPs that use Implied consent and/or Express consent.
HSP-07	Should address consent collection as well as the recording, management, updating and communication of consent directives.

HSP-08	Should support both the use of electronic and physical consent capture/management.
HSP-09	Should support Breach and incident management.
HSP-10	Should include public communication.
HSP-11	Should be flexible enough to accommodate existing policies for client privacy rights support.

Assessment Project Requirements

These high level requirements were gathered from Assessment projects' perspective from project documentation and lessons learned.

Ref #	Requirement
Project-01	Should be in clear and 'easy to understand' language.
Project-02	Must be 'scalable' and equally applicable to large and small HSPs.
Project-03	Must be 'sustainable' and should include provisions for on-going support.
Project-04	Should identify the rationale behind particular recommendations and approaches including the limits, intentions and legal underpinnings.
Project-05	Should support and supplement existing tools, policies and resources.
Project-06	Should include governance including the privacy officer role and reporting structure as one of the key components.
Project-07	Should include consent management that covers the lifecycle of the consent directive as one of the key components.
Project-08	Should support informed consent.
Project-09	Should provide support for Breach management.
Project-10	Should include and provide guidance on log review activities.
Project-11	Should address the public privacy communication requirements of the projects.
Project-12	Should address the privacy operations review requirements of the projects.
Project-13	Should include the process to manage the client's request to access or make changes to their PHI or file a complaint on the HSP's privacy practices.