eHealth NSW

NSW GOVERNMENT

Version 2.1 March 2023

Privacy and Security Assessment Framework (PSAF) Customer Guide

Document history

Version no.	Version date	Description
1.0	02/12/2022	Initial version at launch of new SARA process.
1.1	20/12/2022	Minor text updates in relation to Demands.
2.0	15/03/2023	Updated to align with latest SARA form enhancements. Added further clarification regarding the use of ‘Final’ vs ‘Estimated’ Cost Calculator records.
2.1	23/03/2023	Additional information added to Step 2 under Initiating a PSAF security assessment about requesting Final vs Estimated costs.

eHealth NSW

NSW GOVERNMENT

Contents

1. Introduction

1.1 What is PSAF?

The Privacy and Security Assessment Framework (PSAF) is a security assessment that evaluates NSW Health technology solutions to ensure they are compliant with legal and regulatory frameworks and to identify potential security risks. Depending on the type of information handled by the solution, a privacy component may also be included in the assessment.

Its aim is to prevent avoidable risks by ensuring information security controls are built and embedded into the project. The earlier these risks are identified, the more effectively they can be managed and mitigated.

1.2 Why is PSAF needed?

Information security is becoming increasingly important as NSW Health moves from paper-based to digital systems. More information than ever is being contained in our systems and it is often of a sensitive nature.

PSAF is designed to assess the security of that information, identify risks to the confidentiality, integrity and availability of that information, and provide recommendations to mitigate them.

Completing a PSAF security assessment ensures:

- **access to security advice throughout the duration of your project:** early engagement will ensure that risks can be identified, managed and mitigated throughout the project's design, development and deployment phases and prevent them from becoming more costly issues later in the project.
- **security controls are built into your project:** receive recommendations to enable the right controls to be embedded into the solution to make it easier to manage and operate once implemented.
- **compliance with relevant frameworks:** maintain compliance with eHealth NSW, NSW Health and NSW Government cyber security policies and other NSW and federal legal and regulatory frameworks.

1.3 When is PSAF needed?

Some common scenarios where a PSAF security assessment should be completed include:

- When a new solution, service or application is developed or implemented. This includes those developed by NSW Health as well as those provided by an external vendor.
- When changes or upgrades are implemented for existing software or applications. This could include new functionality, features or modules, or when there is a change to the application architecture, design or network configuration.
- When an information asset that is managed by a health organization is transitioned to eHealth NSW to manage.
- When an information asset is migrated to or created in the eHealth NSW Self-Managed Cloud.

We strongly encourage you to engage with the Cyber Security Advisory team on PSAF as early as possible to ensure risks are identified early in the project.

1.4 What is the cost of completing PSAF?

The cost depends on the size of the project, the associated risks, and the size of the effort to complete the assessment. You can use the Security Assessment Cost Calculator form in SARA to get an estimated cost for your project.

You can also refer to the sizing table below for an indication of costs. Please contact the Cyber Security Advisory team for costings if your project follows the Agile approach or if it is XX-Large.

PSAF type	PSAF project size	Cost range ($)
Standard	Small	4,900 – 7,700
	Medium	8,400 – 13,300
	Large	14,000 – 22,400
	X-Large	18,900 – 32,200
Bespoke	XX-Large / Agile	To be advised by the Cyber Security Advisory team

2. How does the PSAF process work?

The PSAF process is aligned with the project's design, development and deployment phases. It uses questionnaires which are sent as surveys in SARA to identify risks during each phase and to provide recommendations on how to mitigate the risks.

Here is what to expect during each phase. You can also contact your security consultant at any stage if you need additional advice or are unsure of the process.

Initiating a PSAF security assessment

Step 1

- Check if a PSAF security assessment is required for your solution by completing the Request Security Assessment form in SARA. Further information on how to complete this form is available in the SARA article How do I request a PSAF Security Assessment?
- If it's not required, you can either close the form or submit the form to save a record to your SARA My Items.

Step 2

- If a security assessment is required, complete the Security Assessment Cost Calculator form in SARA. Make sure you request a 'Final' cost, not an estimate*. Further information on how to complete this form is available in the SARA article How do I find out the cost of a PSAF Security Assessment using the Cost Calculator? **Please note, it is **not** possible to change an 'Estimated' cost calculator record into a 'Final' cost. If you have completed a request for an 'Estimated' cost, you will need to submit a new request for a 'Final' cost and re-enter the details.*

- Note down the cost calculator number that is generated (format will be ENG1234567).
- Get this cost approved (an approval request will be sent to the business owner when the cost calculator form is submitted).

Step 3

- If you don't already have a Demand, please contact your Customer Account Manager (if you are external to eHealth NSW) to have one created (a Demand is a request for new products, services or enhancements). eHealth NSW customers should obtain a Demand through their usual process, for example, through the Create Demand form in SARA if available for your application, or through an Engagement Manager.

Step 4

- Complete the Request Security Assessment form in SARA and this time enter your approved cost calculator number (that you noted down in Step 2) to submit the request.
- The Cyber Security Advisory team will receive your request and get back to you.

Plan and Gather requirements phase

During this phase, your PSAF security consultant will gather information about your project to understand what specific tasks will need to be completed as part of your assessment.

Step 1:

Your security consultant will send you a survey (Plan and Gather Requirements Survey) to complete in SARA to gather additional information about your project. You will receive an email notification about the survey. You can also access surveys that have been assigned to you by going to the *My Items* tab in SARA. Further information on how to complete the survey is available in the SARA article How do I complete PSAF Security Assessment related surveys in SARA?

Your security consultant will receive a notification when you have completed the survey.

You may need to complete additional surveys if further information is needed.

The information you will be asked to provide during this stage will depend on your project, but may include details such as:

- Who will be using the solution?
- Where it will be hosted?
- What kind of data it will deal with, for example, is it personal and/or sensitive?
- What vendors will be involved?
- What would be the impact if the data was breached, modified or unavailable?

Step 2:

As your security consultant reviews this information and determines the scope of the assessment, these additional components may also be initiated if required:

- Disaster Recovery and Technical Privacy Risk Assessment. (These are sub-processes of the PSAF process and the Disaster Recovery assessment is managed by the eHealth NSW Business

Resilience Team). These assessments will need to be completed before the PSAF is completed or a risk will be raised with an expectation to complete these requirements retrospectively.
- Vendor Security Risk Assessment (using the NSW Government's Vendor Risk Assessment tool UpGuard).

Once all the information for this phase has been gathered and reviewed, your security consultant will decide what design or build tasks need to be completed as part of your assessment.

Design phase

The Security Design document will be completed during this phase. This details what security controls will need to be built into your solution. Vendor Security Risk Assessments and Security Control surveys will also need to be completed during this phase.

Step 1:

Your security consultant will send you a survey to complete in SARA to provide information on the design of your solution. This will involve uploading the security design document for your solution. If required, you can request a Security Design Reference Guideline template from your security consultant.

You will also be required to complete Security Control surveys and Vendor Security Risk Assessments should they be required.

You may need to provide additional information if required to complete the design assessment.

Further information on how to view updates about your assessment is available in the SARA article How do I see updates about my PSAF Security Assessment request?

Step 2:

During this phase, an assigned security consultant will complete some of the following activities:

- Provide information on how the solution should be designed based on secure design principles.
- Review the Security Control assessment responses and design documents.
- Analyse:
  - the technologies and environment being used
  - the logical components the system will be constructed from
  - the interconnectivity between the various components
  - the integration with other systems
  - the various security domains the data will transit through and rest in
  - the user access roles deployed in the solution
  - the data flow
  - firewall rules.
- Conduct a Technical Privacy Risk Assessment if required (see here for further details).
- Provide advice to ensure that the security design addresses the required security and privacy controls.
- Scope the requirements for the Technical Security Assessment (also known as the 'As built' security review). This is completed by an external third-party vendor and may include activities such as penetration testing, configuration reviews, vulnerability scans etc.

- Engage the eHealth NSW Procurement team to appoint the third-party vendor to conduct the Technical Security Assessment.

Once this has been completed, your Cyber Security Consultant will document any risks identified.

Build, test and manage phase

During this phase, tasks related to the build, test and management of your solution will be completed.

Note: Design and build tasks could be initiated concurrently and risks can be identified at any stage during these phases. The steps below can also occur in parallel with one another.

Step 1:

You will complete surveys in SARA to provide information on the build, test and management of your solution.

Step 2:

You will need to complete Operational Security Procedures (SOPs). This details how the solution will be managed once it's live and how the security posture will be maintained throughout the solution's lifecycle. For example, this could cover how users will be granted access to the solution, how vulnerabilities will be managed, and disaster recovery plans etc.

Step 3:

A Technical Security Assessment (or 'As built' security review) will be completed. This is completed by an external third-party vendor who will examine the solution and look for any potential issues. For example, they may conduct a penetration test which looks for ways the solution may be compromised. Your security consultant will liaise with you to provision access for the vendor.

Step 4:

Your security consultant reviews all the information from the surveys, SOPs and Technical Security Assessment review and adds any risks that have been identified to the Security Risk Management Plan (SRMP) spreadsheet. This includes a summary and rating for each identified risk and recommendations on how to manage them.

The SRMP can be started at any stage of the assessment and risks can be added to it at any time.

Step 5:

You will be asked to complete certain sections of the SRMP in consultation with the risk owner. This will be emailed to you by your consultant.

Your security consultant will review your responses and recalculate the risk to arrive at a 'residual risk rating' which is the final risk rating.

Step 6:

The final SRMP is sent to the risk owners for their review and approval. The final SRMP spreadsheet will be attached to your security assessment's Engagement record in ServiceNow.
Step 7: The security assessment is submitted for approval by the risk owner. If the risks identified are high or extreme, this could also include approvals by stakeholders such as executive management or the CIO.
Step 8: Once approved by the risk owner plus any additional stakeholders if required, you will be notified of the outcome and the security assessment will be marked as complete.

3. How do I request a PSAF security assessment?

All relevant forms are now available in SARA. These replace the PSAF SharePoint portal and include:

- Request Security Assessment form
- Security Assessment Cost Calculator form
- Information Security Exemption form.

Please note: Any PSAF assessments created before 5 December 2022 will continue to be managed through the PSAF SharePoint portal and will not be migrated to SARA/ServiceNow.

You can also contact the Cyber Security Advisory team directly if you would like to meet and discuss your project's requirements before you submit a request.

4. Frequently asked questions (FAQs)

Q. How long does a PSAF take?

This is dependent on several factors such as:

- the size of the project
- the complexity and sensitivity of data
- the number of components that need to be included in the assessment
- the number of vendors involved
- high/low availability
- its interface with other systems
- hosting platforms
- what stage the project is in
- how long it takes to receive the information and details required
- the accuracy of the information in the documentation and artifacts

Q. Do I need a Customer Account Manager (CAM) to request a PSAF?

Yes, if you are a customer from outside of eHealth NSW you will need to work with your CAM to create a Demand. If you are an internal customer from within eHealth NSW, you will need to create a Demand through your usual process, for example, through the Create Demand form in SARA if available for your application, or through an Engagement Manager

Q. Do I need a Demand to request a PSAF?

You can request a PSAF cost for funding purposes without a Demand, however a Demand will be required before a PSAF security assessment can be requested. The cost must be approved and a cost centre supplied to your Customer Account Manager so they can raise a Demand. (For internal eHealth customers, your Demand must include an OTL code for charge back).

Q. Can my project go live without a PSAF?

An exemption may be granted in exceptional circumstances. This is contingent on the business authority or risk owner accepting the risk and is only granted for a maximum of 12 months. A PSAF will still be required retrospectively once the exemption has lapsed.

Please refer to the Information Security Exemption Management Procedure and complete the Information Security Exemption form.

Q. How will I know what phase my assessment is up to and what I need to do next?

You will be required to fill out several surveys during the completion of your PSAF. The main surveys are 'Plan and Gather Requirements', 'Design' and 'Build, Test and Manage.' You will be notified if other surveys are required. To view updates or to see the current state of your assessment in *My Items*, refer to this SARA article How do I see updates about my PSAF Security Assessment request? You will also be assigned a security consultant who will advise you throughout your assessment. If you are not sure at any stage or require further information, please contact your security consultant.

Q. I am not building a solution, I just want to use a new tool or application from a vendor. Why do I need to use a PSAF?

PSAFs are not just for NSW Health developed IT solutions, they are also used to assess risks that we may be exposed to by using IT solutions that are provided by external vendors. It is therefore important that a security assessment is also completed whenever a new solution is implemented. A security consultant will evaluate the vendor's security posture to ensure NSW Health data is protected.

Q. Is there a list of vendors that have been though PSAF that we can choose from to avoid going through PSAF?

Completed PSAF assessments can be viewed here. Although PSAF may have been completed for a vendor, a new PSAF may still be required as we are evaluating more than just the vendor.

Q. What happens to assessments that have commenced through the PSAF SharePoint portal now that it has been replaced by SARA?

Any PSAF assessments created before 5 December 2022 will continue to be managed through the PSAF SharePoint portal and will not be migrated to SARA/ServiceNow.

Q. Can my vendor fill in the SARA survey for me?

Only people with a StaffLink ID can access SARA to respond to surveys.

Q. I'm not a technical person. Can I delegate the survey to someone else in my team to complete?

Yes. Please ask your security consultant to reassign the survey to the appropriate person.

Q. What are the policies, standards and frameworks that the PSAF framework is aligned with?

The PSAF framework is aligned with the NSW Cyber Security Policy, which includes Essential 8 and eHealth Information Security Management Standard (ISMS ISO27001). It also considers the legal and regulatory frameworks under which eHealth NSW operates, this includes but is not limited to, the *Privacy and Personal Information Protection Act 1998* (NSW), *Privacy and Personal Information Protection Regulation 2019* (NSW), *Health Records and Information Protection Act 2002* (NSW), and *Health Records and Information Privacy Regulation 2022* (NSW).

Q. What happens after a PSAF is completed?

The output of a PSAF is an SRMP (Security Risk Management Plan) which contains a list of risks that need to be accepted or remediated by the risk owners. If they require remediation, one or more risk treatment owners will need to be allocated. Once the SRMP has been signed off by the risk owners, it is transferred to the ISS Governance team, who will ensure that risk treatments are completed.

5. More information

- Related forms:
  - Request Security Assessment form
  - Security Assessment Cost Calculator form
  - Information Security Exemption form.
- SARA articles:
  - How do I find out the cost of a PSAF Security Assessment using the Cost Calculator?
  - How do I request a PSAF Security Assessment?
  - How do I see updates about my PSAF Security Assessment request?
  - How do I complete PSAF Security Assessment related surveys in SARA?
- PSAF intranet page
- Submit an enquiry in SARA (select Privacy and Security Assessment Framework under Business Service)
- Email EHNSW-CybersecurityAdvisory@health.nsw.gov.au