

Victorian Electronic Patient Health Information Sharing System Privacy Management Framework

Department of Health

OFFICIAL



Department
of Health

OFFICIAL

Acknowledgement of Aboriginal people living in Victoria

The Victorian Department of Health acknowledges the strength of Aboriginal people across Country and the power and resilience they share as members of the world's oldest living culture. We acknowledge Aboriginal people as Australia's First People and recognise the richness and diversity of all Traditional Owners across Victoria.

We recognise that Aboriginal people in Victoria practice their lore, customs and languages, and nurture Country through their deep spiritual and cultural connections and practices to land and water.

We are committed to a future based on equality, truth and justice. We acknowledge that the entrenched systemic injustices experienced by Aboriginal people endure, and that Victoria's ongoing treaty and truth-telling processes provide an opportunity to right these wrongs and ensure Aboriginal people have the freedom and power to make the decisions that affect their communities.

We pay our deepest respect and gratitude to ancestors, Elders and leaders past and present. They have paved the way, with strength and fortitude, for our future generations.

To receive this document in another format, [email the Health Information Exchange program team](mailto:HIEprogram@health.vic.gov.au) <HIEprogram@health.vic.gov.au>.

Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.

© State of Victoria, Australia, Department of Health, May 2024.

Except where otherwise indicated, the images in this document show models and illustrative settings only, and do not necessarily depict actual services, facilities or recipients of services.

In this document, 'Aboriginal' refers to both Aboriginal and Torres Strait Islander people. 'Indigenous' or 'Koori/Koorie' is retained when part of the title of a report, program or quotation.

ISBN/ISSN 978-1-76131-575-6 (online/PDF/Word) or (print)

Available at [Health Information Sharing Legislative Reform](https://www.health.vic.gov.au/quality-safety-service/health-information-sharing-legislation-reform) <https://www.health.vic.gov.au/quality-safety-service/health-information-sharing-legislation-reform>

Navigating this document

This document is the Privacy Management Framework (PMF) for the Victorian Electronic Patient Health Information Sharing System (CareSync Exchange). It is designed to enable a shared understanding across diverse experiences and interactions with the Victorian public health system. It has been prepared for three groups of readers, as shown below.

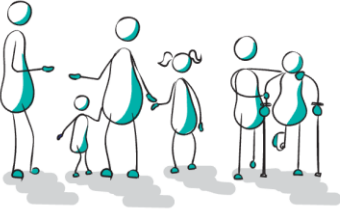


| | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <p>The public</p> | <p>Clinicians and other users</p> | <p>Managers and executives</p> |
| <p>For members of the public, the message from the Minister, commitment from the steward, Introduction, and Chapter 1 are most relevant. Chapters 2 and 3 may also be useful.</p> | <p>Clinicians and other users must read the document up to and including Chapter 4.</p> | <p>Health service and Department of Health executives and managers must read and understand the document in its entirety.</p> |
|  |  |  |

Table of contents

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <p>Message from the Minister</p> | <p>pg 6</p> |
| <p>The message from the Minister introduces readers to the PMF for CareSync Exchange.</p> | |
| <p>Commitment from the steward</p> | <p>pg 7</p> |
| <p>The commitment from the steward, the Secretary of the Department of Health, presents the department’s commitment to implementing the PMF.</p> | |
| <p>Introduction</p> | <p>pg 8</p> |
| <p>The Introduction helps readers understand how Victorian public health services exchange patient information, why CareSync Exchange has been established, its function, and the purpose of this PMF.</p> | |
| <p>The rest of the document sets out the elements of the PMF and how they will be maintained.</p> | |
| <p>Chapter 1: Health consumer rights</p> | <p>pg 15</p> |
| <p>The rights of health consumers to know what is in their own records and who, where and why their records are accessed is at the core of the PMF. Chapter 1 sets out health services’ accountabilities to protect these rights and outlines escalation and complaint mechanisms for health consumers.</p> | |

Chapter 2: Access and use

pg 19

Access and use of CareSync Exchange is strictly controlled. Chapter 2 describes which health services and departmental staff can use CareSync Exchange and under what circumstances.

Chapter 3: Permitted information and controls

pg 23

CareSync Exchange does not collect all health information. Chapter 3 explains what information is collected and how CareSync Exchange handles specific health information.

Chapter 4: Training

pg 28

Chapter 4 describes the obligations on health services to ensure clinicians and other users complete appropriate training on the use of CareSync Exchange.

Chapter 5: Security

pg 33

Chapter 5 sets out the responsibilities of the department and health services to maintain security controls for CareSync Exchange, including security policies, standards and governance.

Chapter 6: Monitoring, reporting and auditing

pg 35

To ensure trust in CareSync Exchange and the controls outlined in this PMF, it is crucial to have strong monitoring, reporting and auditing mechanisms in place. These responsibilities are held by health services and the department and are described in Chapter 6.

Chapter 7: Data breach and incident management

pg 39

Regulated standard controls and recommended mitigations are in place to protect health information. However, in our digitally connected world, there is a risk of data breach. Health services and the department are responsible for managing data incidents as described in Chapter 7.

Chapter 8: Operational governance

pg 41

Chapter 8 describes the operational governance of the PMF and sets out which leaders across the department and health services are responsible and accountable for ensuring each obligation in this PMF is fulfilled.

Chapter 9: Ongoing improvement and review

pg 43

Chapter 9 describes how the Minister and Secretary of the department will facilitate reviews and ongoing improvement of this PMF to ensure it remains fit for purpose.

Glossary

pg 45

All technical terms and relevant legislation have been defined throughout this document in **pink** and in the Glossary.

As you read this document, there are three technical terms to remember:

- **EMR** refers to electronic medical record, which is a digital version of a patient's medical history collected by a health service when the patient receives medical care or treatment. It contains data such as diagnoses, medications and test results.
- **PMF** refers to the Privacy Management Framework, which is this document. The PMF sets out the rights, obligations and governance related to privacy management to protect health information in CareSync Exchange.
- **CareSync Exchange** refers to the Victorian Electronic Patient Health Information Sharing System. It is established by the *Health Legislation Amendment (Information Sharing) Act 2023 (Vic)*, which amends the *Health Services Act 1988 (Vic)*. CareSync Exchange is one component of a broader health information sharing system and only contains general health records. This document is the PMF for CareSync Exchange.

Appendix A: List of public health services with access to CareSync Exchange

pg 51

Appendix A lists the public health services that have or will have access to CareSync Exchange.

Appendix B: Information collected by CareSync Exchange

pg 52

Appendix B lists the types of information that are collected by CareSync Exchange from systems used by health services such as EMRs.

Appendix C: Consultation process to inform the Privacy Management Framework

pg 58

Appendix C presents the PMF consultation process including stakeholders involved in the development of the PMF.

Index

pg 59

The Index lists the main topics, people and organisations discussed in the PMF along with their corresponding page numbers.

Legislative basis for CareSync Exchange and the PMF

The development of CareSync Exchange and this PMF is required under the *Health Legislation Amendment (Information Sharing) Act 2023 (Vic)*, which adds Part 6C to the *Health Services Act 1988 (Vic)*. These changes complement and strengthen the privacy protections already established by the *Health Services Act 1988 (Vic)* and the *Health Records Act 2001 (Vic)*. Further details on relevant legislation are provided in the **Glossary**.



Message from the Minister

Every day thousands of Victorians visit public health services across the state.

Ensuring a carefully coordinated approach with the appropriate safeguards in place to protect people's privacy is essential when building trust with a patient while discussing the next steps in their care.

Making timely and effective decisions about a patient's care choices would undeniably be enhanced by a shared system of health information between public health services.

With this in mind, I am pleased to share with you the newly developed Privacy Management Framework (PMF) for the Victorian Electronic Patient Health Information Sharing System (CareSync Exchange).

The PMF has been shaped by the extensive expertise and experiences of Victorian consumers, as well as our committed healthcare workforce, to provide solutions for patient privacy concerns.

It will ensure the Department of Health and our public health services provide the best patient experience possible by handling private and sensitive information carefully and safely between services.

The PMF provides clear and useful directions, guidelines and responsibilities for dealing with health information. Patients, carers, family members and support people will benefit from the secure handling of CareSync Exchange by providing more information at the time of care.

At the heart of patient-centred care, CareSync Exchange will allow easier and more timely diagnosis, preventing delays in treatment by providing access to comprehensive information about a patient's medical history.

We have a strong commitment to protecting consumers' privacy. The PMF will work to alleviate concerns about appropriate access and use of private patient information across the public health system. Regulatory measures, audits, monitoring and strict security, backed by stringent penalties for misuse, will ensure adherence to the Victorian Government's data requirements and standards.

Each year, in our CareSync Exchange annual report we will publish a summary of user interactions and the types of data accessed through CareSync Exchange. A summary of feedback received, along with actions taken to address concerns, will also be reported.

I have confidence in the diverse panel of experts appointed to the Health Information Sharing Management Committee to provide advice to the Secretary of the department on the operation of CareSync Exchange and the PMF.

I look forward to working in collaboration with the department to continue safeguarding the health data privacy of all Victorians.

The Hon. Mary-Anne Thomas MP

Minister for Health

Minister for Health Infrastructure

Minister for Ambulance Services



Commitment from the steward

Victorians expect our health system to deliver high standards of healthcare delivery when presenting as patients to our health services. This includes how their health information is safeguarded.

The Privacy Management Framework (PMF) for the Victorian Electronic Patient Health Information Sharing System (CareSync Exchange) is a clear guide on how we will continue to protect Victorian health consumers' information while securing trust in clinicians at the point of care.

Health information privacy is important to everyone. It underpins all practices and policies in the health sector. This framework outlines clear guidance to continue our commitment to delivery of person-centred health care to all Victorians.

We ensure the confidentiality and security of information by following the Health Privacy Principles of the *Health Records Act 2001* (Vic). This Act was amended by the *Health Legislation Amendment (Information Sharing) Act 2023* (Vic) to allow for the establishment of CareSync Exchange.

Improvements in digital health technology help us to improve patient safety and efficiency in information collection. A lot of privacy management sits within careful management of modern technology systems, through training, access, controls and governance.

Both on the international stage and locally in other Australian states and territories, public health sharing information systems are providing a great record of success in treating hospital patients.

One of the key measures of success in health information sharing is how the privacy of shared data is managed to provide efficient care.

There are many benefits of statewide health information sharing. Joining up information that is held across the state will:

- save lives and reduce avoidable harm
- enable clinicians to make more timely and informed decisions
- reduce the burden on patients to recall past treatment or relive experiences
- standardise health information sharing practices across Victorian health services and make them transparent.

This PMF sets out the processes and responsibilities we expect from clinicians, health services and Department of Health staff. Privacy and security of patient data is a core accountability in the duty of care for every person who accesses CareSync Exchange.

As the steward of CareSync Exchange, I am confident that the PMF will deliver on the evolving needs and expectations of Victorian health consumers.

The Victorian Government is committed to the rollout of the PMF. I look forward to working on the initiatives outlined in this report to secure the privacy of every Victorian health consumer.

Professor Euan M Wallace AM

Secretary

Department of Health

Introduction



This document is the Privacy Management Framework (PMF) for the Victorian Electronic Patient Health Information Sharing System (CareSync Exchange). It outlines the roles, obligations and governance involved in protecting Victorian health consumers' information privacy in CareSync Exchange.

Background and context

The privacy of Victorians' health information is protected by law. All Victorian public health services (referred to as 'health services' throughout this document) must collect, use, disclose and protect health information in accordance with the *Health Services Act 1988 (Vic)* and the [Health Privacy Principles](#) <<https://go.vic.gov.au/4bLyWNt>> set out in the *Health Records Act 2001 (Vic)*. These principles are embedded into everyday practices and policies throughout the health sector to ensure that health services and staff manage their patients' health information appropriately.

Health services hold information about each patient's care and treatment, tests and diagnoses in an electronic medical record (EMR), other digital health information systems, or in paper-based records. Since the early 2000s, Victorian health services have been increasingly using EMRs.

Electronic records make it easier for clinicians to provide a patient with prompt care and can inform subsequent care for that patient, whether it is a month, year or decade later. However, these benefits are often limited to a particular health service and not readily accessible by other health services across Victoria.

In 2016 the [Targeting Zero](#) review recommended that health information flow should be improved to strengthen the quality and safety of care provided across the Victorian hospital system.¹

To fulfil these recommendations, the Victorian Electronic Patient Health Information Sharing System (referred to as the CareSync Exchange) has been developed to collect and share health information at the point of care across all Victorian public health services.

This PMF has been created to ensure that Victorian health consumers' privacy within CareSync Exchange is protected.

Health information sharing in Victorian health services

There are 78 public health services across Victoria, each with an independent board appointed by the Minister for Health. Each health service has independent management that reports to those boards. The health services operate a wide range of facilities, with some managing a single, multipurpose clinic while others manage several large hospitals. Over time, these services have established different digital health information systems to hold patients' health information.

In most cases, a patient's health information in these systems is restricted to that health service and cannot easily be shared with other health services. Without CareSync Exchange, health information sharing across health services would occur through slower and more time-consuming means like phone or fax. This can lead to delays in treatment. Often these methods leave no paper trail, making it hard to audit and be sure who has seen what information.

¹ Recommendation 4 of *Targeting zero: supporting the Victorian hospital system to eliminate avoidable harm and strengthen quality of care* available at [Targeting Zero](#) on the department's website <<https://go.vic.gov.au/3UzX0vG>>

What is CareSync Exchange?

CareSync Exchange is a secure digital platform that presents important patient health information to clinicians at the point of care across the Victorian public health sector. Health information on CareSync Exchange is collected from separate health record systems – for example, EMR – used at each public health service.

CareSync Exchange has been established by the Victorian Government Department of Health to support an efficient exchange of health information between **health services**. CareSync Exchange works alongside (and does not replace) existing health service systems and the national My Health Record to improve access to comprehensive, timely and accurate health information by **clinicians** when they deliver care. Similar health information sharing systems have already been implemented in other Australian states.

CareSync Exchange will be one source of information for clinicians when **patients** present at a health service. The patient's own description and presenting symptoms will remain the primary source of information for clinicians.

Information on CareSync Exchange has been collected from the health record system at each participating health service and can only be viewed by authorised users for authorised purposes. This is shown in **Figure 1**.

The legislation that established CareSync Exchange permits health services to collect, use or disclose a patient's health information without requiring their consent. This provision aligns with existing laws that allow health services to share health information for patient treatment without requiring patient consent to ensure ongoing care and treatment.

Since CareSync Exchange simply presents collected information, clinicians will continue to document the care they provide patients in the health record system (such as an EMR) at the health service where the clinician is providing care. Other forms of health information sharing as part of transfer or continuity of care will continue to be used by clinicians. This includes referral letters and transfer documentation when a patient is moved between hospitals.

A sample patient journey and case studies are presented in **Figure 2** and **Figure 3** to illustrate how CareSync Exchange is used when patients visit public health services.

In this document, **health services** are organisations that provide health care or medical services funded by the Victorian Government. They include public hospitals and ambulance services, but not private hospitals and general practitioners.

CareSync Exchange will be progressively rolled out to Victorian public health services over several years, beginning with nine metropolitan hospitals (see **Appendix A**: List of public health services with access to CareSync Exchange).

The department will work with each health service to ensure that systems are ready and project governance is in place to support implementation.

Clinicians are healthcare professionals who are trained and qualified to provide clinical services and associated support to patients. Clinical services include diagnosis and treatment of patients, which includes recommending preventive action.

In this document 'clinicians' are healthcare professionals working at Victorian public health services. They include doctors, nurses, paramedics and allied health professionals like physiotherapists and social workers.

Patients are health consumers who are receiving medical help or treatment at a Victorian public health service.

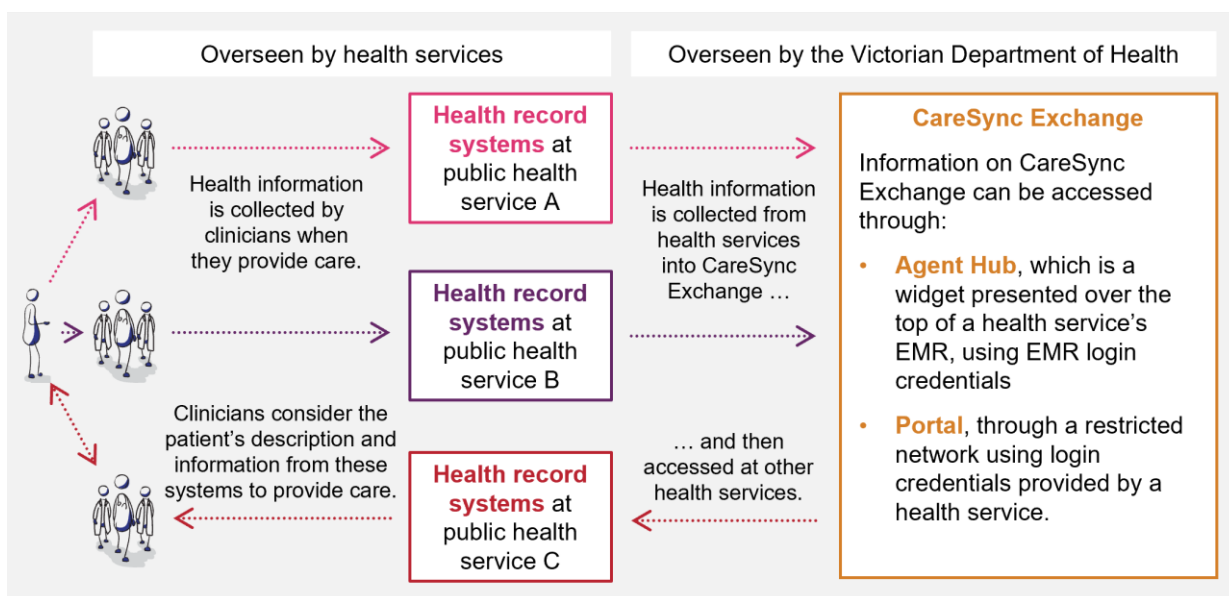
Health consumers is a broader term. It includes individuals who use (or may use) a Victorian public health service. Consumers can be patients and their carers, family members and other support people.

How is CareSync Exchange different to My Health Record?

CareSync Exchange complements and does not replace My Health Record.

- **CareSync Exchange is optimised for clinicians in Victorian public health services.** It will be used when patients visit public health services in Victoria and when they are transferred across Victorian public health services. It is operated by the department.
- **My Health Record is a national system that offers a view of patient health information across primary care (general practice), private and public health services.** My Health Record is used when patients have received health care in primary or aged care settings before their visit to a health service. Patients can opt out of My Health Record. It is operated by the Australian Digital Health Agency.

Figure 1 | CareSync Exchange collects information from health record systems



How are records matched?

Victorian public health services use a matching algorithm to join patient records. This approach eliminates the need for a statewide identifier. Each record from a health service is checked for details like name, date of birth, address and other identifying information. If enough details are identical, the records are joined to make a patient record in CareSync Exchange.

Indigenous Data Sovereignty relating to CareSync Exchange

The department recognises the importance of Indigenous Data Sovereignty and acknowledges the marginalisation of Aboriginal peoples, which has been perpetuated through exclusion of control over their data. [Indigenous Data Sovereignty](http://vaccho.org.au/policy-and-advocacy/systems-and-systemic-reform) <vaccho.org.au/policy-and-advocacy/systems-and-systemic-reform> refers to the right of Indigenous people to exercise ownership over Indigenous Data. It enables Aboriginal communities to realise and benefit from the vast cultural, strategic and economic value that data holds for Aboriginal peoples.

The Victorian Government is dedicated to collaborating with Aboriginal communities and organisations to develop appropriate policies and frameworks in line with its commitment under the [Victorian Aboriginal affairs framework 2018–2023](https://go.vic.gov.au/3yaGF94) <https://go.vic.gov.au/3yaGF94> and the *National agreement on closing the gap*. This commitment extends to future initiatives concerning Indigenous Data Sovereignty and Indigenous Data Governance, which will be reflected in future governance of CareSync Exchange.

Figure 2 | Sample patient journey with CareSync Exchange

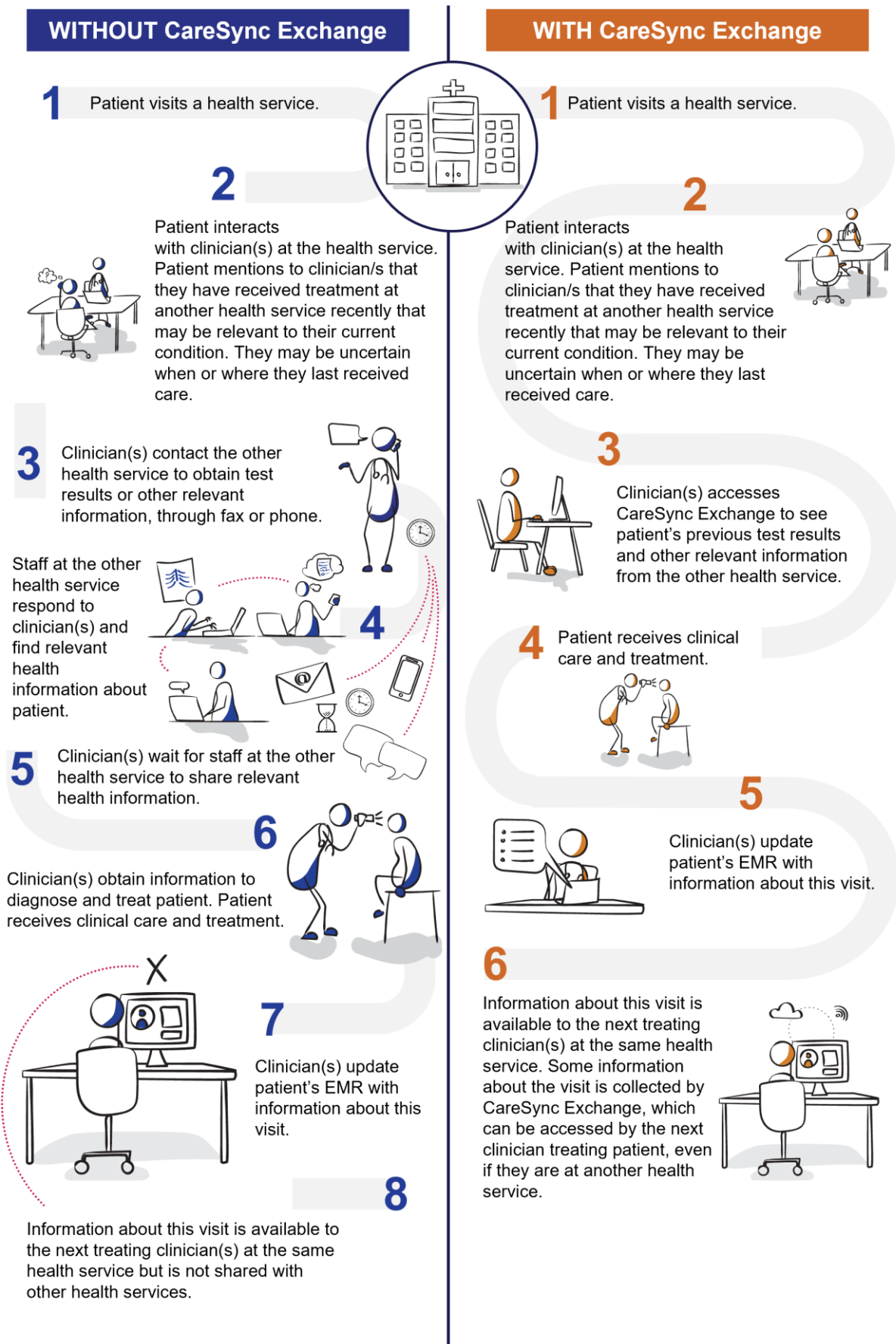


Figure 3 | How will CareSync Exchange benefit health consumers?

What does this mean for health consumers?

The following scenarios explore how clinicians may use CareSync Exchange.



Omar is a university student visiting his hometown in rural Victoria when he experiences severe abdominal pain and vomiting. He is taken to the local hospital by his cousin.

At the hospital, Omar’s cousin tells the clinicians that Omar had recently been to a hospital in Melbourne, but he isn’t sure which one or what for. Omar is distressed with his pain and is unable to communicate about his treatment in Melbourne.

The clinicians access Omar’s most up-to-date record on CareSync Exchange through their local EMR. They find recent test results at a hospital in Melbourne from a month ago. This information is used to help inform Omar’s diagnosis and treatment.

- ✓ Clinicians can make **timely and informed decisions** to support Omar’s care and treatment, without needing to wait for information held at other health services.
- ✓ Access to the test results at the other hospital **assists Omar to recall past treatment**.
- ✓ The clinicians **do not need to duplicate tests** already done at the hospital in Melbourne.

Jane is undergoing chemotherapy to treat her cancer. To have the family support she needs, Jane moves back to Melbourne to stay with her parents.



To continue her treatment, Jane consults with a new oncologist at the metropolitan hospital. As the oncologist is reviewing Jane’s history with her on the local EMR, Jane advises that she had some tumour marker tests done at another hospital before she moved. The oncologist accesses pathology reports from the other hospital on CareSync Exchange. The test results in these reports are used to determine the effectiveness of the chemotherapy dosage and other treatments.

- ✓ The oncologist can **make timely and informed decisions** to support Jane’s care, without needing to follow up and wait for information held at the other hospital. This **supports the handover and continuity of care for Jane**.
- ✓ The oncologist **does not need to duplicate tests** already done at the other hospital.

What are some instances where CareSync Exchange is not used?

- Clinicians will continue to speak to patients and use the local EMR as part of their regular clinical practice. They may not require CareSync Exchange to inform a patient’s care, particularly if a patient regularly visits one health service to receive care.
- General practitioners and other clinicians working in private health services will not be able to access CareSync Exchange.

What is the Privacy Management Framework?

The PMF describes the rights, obligations and governance to protect health information within CareSync Exchange.

The quality and speed of patient care depends on the information available to clinicians. The more information a clinician has, the more easily they can make diagnosis and provide treatments tailored to the needs of each patient.

However, health information is sensitive. It needs to be used with care and protected. Its sensitivity may be heightened for some consumers due to concerns about stigma, theft, misuse or accidental disclosure. These concerns may be based on past experience, stories of incidents, or other life experiences outside the health sector. Given these concerns, consumers need to know that their health information will be handled carefully by all who may access the information.

It is important to strike a balance between improved health outcomes through information sharing and safeguards to protect Victorian health consumers' privacy. These safeguards must ensure that consumers' personal information is handled in accordance with privacy standards and legal requirements.

To find this balance and address privacy concerns, the PMF establishes a set of actions, guidelines and responsibilities that govern the use of health information within CareSync Exchange. All users who are granted access to CareSync Exchange and those involved in the management and oversight of CareSync Exchange must follow this PMF. The PMF and operation of CareSync Exchange is the responsibility of the Secretary of the department, who will receive advice from an independent Health Information Sharing Management Committee.

While the PMF specifies privacy safeguards to protect health information on CareSync Exchange, it does not apply to local health information systems like EMRs, which already have privacy protections in place. The PMF may provide reference to, but not detail, other privacy management measures and clinical practice guidelines that apply to the existing health information systems used by health services

The PMF does not apply to privacy concerns related to clinical practice. It reinforces the importance of clinical practice when using the health information. It also sets out mandatory training on privacy in CareSync Exchange and describes what consumers can do if they have a concern or complaint regarding how their health information was used. However, the scope of the PMF does not extend to governing clinical practice across the Victorian health system.

To align with the requirements of the *Health Legislation Amendment (Information Sharing) Act 2023* (Vic), the PMF has been co-designed with Victorian health consumers, clinicians, clinical and service managers and executives in the health sector, and other interested parties to ensure the PMF can be implemented (refer to **Appendix C**: The consultation process to inform the Privacy Management Framework). A summary of consumer rights for CareSync Exchange is shown in **Figure 4**.

Alongside the PMF, there will be a suite of supporting materials, including:

- communication resources for consumers
- detailed policies, procedural guidelines and breach management materials for clinicians, health services and the department.

Figure 4 | Summary of consumer rights for CareSync Exchange

My rights as a consumer



“ I have the right to know what information is collected about me on CareSync Exchange, and how it is used and shared (Chapter 1). ”

“ I have the right to seek access to my medical record in an EMR or other health service system but not CareSync Exchange (Chapter 1). ”





“ I have the right to request information about who has accessed my record on CareSync Exchange (Chapter 1). ”

“ I can expect that health services may use a pseudonym (different name) to protect my identity when they provide care (Chapter 1). ”






“ If I think my health records have inaccuracies, I can discuss this with clinicians or health information management staff at health services (Chapter 1). ”

“ I can discuss privacy concerns with clinicians or health information management staff at health services. I have ways to lodge a complaint or escalate if needed (Chapter 1). ”





“ I can expect that access to my information on CareSync Exchange is restricted to only authorised users who need to know it (Chapter 2). ”

“ I can expect that only relevant information to inform my care will be collected (Chapter 3). ”





“ I have the right for my information on CareSync Exchange to be handled carefully, especially for particularly sensitive information (Chapters 3 and 4). ”

“ I have the right for my information on CareSync Exchange to be protected from cyber threats and unauthorised access (Chapters 5, 6 and 7). ”



Chapter 1: Health consumer rights



The department and health services must be transparent to health consumers about how their information is handled on CareSync Exchange and provide a mechanism for resolution of complaints.

Whenever consumers visit health services, they can expect that their care will be shaped by ongoing discussion with clinicians. Clinicians will first explore a patient's immediate needs and concerns. They will discuss any earlier care a patient has received and, if required, access other sources of information such as CareSync Exchange.

How consumers' health information is handled

Health consumers have the right to know what type of health information is collected on CareSync Exchange, the purposes for which it is used, and how it is shared.

Transparency about the access and use of health information on CareSync Exchange is essential for establishing consumer confidence that information is used and managed appropriately. It is also required by the Health Records Act and the Health Services Act.

The PMF and information about CareSync Exchange is available in [Health Information Sharing Legislation Reform](https://go.vic.gov.au/483vAUA) on the department's website <<https://go.vic.gov.au/483vAUA>>. It includes information about privacy notices that specify the types of health information collected and shared, and updates on the rollout of CareSync Exchange.

Consumers can seek access to their health information from health services and also information about who has accessed it on CareSync Exchange.

Consumers may seek further information about their health records. There are different steps to achieve this, depending on what information is needed. **Figure 5** presents these steps.

Consumers can lodge a request for health information on a health service system (such as an EMR). However, they are unable to lodge a request for health information on CareSync Exchange.

While consumers cannot directly request health information on CareSync Exchange, they can request information about who accessed their record on CareSync Exchange, when it was accessed and how it was accessed.

Figure 5 | Process to access your information

| Type of information request | Where to submit request | Where to go for further queries |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Medical record Health information in an EMR or other health service system (note that this is not CareSync Exchange)</p> | <ol style="list-style-type: none"> 1. Speak to a clinician or health information officer at a health service where you have previously received care. 2. If you require your medical record, you may need to lodge a freedom of information request to that health service. <p>Note: Consumers can lodge a request for health information on a health service system (like an EMR). However, they are unable to lodge a request for health information on CareSync Exchange.</p> | <p>Raise any further queries with the health service that processed the request.</p> |
| <p>User activity report Information about who, when and how your record has been accessed on CareSync Exchange</p> | <ol style="list-style-type: none"> 1. Speak to a clinician or health information officer at any health service where you have previously received care. 2. If you require a user activity report, you may need to make a request to that health service. | <p>For queries about specific items in the user activity report, raise this with the relevant health service in that item (this may be a different health service to the one that processed the user activity report).</p> |

If consumers wish to access their health information (that is, their **medical record**), they can make a request to the health service where they have received care.

Health services can provide consumers with access to their health information stored on the health record systems. This may be achieved through an informal process determined by the health service,² or through a formal freedom of information request to the health service.

Access to health information

CareSync Exchange only holds copies of some of a consumers' health information stored on health services' health record systems. As a result, the rights to access health information, as granted in the Health Records Act and the *Freedom of Information Act 1982* (Vic), apply only to information within health service systems like EMR, and not to CareSync Exchange itself.

² OVIC has a [practice note](https://go.vic.gov.au/3wCpVah) that details the circumstances in which health services are able to informally release health records under the *Health Services Act 1988* (Vic) or the Health Records Act, available at <<https://go.vic.gov.au/3wCpVah>>

Consumers can request information on who has accessed their information in CareSync Exchange (through a **user activity report**).

This is done by submitting a request to health information staff at any health service where they have received care.

If a consumer suspects that there has been unauthorised access to their record, they should contact the health service where they think the unauthorised access occurred. Health information management staff at the health service are responsible for investigating and responding to privacy breaches. Consumers must be kept informed of the investigation and outcome.

The user activity report can be generated by any Victorian public health service where CareSync Exchange is used. The department will provide functionality for health services to achieve this. The user activity report specifies the role of the user who accessed the record, the location (which health service) and the timestamp. Clinicians' names are generally not released to protect their privacy, but they may be disclosed where necessary by the health service that employs the clinician.

This report is derived from **user activity logs** that record all uses of CareSync Exchange. The department is responsible for ensuring that CareSync Exchange has this capability.

Pseudonymity

Health consumers may have a pseudonym (different name) when receiving care.

Health services may assign pseudonyms to certain patients who need their identity protected at the time of receiving care. CareSync Exchange collects information from the records of multiple health services. Matching patient identity details (such as name, date of birth and address) occurs at the time of care from details received from the health services' local systems. CareSync Exchange does not generate matches by looking deeper for links in treatment or diagnoses or other health data.

While this serves as an additional layer of privacy protection, health services and health consumers should be aware of the potential outcomes of using a pseudonym. Records may not be matched on CareSync Exchange with those held at other health services. Additionally, there may be limitations in accessing follow-up care or potential critical delays if health service staff need to verify identity, medical history, Medicare or insurance details.

Discussing and correcting records

If consumers believe their health records contain inaccuracies or discrepancies, they are encouraged to discuss this with clinicians or health information management staff at a health service where they have received care.

Identity information

Health information management staff at the health service are responsible for verifying and resolving inaccuracies in identity information. They will work with health information staff in other health services and the department to resolve issues, especially concerning mismatched records or where incorrect information may be stored across different health services.

Health information

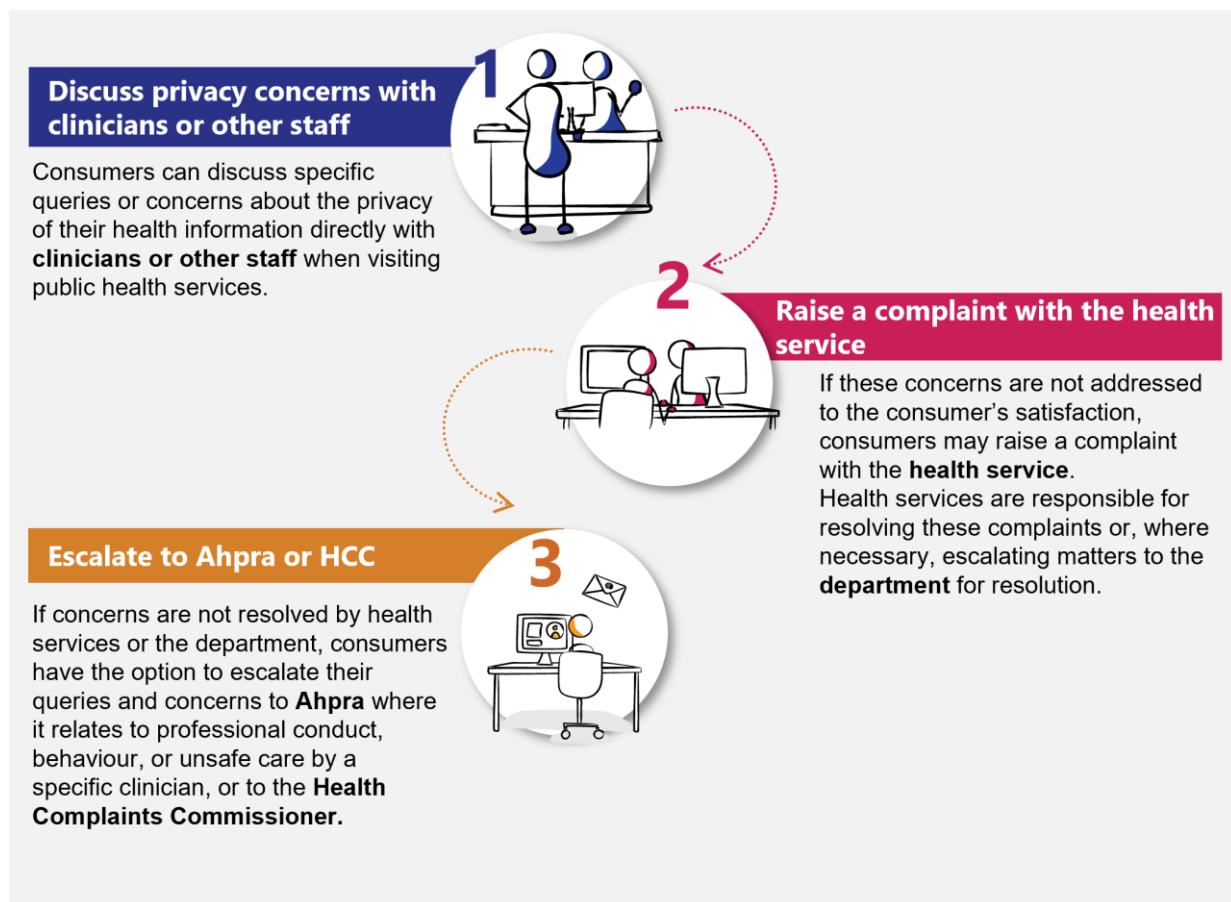
Clinicians and health information management staff at the health service can help consumers to resolve inaccuracies or discrepancies in their record or, if necessary, they can connect the consumer to the health service where the information is held. It is the consumer's responsibility to follow up with the appropriate health service where the information is held.

Resolving concerns or lodging complaints

Consumers seeking more information or clarification about health information privacy in CareSync Exchange should refer to the [Health Information Sharing Legislation Reform](#) on the department’s website <<https://go.vic.gov.au/483vAUA>>. Further general information and resources on health information privacy can be found on the websites of the [Office of the Victorian Information Commissioner](#) (OVIC) at <ovic.vic.gov.au/privacy/for-the-public/your-privacy-rights> and the [Health Complaints Commissioner](#) (HCC) at <hcc.vic.gov.au/public/health-records-individuals>.

If a consumer has a privacy concern, or a complaint about how their health information has been managed or accessed, they can use the three-step issue resolution process described in **Figure 6**.

Figure 6 | Complaints and escalation mechanisms



Chapter 2: Access and use



Health services and the department must ensure that only authorised staff can access and use CareSync Exchange.

CareSync Exchange has been developed for clinicians to use when providing clinical care to a patient. This means that a patient’s health information may be accessed and used by clinicians to help make care decisions. The only other authorised use is to operate and maintain CareSync Exchange, which includes security, record-matching, reporting and auditing activities.

Other uses of patient health record data in CareSync Exchange, such as for research, are not permitted.

Access to CareSync Exchange for clinicians

Clinicians working in Victorian public health services, like public hospitals and ambulance services, will have access to CareSync Exchange for the purpose of informing clinical care for their patient (see **Appendix A**: List of public health services with access to CareSync Exchange). CareSync Exchange will be progressively rolled out at public health services over several years.

Clinicians working in private hospitals, general practice and pharmacies will not have access to CareSync Exchange.

Table 1 | Permitted uses of CareSync Exchange

| Use | Health services | Department of Health |
|------------------------------------------------|-----------------|----------------------|
| Inform clinical care for a patient | ✓ | ✗ |
| Operation and maintenance of CareSync Exchange | ✓ | ✓ |
| Research | ✗ | ✗ |

Health services and the department are responsible for controlling access to CareSync Exchange within their own organisations, subject to limitations on user roles and other access controls on CareSync Exchange discussed later in this document.

There are two ways to access CareSync Exchange:

- Agent Hub.** Users access CareSync Exchange through their local EMR system using their EMR login credentials. Agent Hub presents additional statewide patient health information that is not in the local EMR, enabling a view of recent information about the patient collected across the Victorian public health sector.
- Portal.** Users access CareSync Exchange using login credentials provided by their health service. Portal is restricted to a clinical network accessible inside Victorian public health services. It will be made available to health services that do not have an EMR.

Who can access CareSync Exchange?

Permitted users of CareSync Exchange are set out in **Table 2** for health services and **Table 3** for the department.

Health services are responsible for granting and removing access for users within their organisation, subject to policies set by the department. Departmental users must be authorised by the Secretary.

Table 2 | Users in health services³

| CareSync Exchange user | Function related to CareSync Exchange | Access to health information |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clinician type 1 roles – roles involved in clinical decision-making with the patient, including medical treatment planning (doctors, nurses, midwives, paramedics and allied health professionals such as physiotherapists and social workers) | Access information and make clinical decisions to inform care and treatment | Access to all health information, subject to any additional technical controls outlined in Chapter 3: Permitted information and controls |
| Clinician type 2 roles – roles involved in patient care and treatment (medical students, midwifery and nursing students) | Access information to deliver care and treatment | Access to all health information, except those under additional technical controls, outlined in Chapter 3: Permitted information and controls) |
| Clinical management roles – clinical roles involved in incident management, for example, a senior responsible officer (SRO) or other senior clinical leadership roles | Determine whether access and use of information on CareSync Exchange is appropriate | Access records only to perform audits or investigations |
| Health information management roles – specialised data management roles | <p>Confirm or manage patient identity, incident management relating to matching records or health information accuracy (with the department)</p> <p>Use identification information to fulfil breach and incident management obligations as set out in Chapter 7: Data breach and incident management</p> | <p>Access to identification information (such as the patient's name, date of birth and contact information)</p> <p>Access to health information only for incident management and system operations</p> |

³ Some of the roles described in Table 2 may be performed by the same person.

| CareSync Exchange user | Function related to CareSync Exchange | Access to health information |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Monitoring and audit roles | Identify patterns of use and investigate reports of alleged misuse within the health service as set out in Chapter 6: Monitoring, reporting and auditing | Only access records to perform audits or investigations |
| User administrators | Manage user roles and access to CareSync Exchange within the health service Troubleshoot and provide technical support | No access to health information |

Table 3 | Users in the department

| CareSync Exchange user | Function related to CareSync Exchange | Access to health information |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Departmental super users | Investigate unusual health data reported by users and assess data quality | Access records only to perform audits and investigations or to resolve technical issues |
| Monitoring and audit users | Identify patterns of use and investigate reports of misuse across the state | Access records only to perform audits or investigations |
| User administrators | Manage user roles and access within the department and for Portal users Troubleshoot and provide technical support | No access to health information |
| Departmental CareSync Exchange administration users | Administer the flow of records from health service systems (such as EMRs) into CareSync Exchange Troubleshoot and provide technical support | Access only to maintain flow of records |
| Clinical data management users – specialised data management roles | Confirm or manage patient identity, incident management relating to matching records or health information accuracy (with health services) Use identification information to fulfil breach and incident management obligations as set out in Chapter 7: Data breach and incident management | Access to identification information (such as the patient’s name, date of birth and contact information) Access to health information only for incident management and system operations |

| CareSync Exchange user | Function related to CareSync Exchange | Access to health information |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identity management users | Manage the identity linkages of records across CareSync Exchange Incident management relating to matching records or health information accuracy | Access to identification information (such as the patient’s name, date of birth and contact information) Access to health information only for incident management |

Other access controls

Given the dynamic and public environment of health services, the department and health services must ensure that accidental disclosure of information on CareSync Exchange is minimised through general access controls and work practices.

Table 4 | Access controls and work practices

| Access control | Access to the system | Managed by |
|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------------|
| Login details to ensure only authorised users have access | Agent Hub (through the health service’s local EMR) | Health service |
| | Portal | Health service or department (depending on user type) |
| Timeout feature to ensure that access to CareSync Exchange is not left open | Agent Hub (through the health service’s local EMR) | Health service (as per the EMR timeout feature) |
| | Portal | Health service or department (depending on user type) |
| Physical and ergonomic controls to prevent accidental disclosure, for example, privacy screen filters and desk set-up | N/A | Health service |
| Data loss prevention measures that describe permitted and prohibited actions like printing, copying and emailing health information | N/A | Health services or department (depending on user type) |

Chapter 3: Permitted information and controls



This chapter explains what information is held in CareSync Exchange and how it is presented to users. It outlines the responsibilities of clinicians, health services and the department for maintaining that information. These responsibilities include ensuring that only specific health information is presented and that there are additional controls in place where required.

Health consumers hold different opinions regarding the sensitivity of their own health information. Nevertheless, CareSync Exchange presumes that all health information is sensitive and should be treated in a way that prioritises privacy.

This chapter describes the types of information that is collected in the system, and how specific, sensitive health information is presented to users.

Permitted information and controls are also described in the chapters that outline restrictions on access and use ([Chapter 2: Access and use](#)) and security ([Chapter 4: Training](#)),

Types of information collected by CareSync Exchange

CareSync Exchange does not collect every detail from systems in the health services. It is limited to information groups that have been selected to provide clinicians with the most relevant information to help inform a patient's care. These may include:

- Identity details of the patient (like their name, date of birth and contact information)
- Information about their previous visits to health services:
 - the health service(s) they have visited
 - the reason for their visit(s) and the duration of their visit(s)
 - medications
 - allergies
 - alerts
 - documents (such as discharge summaries)
 - emergency department letters
 - outpatient letters
 - pathology reports
 - lab reports
 - radiology reports

The department is responsible for ensuring CareSync Exchange only collects information in these groups. Other health information that is currently collected by health services, such as detailed clinician notes about patient visits, is excluded from CareSync Exchange.

How is sensitive information managed?

While all health information on CareSync Exchange is sensitive, some types of health information have heightened sensitivity due to:

- a greater risk of misuse of personal information
- more serious repercussions if there is a privacy breach, including risks to patient or clinician safety, or stigma associated with the sensitive information.

When using CareSync Exchange, users must exercise care when viewing sensitive categories of health information. This may include the following categories:

- Aboriginal and/or Torres Strait Islander status
- alcohol and other drug use
- children and young people in out-of-home care
- chronic and complex medical conditions or conditions that are susceptible to misdiagnosis
- disability
- family violence
- gender and identity
- genetic conditions
- infectious diseases
- mental health
- multicultural communities
- neurodivergence
- public-profile individuals
- sexual assault or harm
- sexual and reproductive health.

Health services have existing protections in place for these sensitive categories of health information and CareSync Exchange builds on these. It has additional protections for some sensitive categories of health information, either by not collating the information, putting the information behind break glass, or through operational procedures and training. This will be reviewed periodically as outlined in [Chapter 9](#):

Ongoing improvement and review.

Health services are responsible for establishing processes and configuring their health information systems to ensure that clinicians record information in the EMR accurately, so that sensitive information is appropriately managed when the consumer next visits a health service.

Most mental health information will not be visible on CareSync Exchange

General health information and mental health information are handled differently.

CareSync Exchange has been designed to store and handle general health records as enabled by the Health Legislation Amendment (Information Sharing) Act. Mental health information is governed by separate legislation – the *Mental Health and Wellbeing Act 2022* (Vic).

Most mental health information will not be visible on CareSync Exchange.

When clinicians provide care to patients, they document information in the EMR like the reason for the patient's visit, the primary diagnosis and the place of care (that is, the clinical department or unit).

When CareSync Exchange collects information held by an EMR and health service systems, it checks for indicators of mental health information such as a mental health diagnoses and treatment at a mental health unit in a health service.

Any visits that have this mental health information will be tagged by CareSync Exchange. Information that has been tagged as mental health information will not be visible to users of CareSync Exchange. This means that clinicians will not be able to see those records. Patients may choose to make the clinician aware of their mental health history when discussing their clinical history.

However, some information on CareSync Exchange may include references to mental health.

Some information relating to a person's mental health may be collected as part of general health records, for example, in discharge medications and summaries of visits where patients present with symptoms related to general health. This information will be visible in CareSync Exchange.

There will be a separate project outside of this PMF for mental health information sharing.

This separate project will implement [Recommendation 62](#) of the Royal Commission into Victoria's Mental Health System <<https://go.vic.gov.au/4acF4Nx>> by designing an information sharing system for mental health. The information sharing system for mental health will only be available to authorised staff working at **mental health and wellbeing services**.

This project is still to be established and will be handled under the Mental Health and Wellbeing Act with its own governance and consumer engagement process.

As defined in the *Mental Health and Wellbeing Act 2022* (Vic), **mental health and wellbeing services** are professional services that:

- improve or support a person's mental health or wellbeing
- assess or provide treatment or support to a person with mental illness or psychological distress
- provide care or support to a person who is a family member, carer or supporter of a person with mental illness or psychological distress.

Some categories of sensitive information will be behind break glass

CareSync Exchange has additional protections for some specific sensitive health information that poses a greater risk to patient safety or misuse of personal information. This is achieved by using a **'break-glass'** feature as a technical control to limit visibility of information and reinforce the significance of the sensitivity.

The categories of sensitive information that will have a break-glass feature include:

- family violence

Break glass is an informal term for where a system asks the user to confirm they want to proceed beyond a point. In CareSync Exchange it is used for certain categories of sensitive information or the records of certain individuals who are particularly vulnerable. Access to information behind break glass will be restricted and not immediately available unless clinicians indicate a reason to see the information. Users are reminded that access to sensitive information will be monitored and audited.

- children and young people in out-of-home care
- public-profile individuals
- sexual assault or harm.

If an EMR records that the patient has been subject to family violence, sexual assault or harm, is a child or young person in out-of-home care or is a public-profile individual, their record (and therefore their health information) on CareSync Exchange is held behind break glass. The clinician must acknowledge this by selecting 'I agree' and providing a reason on a panel before the information is visible to them, as shown in **Figure 7**.

Only clinician type 1 users (those who are involved in clinical decision-making) will be able to access information behind break glass. Clinician type 2 users (those who are involved in patient care and support) will not be able to access this information.

CareSync Exchange will also have a flag on the patient's record to indicate additional sensitivity and to help the clinician tailor their care. Training will be provided to guide clinicians to discuss the likely relevance of the information with patients before breaking glass. Break-glass events must be monitored and audited by the relevant health service and the department.

Figure 7 | Case study: How does break glass work to protect sensitive information?

How does break-glass work?

The following scenario explores how clinicians may use the break-glass feature on CareSync Exchange.



Maya is a recent survivor of family violence. She lives in Mildura. Maya is spending the weekend in Melbourne visiting a friend. Maya has frequent migraines, and she is starting to feel unwell.

Maya is semiconscious and struggling to breathe, so her friend takes her to a hospital in Melbourne. Her friend shares with emergency staff that Maya complains about headaches often, but she does not know what is causing them. Emergency staff discuss her symptoms and potential causes.

With the help of Maya's friend, the emergency clinician (clinician type 1 user) treating Maya locates her record in CareSync Exchange. The clinician sees that Maya's entire record is behind break glass, so no information about Maya is immediately visible. The clinician needs to access the information to immediately care for Maya, so they click on the 'I agree' panel and select the reason for viewing Maya's record.

Using the information on CareSync Exchange, the clinician diagnoses Maya and admits her to the hospital ward for treatment.

- ✓ The clinician's break-glass action is recorded in the user activity log for later audit or review.
- ✓ As part of their supervisory role, the senior responsible officer will promptly review the clinician's access and use of CareSync Exchange and determine whether it was appropriate.
- ✓ Maya can request a user activity report to see who has accessed her record on CareSync Exchange.

Other categories of sensitive information are protected through operational procedures and training

Other categories of sensitive information will be visible to clinicians (types 1 and 2) and other users of CareSync Exchange in health services and the department with some additional operational procedures and training to guide clinicians. These are described in more detail in [Chapter 4: Training](#). Access to sensitive information will also be captured in the audit logs.

Data collection, retention and destruction

CareSync Exchange does not collect or hold information collected prior to 7 February 2021. The department is responsible for ensuring CareSync Exchanges is compliant with the *Public Records Act 1973* (Vic) and standards set by the Keeper of Public Records for the retention or destruction of health information and user activity logs on CareSync Exchange.

Chapter 4: Training



The department and health services must ensure that users have the necessary technical skills and clinical knowledge to appropriately access and use CareSync Exchange.

Training for users of CareSync Exchange

In line with existing Victorian public health service practices and the National Safety and Quality Health Service Standards, health services already provide training to clinicians so that they understand the importance of ethical and regulatory requirements that protect consumers’ privacy.

Furthermore, all users must complete training for CareSync Exchange. The training must cover the operation of CareSync Exchange and compliance with the PMF as described in **Table 5**.

The department is responsible for developing the training modules and materials delivered by all health services. These modules and materials should be incorporated into existing staff training that covers privacy, digital records and health information sensitivities. Health services must ensure that there is periodic refresher training for users, coordinated with other recurring training.

Table 5 | Relevant training for CareSync Exchange users

| CareSync Exchange user | Training content |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clinicians | <ul style="list-style-type: none"> • Background and context of CareSync Exchange, including legislative requirements and obligations • Information privacy obligations • Access and use of CareSync Exchange, relevant to their role within the health service • CareSync Exchange features, including sensitive categories of health information and what sensitive information is intentionally excluded or under additional technical controls • Implications of CareSync Exchange for clinical practice, for example, reinforcing patient-centred care, mitigating cognitive bias and exercising discretion in interactions • Relevant case studies of good practice and common pitfalls to avoid • Escalation process for incidents or other issues |
| Other system users including: <ul style="list-style-type: none"> • department super users • clinical management roles (health services) • health information management roles (health services) • monitoring and audit users | <ul style="list-style-type: none"> • Background and context of CareSync Exchange • Information privacy obligations • Access and use of CareSync Exchange, relevant to their specific roles (including all relevant training content provided to clinicians for clinical management roles) |

| CareSync Exchange user | Training content |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • user administrators • departmental system administration users • identity management users | <ul style="list-style-type: none"> • Escalation process for incidents or other issues |

Good clinical practice

While CareSync Exchange has multiple measures to protect consumer privacy, consumers also have concerns about clinical practice when their information is accessed and used. These concerns related to clinical practice- are not unique to CareSync Exchange – they occur across other healthcare contexts.

Nevertheless, it is important that communication with and training materials for CareSync Exchange users recognise and reinforce the foundational privacy principles inherent to clinical practice that are aligned with the Health Records Act, the *Australian charter of healthcare rights (second edition)* and resources provided by the Australian Health Practitioner Regulation Agency (Ahpra) for [managing health records](#). This guidance includes several important considerations:

- **Patient-centred care.** CareSync Exchange should be used in a way that complements, rather than overlooks, the patient’s perspective. Clinicians will continue to focus on communicating with their patient to understand the nuances in their clinical history, rather than relying on an interpretation of the patient made by other clinicians.
- **Mitigating cognitive bias.** Cognitive bias in clinicians can impact on a health consumer's experience, treatment and outcome. Increased awareness of cognitive bias and strategies to mitigate its impact can reduce harmful, discriminatory or stigmatising practice. Clinicians will be aware that CareSync Exchange offers a partial view of health information. Although this is very useful, it will not provide the patient's entire health history. Education and training materials for clinicians who use CareSync Exchange will include approaches to mitigate the impact of cognitive bias. Other resources, such as Ahpra’s practice note on managing health records,⁴ will also support clinicians to maintain clear and accurate records in their local systems to minimise cognitive bias.
- **Appropriate access and use of information.** Access and use of health consumer information on CareSync Exchange will be carefully considered, especially information behind additional protections like break-glass features.
- **Sensitive information.** Clinicians will exercise additional discretion in interactions involving categories of sensitive information that raise additional specific privacy concerns. These categories are shown in **Table 6**. Clinicians should only seek to access this sensitive information if they think it will help them make decisions that lead to the provision of safe and effective clinical care.

⁴ Ahpra has a [practice note](#) on managing health records.

Table 6 | Considerations for clinical practice when handling sensitive information

| Sensitive information | Description | Reasons for additional sensitivity |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aboriginal and/or Torres Strait Islander status | Information about a person’s Aboriginal and/or Torres Strait Islander status | <ul style="list-style-type: none"> • Risk of stigma and bias associated with Aboriginal and/or Torres Strait Islander status • Focus on cultural safety when accessing and using healthcare services |
| Alcohol and other drugs | Information related to alcohol and other drug use, including substance dependency and treatment | <ul style="list-style-type: none"> • Risk of stigma and bias associated with alcohol and drug use |
| Children and young people in out-of-home care | Information about children and young people in out-of-home care | <ul style="list-style-type: none"> • Risk of stigma and bias associated with children and young people in out-of-home care • Risk of retraumatising the patient |
| Chronic and complex conditions, or conditions that are susceptible to misdiagnosis | Information about chronic and complex medical conditions that are often long-term and require ongoing management These conditions may be susceptible to misdiagnosis. | <ul style="list-style-type: none"> • Risk of stigma and bias associated with chronic and complex conditions • Risk of biases from past diagnoses, which may not be accurate or contemporary |
| Disability | Information about physical, cognitive or psychiatric conditions that may require specialised care or adjustments | <ul style="list-style-type: none"> • Risk of stigma and bias associated with disability • Risk of over-reliance on information from health information systems rather than a patient’s needs and perspectives |
| Family violence | Information related to incidents or risks of family violence | <ul style="list-style-type: none"> • Risk of stigma and bias associated with family violence • Greater risk to personal safety if disclosed to a third party or accessed without authorisation by a health service employee • Risk of retraumatising the patient |
| Gender and identity | Information about an individual's gender identity, including whether they identify as transgender, non-binary or gender diverse | <ul style="list-style-type: none"> • Risk of stigma and bias associated with gender and identity • In small communities, greater risk of disclosure and judgement outside of the health service setting |
| Genetic conditions | Information about an individual's diagnosed disease related to known genetic predispositions | <ul style="list-style-type: none"> • Risk of stigma and bias associated with genetic conditions • Risk of unintended disclosure to a family member |

| Sensitive information | Description | Reasons for additional sensitivity |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | <ul style="list-style-type: none"> • Risk of disclosing rare genetic conditions to other clinicians not involved in the patient's care |
| Infectious diseases | Information about infectious diseases that may carry risks for clinicians | <ul style="list-style-type: none"> • Risk of stigma and bias associated with some infectious diseases like tuberculosis, HIV and hepatitis B and C |
| Mental health | <p>Information about mental health condition(s)</p> <p>Most mental information will not be visible on CareSync Exchange. However, there may be some instances where mental health information is visible, for example, in discharge records and summaries for patients experiencing symptoms related to general health.</p> | <ul style="list-style-type: none"> • Risk of stigma and bias associated with mental health condition(s) • Patient's perception that clinicians may incorrectly attribute their physical symptoms to a mental health condition |
| Multicultural communities | Information about a person's heritage, community affiliations, and sometimes health conditions that are of particular prevalence or concern within these communities | <ul style="list-style-type: none"> • Risk of stigma and bias associated with multicultural communities • Focus on cultural safety when accessing and using healthcare services |
| Neurodivergence | <p>Information related to the variations in how an individual's brain functions and processes information</p> <p>This encompasses various conditions including but not limited to autism spectrum disorder, attention deficit hyperactivity disorder and dyslexia.</p> | <ul style="list-style-type: none"> • Risk of stigma and bias associated with neurodivergence • Risk of over-reliance on information from health information systems, or such information taking precedence over a patient's individual needs and perspectives |
| Information about public-profile individuals | Information related to public-profile individuals or people in smaller communities where it is easy to identify the individual | <ul style="list-style-type: none"> • Greater risk of misuse by users of CareSync Exchange, for example, by accessing patient information out of curiosity • In small communities, greater risk of disclosure outside the health service setting |
| Sexual assault or harm | Information related to incidents involving unwanted, nonconsensual behaviour of a sexual nature | <ul style="list-style-type: none"> • Risk of retraumatising the patient • Risk of disclosure to a third party, such as a family member or guardian |
| Sexual and reproductive health | Information regarding sexual health, reproductive history and related medical conditions | <ul style="list-style-type: none"> • Risk of stigma and bias associated with sexual and reproductive health • Risk of disclosure to a third party such as a family member or guardian, particularly if the patient is a minor |

| Sensitive information | Description | Reasons for additional sensitivity |
|-----------------------|-------------|----------------------------------------------------------------------------------------------------------------------|
| | | <ul style="list-style-type: none"> <li data-bbox="930 320 1342 344">• Risk of re-traumatising the patient |

Information for management and executive roles

In addition to receiving user training for CareSync Exchange, staff in department and health service management and executive roles must know their responsibilities and accountabilities relating to management and oversight of CareSync Exchange and PMF within their organisations. This is described in **Chapter 8: Operational governance**.



Chapter 5: Security

The department and health services must ensure that CareSync Exchange has appropriate cybersecurity infrastructure in place to protect information on CareSync Exchange from unauthorised access and tampering.

Cybersecurity refers to protecting data in CareSync Exchange through security measures for data, networks and devices to prevent unauthorised access and use, disclosure, modification, disruption or destruction of data.

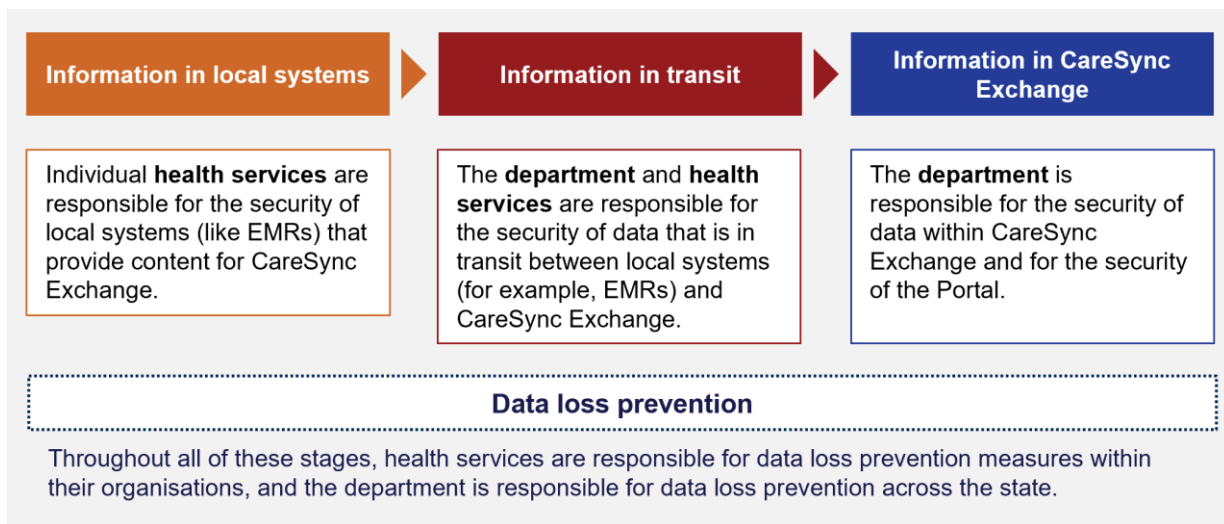
The Victorian public health sector already delivers digital solutions with high standards for security. CareSync Exchange will draw upon the expertise of these Victorian digital health solutions.

The department and health services have joint responsibility for cybersecurity and must ensure the implementation of **data loss prevention** measures on CareSync Exchange, illustrated in **Figure 8** below. An essential element of security is vigilance, which is covered in **Chapter 6**:

Monitoring, reporting and auditing. In the event of a security breach, the department and health services must fulfil responsibilities set out in **Chapter 7**: Data breach and incident management.

Data loss prevention involves identifying and preventing inappropriate sharing, transfer and use of health information, whether it is malicious or well-intentioned. Data loss prevention measures include using secure networks for CareSync Exchange data in storage and in transit, and restricting creation and distribution (for example, by printing) of hard copies containing health information.

Figure 8 | Cybersecurity responsibilities



Data storage in CareSync Exchange

All CareSync Exchange data, which includes health information and user activity data, must be stored exclusively in secure department servers located within Australia. The department is to maintain cybersecurity infrastructure, protocols and oversight to protect CareSync Exchange.

These security measures must encompass people, processes, governance and technical security measures. Examples of such measures include (but are not limited to) storage facilities with

restricted access, user access reviews, role-based access control, authentication and authorisation processes, and monitoring by the department of any third party access to servers or CareSync Exchange.

Security of data in transit between systems

The department and health services are responsible for protecting data in transit from individual health services to CareSync Exchange. They should use security measures that align with Victorian Government legislative and regulatory requirements and standards relating to data transmission,⁵ including advanced encryption standards, departmental data communication protocols, and any relevant Commonwealth Government guidance. Health services must also ensure that security controls are in place on local systems like an EMR to support these security measures.

Security testing

Health services are required to implement and attest to the department's Health Sector Cyber Security Assessment package,⁶ which includes cybersecurity baseline controls for the Victorian health sector. This tool strengthens health services' ability to detect, protect and respond to the evolving cybersecurity threat environment. The department must ensure that health services meet the appropriate cybersecurity standards before onboarding to CareSync Exchange.

CareSync Exchange and its associated infrastructure must undergo rigorous penetration testing and other cybersecurity testing that comply with the Health Sector Cyber Security Assessment package, established Victorian Government cybersecurity guidelines and the Victorian Protective Data Security Standards. This approach includes testing by independent third parties to ensure the security of data stored in CareSync Exchange.

Security for the Portal

The department and health services are responsible for additional security restrictions to access and use the Portal. Access to the Portal will be restricted to a clinical grade network that is only accessible inside the department and Victorian public health services. Patient search functions on the Portal will be restricted to limit unauthorised access.

⁵ Standards include those specified in the department's Health Sector Cyber Security Assessment, the Commonwealth Government's *Protective security policy framework* and *Information security manual*, and *Victoria's cyber strategy 2021: a cyber safe Victoria*.

⁶ The Health Sector Cyber Security Assessment is a package of cybersecurity controls drawn from leading national and international cybersecurity organisations and frameworks like the Australian Signals Directorate's *Information security manual* and the National Institute of Standards and Technology in the United States. The Health Sector Cyber Security Assessment is tailored to the requirements of the Victorian health sector. Maturity levels for each control provide an indication of an organisation's cybersecurity maturity.

Chapter 6:

Monitoring, reporting and auditing



The department and health services must establish and undertake monitoring, reporting and auditing to ensure that access and use of CareSync Exchange is appropriate.

The department and health services must ensure that only authorised people access CareSync Exchange and that their access is only for permitted uses. CareSync Exchange must record every access and use action, for every use, in user activity logs.

Monitoring, reporting and auditing are three tools the department must use to ensure that access and use of CareSync Exchange across Victorian public health services is aligned with the Health Legislation Amendment (Information Sharing) Act and the PMF.

Each health service must undertake monitoring and reporting within their own organisation and facilitate auditing by the department.

The department will support health services with their monitoring, reporting and auditing responsibilities by providing access to relevant tools and procedures.

Monitoring

Monitoring is the supervision of access to, and use of, CareSync Exchange to detect and prevent misuse of consumer health information by users or unauthorised persons.

Break glass

The department must ensure that CareSync Exchange has a mechanism to detect when a user takes a break-glass action. The action must be recorded with details including, at a minimum, the user's identity, their reason for breaking glass (entered by the user at the time of breaking glass), the health service, the type of sensitive information accessed, and date and time information.

Records of break-glass events must be stored by the department for reporting and auditing purposes, and to fulfil consumers' rights to know when their health information has been accessed.

The department must ensure that health services are able to access these logs as required for monitoring purposes.

Additionally, the department is to ensure that CareSync Exchange has functionality to alert the SRO or equivalent role whenever a break-glass event occurs in their health service. The SRO must review break-glass events, as illustrated in [Figure 9](#). Health services must ensure that SROs are appropriately equipped to monitor and consider the appropriateness of the break-glass usage in accordance with the department's policy and training materials.

The purpose of break glass is to provide a signal to clinician type 1 users that they are proceeding to view more sensitive information, without creating workflows that delay the delivery of clinical care.

Central to break glass is **attestation**, which means that the clinician must give a reason for accessing the information. CareSync Exchange must present a small set of reasons for the clinician to choose from, along with a free-text option.

The department and health services must maintain a process to address instances of inappropriate break-glass use and escalate these events to a breach or incident response if necessary (see **Chapter 7: Data breach and incident management**).

Figure 9 | Case study: how will break glass be monitored?

How is break-glass monitored and audited?

The following scenario explores how break-glass use is supervised and reviewed for appropriateness in CareSync Exchange.

Maya is being treated for frequent migraines in a hospital emergency department. The emergency clinician breaks glass, providing a reason for doing so to view Maya's patient record, as it is protected due to her recorded family violence history.



When a clinician (clinician type 1 user) breaks glass, their username, reason for breaking glass, and the date and time are logged and sent via an alert to a senior responsible officer (or equivalent role) in the health service.

Brian is a senior responsible officer (monitoring and audit user) at the hospital for CareSync Exchange. Brian promptly reviews the break-glass alerts for the emergency clinician's access event relating to Maya's care and treatment. The clinician has selected 'emergency situation' as the reason for the break glass. Considering this reason given for the break glass, and the fact that the emergency clinician only broke glass only once, Brian deems the decision appropriate and takes no further action.

- ✓ Health services have a process to review instances of break glass with consideration of risk, and a process to review other activity at least monthly, to ensure that user access and break-glass use is appropriate.
- ✓ In this case, if the emergency clinician had misused break-glass – for example, by using break-glass repeatedly, even after Maya was no longer under their care – the health service would have implemented corrective action and notified Maya of the privacy breach.
- ✓ Staff training ensures that clinicians do not seek to breach privacy (for example, by breaking glass) and that health information staff, like Senior Responsible Officers, are able to recognise inappropriate use.

Unauthorised access

Health services must ensure that their EMRs have a mechanism to detect unauthorised access attempts and block repeated unsuccessful attempts when they occur in near real-time.

Similarly, the department must ensure the Portal has a mechanism to detect unauthorised access attempts and block repeated unsuccessful attempts when they occur in near real-time.

Details of these events must be recorded when they are detected including, at a minimum, the username associated with the attempt (for attempts through viewing agents), geographic information, and date and time information.

The department and health services must have a process to initiate data breach and incident management if the access or use is deemed suspicious or has resulted in a data breach (see **Chapter 7: Data breach and incident management**).

Reporting

Reporting is the regular review of access to CareSync Exchange across a health service to identify patterns or trends of use that require a systemic corrective response.

Monthly reporting on break-glass and unauthorised access events

The department must ensure that CareSync Exchange has a mechanism for monthly tabulation of all break-glass and unauthorised access events via viewing agents in each health service. The department must facilitate health services to present this report to their nominated SRO (or equivalent).

Health services must have processes and delegations to ensure access reports are reviewed and any patterns or trends in use are considered in line with both health service and department guidelines on unauthorised access.

The department and health services must also maintain processes to:

- address patterns of unauthorised access
- initiate data breach and incident management if an access event is deemed suspicious or results in a data breach.

Annual usage reporting

Internal report for each health service and the department

Each public health service must prepare for management an annual report of CareSync Exchange usage for managers and executives in their health service and the department. It should include the following information:

- **CareSync Exchange interactions** – metrics on user logins (including whether CareSync Exchange was accessed on Agent Hub or through the Portal), types of health information accessed, instances of break-glass events, and attempts at unauthorised access occurrence.
- **Unusual activity detection** – a summarised breakdown of detected unusual activity and misuse patterns within the health service. This involves specific user activity and trends that deviate from their normal operations.
- **Feedback and complaints** – feedback and complaints about PMF adherence and CareSync Exchange performance and functionality, made directly by staff and patients to the health service and indirectly through the HCC. This will align with incident reporting through the Victorian Health Incident Management System.
- **Recommendations** – identified recommendations for improvements and progress report on implementation of recommendations, to be informed by feedback and complaints from previous reporting and relevant department input, such as external audit results.
- **CareSync Exchange update information** – details on CareSync Exchange updates and associated impact on local operations, as well as any customisations or configurations made specific to the individual public health service.
- **CareSync Exchange performance metrics** – the department is responsible for monitoring data on CareSync Exchange uptime, downtime, and technical issues encountered.

Public-facing report for consumers

The department must prepare an annual report for the Victorian public on CareSync Exchange and publish it on the [department's website](https://go.vic.gov.au/483vAUA) <https://go.vic.gov.au/483vAUA>. This report must be accessible and provide consumers with sufficient understanding of:

- [CareSync Exchange interactions](#) – a summary of user interactions and types of data accessed across Victorian public health services
- [feedback and responses](#) – a summary of feedback and complaints received across Victoria, along with actions taken or proposed to address identified areas of concern.

Auditing

Auditing is the periodic assessment of access to and usage of CareSync Exchange across Victoria. It includes checking systems and permissions to ensure they are configured to facilitate appropriate access and use.

The department must establish a process to assess patterns of use across the state and undertake spot checks of access and use. The department must also conduct regular checks of the user lists maintained by each health service and the department to confirm that only appropriate staff have access to CareSync Exchange.

Chapter 7: Data breach and incident management



The department and health services must establish and follow processes to prevent, mitigate and manage suspected and confirmed data breaches and incidents, including near misses.

A data breach is unauthorised access, use, disclosure, modification or loss of data that compromises the privacy, security, confidentiality or integrity of CareSync Exchange.

A data breach in CareSync Exchange might mean that health information is inadvertently disclosed, accessed by an unauthorised system user or stolen.

A data breach typically involves non-compliance with a privacy principle. The department and health services must comply with the following privacy principles:

- Health Privacy Principles set out in the Health Records Act
- Information Privacy Principles of the *Privacy and Data Protection Act 2014* (Vic).

A data breach can occur when unauthorised users gain improper access to CareSync Exchange, for example, if a malicious actor (such as a hacker) accesses CareSync Exchange.

Breaches may also occur when an authorised user misuses the system, for example, if a clinician accesses the records of a public-profile patient out of curiosity.

There are other instances that are not data breaches, especially where clinicians are collaborating with their colleagues for the purpose of caring for their patients, for example:

- When a patient is in the process of being transferred from health service A to health service B, the clinician at health service B may need to access the patient's record on CareSync Exchange to support continuity of care.
- A clinician may consult with a peer clinician about a patient's health record on CareSync Exchange to better inform the patient's care.

The department's agreements with health services require them to immediately notify the department when they become aware of a breach or possible breach of the organisation's privacy and data protection obligations.

The department and health services already have robust data breach processes in place for EMR and other systems. In the event of a breach, the department and health services must also follow breach management processes specific to CareSync Exchange.

Any unauthorised access or use of CareSync Exchange (or disclosure of sensitive information from within it) is a criminal offence and may incur a penalty of 240 penalty units (\$44,380 in 2023) or two years of imprisonment.

Figure 10 outlines the department's and health services' responsibilities regarding breach and incident management.

Figure 10 | Breach and incident management process



Chapter 8: Operational governance



The department and health services are responsible and accountable for ensuring the PMF is followed. This chapter explains those responsibilities and accountabilities.

Roles and responsibilities

Victorian Minister for Health

The Victorian Minister for Health is required to establish the PMF under the Health Legislation Amendment (Information Sharing) Act.

Victorian Department of Health

The department must ensure that CareSync Exchange operates in a way that complies with the PMF. The department is accountable for both the PMF and CareSync Exchange's adherence to it. Also, the department is responsible for updating and aligning the PMF with legislation and other government policies.

Secretary of the Department of Health

As the steward of CareSync Exchange, the Secretary of the department has authority and accountability for CareSync Exchange and the PMF under the Health Services Act. The Secretary may delegate responsibilities to other departmental officers with program responsibilities.

The Secretary will also appoint suitably qualified stakeholders to form the Health Information Sharing Management Committee. This committee will provide advice to the Secretary to oversee the operation of CareSync Exchange and the PMF.

Executives at health services

Health service executives are required to ensure that effective systems and processes are in place so that users accessing CareSync Exchange within their health service comply with the PMF. It is the responsibility of health service executives to implement corrective actions when individuals within their health service fail to comply with the PMF.

Health service executives and boards are accountable to the Minister, the Secretary, the department and the Victorian Auditor-General for their organisations.

Health service boards may delegate responsibilities to the chief executive officer and other executive officers of the health service as appropriate and in alignment with other responsibilities under the Health Services Act.

Transition to operational governance

A project governance structure is in place to support implementation and delivery of CareSync Exchange and the PMF. This will transition to operational governance (as described in this chapter) in alignment with the rollout of CareSync Exchange at health services.

In addition to the PMF, there is a range of supporting materials catering to the needs of different groups that interact with CareSync Exchange. These materials encompass communication

resources, detailed policies, procedural guidelines, breach management materials, and other resources that are essential for the secure and effective operation of CareSync Exchange.

The department maintains an ongoing commitment to engage with representatives from vulnerable communities, including Aboriginal communities, children in out-of-home care and Victorians affected by violence.

Chapter 9: Ongoing improvement and review



The department and health services must ensure that the PMF remains fit for purpose and adaptable to changes in the health information privacy landscape.

Ongoing improvement

As part of ongoing improvement to CareSync Exchange and the PMF, the department is responsible for monitoring compliance with the PMF and reporting this to the Health Information Sharing Management Committee.

Established by the Secretary, this committee is an independent body that provides advice to the Secretary to oversee CareSync Exchange, PMF and related policies and strategic improvements.

The reporting includes assessing CareSync Exchange technical maintenance and enhancements, as well as existing privacy policies and procedures protecting the privacy of health consumers within CareSync Exchange.

An assessment of opportunities for improvement will occur:

- six months after CareSync Exchange has been rolled out at the first health service
- every two years thereafter
- after an incident or breach on CareSync Exchange.

When monitoring adherence to the PMF and seeking continuous improvement, the department may consult the following groups:

- [consumers and clinicians](#), to ensure technical controls and other measures are appropriate and address specific privacy concerns
- [CareSync Exchange users](#), to receive suggestions on improvement opportunities (users must be able to provide suggestions through their employer)
- [health service and vendor representatives](#), to consider the legal, policy, technical and design implications of suggested improvements on CareSync Exchange, including updates to training materials for CareSync Exchange users
- [relevant governance and advisory groups, including the Health Information Sharing Management Committee](#), to receive advice and endorsement of any updates to CareSync Exchange, the PMF and supporting documents
- [other department representatives](#), to implement updates to CareSync Exchange, the PMF and other supporting documents.

Independent review

An expert panel convened by the Victorian Minister for Health must carry out a review of the PMF and CareSync Exchange after 7 February 2026. The review must be completed no later than 7 February 2027.

The expert panel must include members with expertise in human rights and privacy matters, legal and regulatory compliance, health information systems, clinical care, healthcare quality and patient safety and consumer or patient advocacy.

The outcomes of the review and recommended changes to the PMF must be tabled in Victorian Parliament within three sitting days after the independent review's final report is provided to the Minister.

The review should investigate and provide recommendations on:

- whether health information is sufficiently protected
- which health services should be participating services
- inappropriate use of specified health information
- financial implications and administrative challenges for participating health services
- the effectiveness of CareSync Exchange in fulfilling its intended purpose, including analysis of data from quarterly reports on patient health outcomes, safety and experience, and any other factors that impact the privacy management and benefits on CareSync Exchange.

The review may also examine and provide recommendations on:

- current issues and trends relating to health information systems
- data management
- information technology security
- patient privacy
- any other matters deemed relevant.

The Minister must consider any recommendations made by the independent review, including any recommendations to amend relevant legislation, within 18 months of receiving the final report.

Glossary

People and organisations

Table 7 | People and organisations mentioned in the Privacy Management Framework

| Term | Definition |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allied health professional | <p>Allied health professionals are clinicians who work collaboratively as part of a team alongside medical doctors, nurses and midwives and other professionals to provide care. Many professions fall under allied health, for example:</p> <ul style="list-style-type: none"> • audiologists • pharmacists • physiotherapists • orthotists/prosthetists • radiographers • social workers. |
| Australian Health Practitioner Regulation Agency (Ahpra) | <p>The Australian Health Practitioner Regulation Agency (Ahpra) is the national body responsible for regulating health practitioners across Australia. It works in collaboration with 15 national boards that are responsible for regulating specific professions, including medicine, nursing, midwifery, dentistry, pharmacy and others. Ahpra’s primary role is to register health practitioners, develop standards, codes and guidelines for practice, and investigate complaints and disciplinary actions regarding health practitioners.</p> |
| Clinician | <p>A clinician is a healthcare professional who is trained and qualified to provide clinical services to patients. Clinicians mentioned in this document are those working at Victorian public health services, including:</p> <ul style="list-style-type: none"> • medical doctors • nurses • midwives • allied health professionals • paramedics. <p>Private health services, general practice and pharmacies are not included.</p> <p>The Australian Commission on Safety and Quality in Health Care provides further guidance on who is considered to be a clinician.</p> |
| Health consumer | <p>A health consumer (also referred to as a consumer in this document) is an individual who uses (or may use) a Victorian public health service, or someone who provides support for a person using a Victorian public health service. Consumers can be patients, carers, family members or other support people.</p> |
| Health Complaints Commissioner (HCC) | <p>The Health Complaints Commissioner (HCC) is an independent statutory body that provides health consumers and service providers in Victoria with an independent complaints resolution mechanism for complaints about health care and the handling of health information in Victoria.</p> |

| Term | Definition |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Keeper of Public Records | The Keeper of Public Records is a role within the Public Records Office that establishes standards for management of public records. In the context of this document, public records are information on CareSync Exchange such as health information and user activity logs. |
| Office of the Victorian Information Commissioner (OVIC) | The Office of the Victorian Information Commissioner (OVIC) is the regulator of public sector information in Victoria. It oversees data protection, freedom of information and privacy, ensuring compliance with relevant laws. |
| Patient | A patient is a health consumer who is receiving emergency care or clinical care at a Victorian public health service. |
| Senior responsible officer (SRO) | The senior responsible officer (SRO) is a senior clinical leadership role (for example, a chief medical officer, chief medical information officer or chief nursing and midwifery information officer) in a health service. The SRO has the authority to act on behalf of a health service. |
| CareSync Exchange user | A user of the Victorian Electronic Patient Health Information Sharing System, either for the purpose of accessing information to inform medical treatment and care or maintenance of CareSync Exchange’s functionality. CareSync Exchange users include clinicians, administrative, and technical roles within health services and the department. A complete list of users is presented in Table 2 . |
| Victorian public health services | Victorian public health services are entities that provide health care or medical services funded by the Victorian Government. In this document, relevant Victorian public health services are listed in Appendix A: List of public health services with access to CareSync Exchange as defined by the <i>Health Services Act 1988 (Vic)</i> . |

Other terms and references

Table 8 | Terms and acronyms referenced in the Privacy Management Framework

| Term | Definition |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agent Hub | Agent Hub is a user interface to the Victorian Electronic Patient Health Information Sharing System (CareSync Exchange) and is accessed through a local health service’s clinical system, for example, an electronic medical record (EMR). Users access Agent Hub through their local EMR using their EMR login credentials. Agent Hub presents statewide patient health information that is not in the local EMR, enabling the user to view recent information collected across the Victorian public health sector. The Portal is the alternative way of accessing CareSync Exchange (defined below). |

| Term | Definition |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Break glass | Break glass is a technical control feature on CareSync Exchange for certain categories of sensitive information. Access to information behind break glass will be restricted and not immediately available unless a clinician provides a reason to see the information. Access to the sensitive information will be monitored and audited. |
| Collecting | Collecting is the process of bringing together information in a system. In the context of CareSync Exchange, collecting is the process of gathering information from Victorian public health services to establish and maintain CareSync Exchange. There are two points of collection: <ul style="list-style-type: none"> • information that is collected in a health service system (such as an EMR) when clinicians document information about a patient • information that is collected from health service systems (such as an EMR) into CareSync Exchange. |
| Data | In this document, data refers to raw and unprocessed facts that lack content and significance. Data can take various forms like numbers, text, images and other representations. |
| Electronic medical record (EMR) | An electronic medical record (EMR) is a digital version of a patient's medical history collected by a health service when the patient receives medical care or treatment. It contains data like diagnoses, medications and test results. |
| Health information | In this document, health information refers to health data that has been processed or interpreted to make it meaningful and useful. Knowledge and opinions about a patient's physical or mental health, or disability, are examples of health information. |
| Health Sector Cyber Security Assessment | The Health Sector Cyber Security Assessment is a package of cybersecurity controls drawn from leading national and international cybersecurity organisations and frameworks like the Australian Signals Directorate's <i>Information security manual</i> and the National Institute of Standards and Technology in the United States. It is tailored to the requirements of the Victorian health sector. This tool strengthens health services' ability to detect, protect and respond to the evolving cybersecurity threat environment. Maturity levels for each control provide an indication of an organisation's cybersecurity maturity. |
| Indigenous Data Sovereignty | Indigenous Data Sovereignty refers to the right of Aboriginal people to exercise ownership over Indigenous Data. Indigenous Data refers to information or knowledge, in any format or medium, which is about and may affect Aboriginal people both collectively and individually. This definition was established by Mayam nairi Wingara , see <maiamnayriwingara.org/definitions>. Ownership of data can be expressed through the creation, collection, access, analysis, interpretation, management, sharing and reuse of Indigenous Data. |
| Indigenous Data Governance | Indigenous Data Governance refers to the right of Aboriginal people to autonomously decide what, how and why Indigenous Data is collected, accessed and used. It ensures that data on or about Aboriginal people reflects their priorities, values, cultures, worldviews and diversity. |

| Term | Definition |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Information security manual</i> | The Information security manual is a resource for government agencies and organisations to secure their information and communication technology systems, created by the Australian Cyber Security Centre. It outlines a framework for protecting sensitive information and critical infrastructure from various cyber threats and risks. |
| Mental health and wellbeing services | As defined in the <i>Mental Health and Wellbeing Act 2022 (Vic)</i> , mental health and wellbeing services are professional services that: <ul style="list-style-type: none"> • improve or support a person’s mental health or wellbeing • assess or provide treatment or support to a person with mental illness or psychological distress • provide care or support to a person who is a family member, carer or supporter of a person with mental illness or psychological distress. |
| My Health Record | My Health Record is a national system that stores key health information for Australians. My Health Record is managed by the Australian Digital Health Agency and allows healthcare providers to access a patient’s medical history, medications, and test results. Consumers can access and control who can view their record. Consumers can also opt-out of having a record. The new CareSync Exchange complements My Health Record, offering a more localised and complete view for Victorian public health services. |
| Patient visit | A patient visit is an interaction between a patient and a health service for the purpose of diagnosis or treatment of an illness or injury. This includes an inpatient, outpatient or emergency department visit to a health service. The technical term for this is <i>encounter</i> . |
| Portal | Portal is a user interface gateway to the Health Information Sharing System, providing users with login access through a restricted network. Agent Hub is the alternative way of accessing CareSync Exchange (defined above). |
| Primary care | Primary care is generally the first service people go to for health care outside of a hospital or specialist setting. It is delivered by a range of clinicians including general practitioners. Primary care includes diagnosis and treatment of health conditions and long-term care. It also covers health promotion and prevention services. Unless the primary care is provided by a Victorian public health service (see definition in Table 7), the clinician will not be able to access CareSync Exchange. |
| Privacy Management Framework (PMF) | A privacy management framework is a document that offers a formal set of guidelines and rules to help individuals and organisations to maintain strong privacy practices. This document is the Privacy Management Framework (PMF) for CareSync Exchange, established by and operating in accordance with a new Part 6C of the Health Services Act. |

| Term | Definition |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Protective security policy framework</i> | The Protective security policy framework is the Commonwealth Government’s comprehensive framework for protecting assets, people and information against security threats, including cyber attacks, espionage and terrorism. It aims to improve the security of government agencies. |
| CareSync Exchange | CareSync Exchange refers to the Victorian Electronic Patient Health Information Sharing System to which this PMF relates. It has been established by the <i>Health Legislation Amendment (Information Sharing) Act 2023 (Vic)</i> , which amends the Health Services Act. CareSync Exchange is one component of a broader health information sharing system and only contains general health records. |
| Unauthorised access | Unauthorised access refers to the act of gaining entry to CareSync Exchange without proper authorisation. This could occur: <ul style="list-style-type: none"> • When an authorised user intentionally accesses unauthorised information, such as by accessing confidential records for curiosity or malicious intent. • When an individual inadvertently accesses CareSync Exchange as a result of lapses in security protocols, such as an unlocked computer displaying confidential records. • When an unauthorised individual deliberately breaches security measures to gain access to sensitive information on CareSync Exchange, as seen in the actions of malicious actors (such as hackers). |
| User activity log | User activity logs document all use of CareSync Exchange. The department is responsible for ensuring CareSync Exchange has this capability. |
| User activity report | The user activity report is generated by health services upon consumer request. This report includes the role of the user who accessed the record, the location (which health service) and timestamp. |

Applicable legislation

Table 9 | Applicable legislation in the Privacy Management Framework

| Term | Definition |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Freedom of Information Act 1982 (Vic) | A law that provides members of the public the right to request access to government documents and information. It aims to promote transparency and accountability in government operations. |
| Health Legislation Amendment (Information Sharing) Act 2023 (Vic) | A law that adds Part 6C to the <i>Health Services Act 1988 (Vic)</i> and allows for the establishment of the Victorian Electronic Patient Health Information Sharing System (CareSync Exchange) and the PMF. |
| Health Records Act 2001 (Vic) | A law that governs the collection, use, and disclosure of health information in Victoria. It was consequentially amended in 2023 to allow for the establishment of CareSync Exchange. |

| Term | Definition |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>The Act sets out the Health Privacy Principles, which the Department of Health and Victorian public health services must follow to ensure the confidentiality and security of information collected or held by CareSync Exchange.</p> <p>It was amended by the <i>Health Legislation Amendment (Information Sharing) Act 2023 (Vic)</i> to allow for the establishment of CareSync Exchange.</p> |
| <p>Health Services Act 1988 (Vic)</p> | <p>A law that provides the legal framework for regulating and overseeing health services in Victoria.</p> <p>It was amended in 2023 to include Part 6C which allows for the establishment of CareSync Exchange.</p> |
| <p>Mental Health and Wellbeing Act 2023 (Vic)</p> | <p>The Act supports changes to achieve the highest possible standard of mental health and wellbeing for all Victorians. It replaces the <i>Mental Health Act 2014 (Vic)</i> and is a key recommendation of the <i>Royal Commission into Victoria’s Mental Health System</i>.</p> |
| <p>Privacy and Data Protection Act 2014 (Vic)</p> | <p>This Act places obligations on Victorian public sector organisations (and certain contracted service providers) to handle personal information in accordance with 10 information privacy principles. It does not apply to health information, however, it does outline requirements for the Victorian Protective Data Security Standards.</p> |
| <p>Public Records Act 1973 (Vic)</p> | <p>This Act governs the management and disposal of public records created by Victorian Government agencies. The two types of data on CareSync Exchange – health information and user activity logs – are retained or destroyed consistent with the Act.</p> |
| <p>Victorian Protective Data Security Standards</p> | <p>The Victorian Protective Data Security Standards establish 12 high-level mandatory requirements to ensure the protection of sensitive and personal information held by Victorian Government agencies.</p> |

Appendices

Appendix A: List of public health services with access to CareSync Exchange

The initial launch of CareSync Exchange includes nine major Victorian public hospitals: Alfred Health, Austin Health, Eastern Health, Monash Health, Northern Health, Peter MacCallum Cancer Centre, The Royal Children's Hospital, the Royal Melbourne Hospital and the Royal Women's Hospital.

CareSync Exchange will be progressively rolled out to other health services specified in the *Health Services Act 1998* (Vic), including:

- ambulance services
- metropolitan hospitals listed in Schedule 3
- multipurpose services
- public health services listed in Schedule 5
- public hospitals listed in Schedule 1
- public hospitals listed in Schedule 2
- registered community health centres
- residential care services within the meaning of the *Aged Care Act 1997* (Vic), including state-funded residential aged care services
- the Victorian Institute of Forensic Mental Health (known as Forensicare)
- the Victorian Collaborative Centre for Mental Health and Wellbeing
- a prescribed class of entity that provides health services.

It does not include:

- dental clinics
- drug and alcohol rehabilitation services
- general practice
- mental health services
- pharmacies
- private health services
- research institutions
- supported residential services within the meaning of the *Supported Residential Services (Private Proprietors) Act 2010* (Vic).

Please visit the [department's website](https://go.vic.gov.au/483vAUA) <<https://go.vic.gov.au/483vAUA>> for the latest updates on the rollout of CareSync Exchange.

Appendix B: Information collected by CareSync Exchange

CareSync Exchange collects information from systems used by health services, for example, EMRs.

Table 10 below outlines the types of information that are collected by CareSync Exchange.

Information groups are listed in the table in the sequence in which they are presented within CareSync Exchange. Some of the information groups will be progressively rolled out.

Please visit the [department's website](https://go.vic.gov.au/483vAUA) <<https://go.vic.gov.au/483vAUA>> for the latest updates on the rollout of CareSync Exchange.

Table 10 | Information elements within CareSync Exchange

| Information group | Information element | Description |
|-------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Patient | Confidentiality | A flag to indicate information is confidential |
| | Patient's Name | The first, middle and last name of the patient |
| | Date of Birth | The patient's date of birth |
| | Gender | The gender of the patient |
| | Patient Identifier – Primary | The patient's unique record number (URN) at the health service where the patient record exists |
| | Patient Identifiers – Secondary | Secondary identifiers include: <ul style="list-style-type: none"> a health services' enterprise master patient index identifier, to assist in linking a shared patient record across health services a patient's individual health identifier (IHI) – this is required for a launch of My Health Record from CareSync Exchange a patient's Medicare or Department of Veterans' Affairs veteran card number, for the purpose of assisting in patient demographic searches. |
| | Contact Information – Patient | The patient's address(es), phone number(s) and email contact information |
| | Contact Information – Next of Kin | The name and phone number(s) of the patient's next of kin, and their relationship to the patient |
| | Preferred Language | The preferred language of the patient |
| | Country of Birth | The patient's country of birth supports culturally responsive and person-centred care |
| | Indigenous Status | The patient's Indigenous status |
| | Care Providers – General Practitioner | The name of the patient's primary care provider |
| | Deceased Indicator and Date | The deceased indicator and deceased date |
| | Protected Patients Indicator | This indicator is used to cover a range of patient sensitivity scenarios, for example, family violence. |
| Encounter | Confidentiality | A flag to indicate that information is confidential |
| | Patient Class | The type of patient episode (inpatient, outpatient, emergency and so on) |
| | Encounter ID | The identification number of the encounter |
| | Encounter Organisation | The organisation / health service where the encounter took place |
| | Facility/Campus | The facility/campus where the patient was admitted |
| | Service Type | The service line / clinical unit type provided by this unit |

| Information group | Information element | Description |
|-------------------------|-------------------------|---------------------------------------------------------------------------------------------------|
| | Admission Date | The encounter start date and time |
| | Length Of Stay | The encounter duration in days |
| | Provider Start Date | The date when the clinician started treating the patient in this encounter |
| | Attending Provider | The name of the attending clinician |
| | Provider Type | The clinician type for this encounter (for example, attending or discharging) |
| | Reason for Visit | The reason why the patient was admitted |
| | Arrived From | The type of place or organisation responsible for the patient immediately prior to this encounter |
| | Discharged To | The destination of the patient after discharge from the hospital |
| | Discharge Date | The encounter end date and time |
| | Referred Facility | The organisation or health service from which the patient was referred |
| | Referred Unit | The name of the unit in the referred facility where the patient was last treated |
| | Chief complaint | The chief complaint of the patient from the patient's perspective on their condition |
| Alert or problem | Alert or Problem Name | The alert or problem name |
| | Type | The type of alert or problem |
| | Uncertainty | The uncertainty code |
| | Onset Date | The alert or problem documented date |
| | Status | The alert or problem status |
| | Severity | High or low |
| | Code | The baseline ID code |
| | Facility | The name of the hospital the patient was admitted to |
| | Documented By | The name of the person who documented the problem |
| | Source | The data source system |
| | Comments | Comments about the alert or problem |
| Diagnosis | Confidentiality | A flag to indicate that the information is confidential |
| | Diagnosis Name | The diagnosis name |
| | Diagnosis Code | The diagnosis code |
| | Diagnosis Coding System | The coding system/terminology of the diagnosis (for example, ICD10) |
| | Type | The diagnosis type |
| | Priority | The diagnosis priority (for example, primary or secondary diagnosis) |
| | Onset Date | The diagnosis start date |
| | Facility/Campus | The facility where the diagnosis was documented |
| | Documented By | The provider that documented the diagnosis |
| | Comments | Comments |
| Allergies | Allergy Name | The name of the allergy |
| | Onset Date | The date the allergy first presented |

| Information group | Information element | Description |
|-------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Status | The status of the allergy, for example, active or inactive |
| | Allergy Severity | The severity of the allergy |
| | Allergy Type | The type of allergy (for example, with a propensity to adverse reactions to drugs) |
| | Facility | The facility where the allergy was reported |
| | Documented By | The name of the person who documented the allergy |
| | Source | System from which information was received |
| | Reaction (Severity) | A list of reactions with their severity in parentheses. When the reaction is 'High' or 'Very high' severity, the reaction is displayed with red, bold and underlined text |
| | Comments | A free-text description of the allergy and any related comments |
| Medication | Medication Name | The name of the medication |
| | Form | The form of the medication, for example, powder spray |
| | Activity Type | The mode code: <ul style="list-style-type: none"> • Administered • Prescribed • Dispensed • Reported • Recommended |
| | Date | The date when the medication activity occurred |
| | Status | Calculated status: <ul style="list-style-type: none"> • Active • Inactive • Cancelled • Unspecified The Status field displays the Status code designation according to the Calculated Status. In addition, it displays the Status subdomain designation, if it exists. |
| | SIG | A clinician's directions to the patient regarding consumption of the prescription. When the SIG value is NULL, three separate fields are displayed on the Details pane. <ul style="list-style-type: none"> • Dose • Route • Frequency |
| | PRN | Whether the medication can be taken as needed, and the reason why |
| | Dispense As Written | An instruction to dispense exactly as prescribed. Possible values are: <ul style="list-style-type: none"> • Yes • No • Unknown |
| | Duration | The length of time the medication is to be taken |
| | Refill | The number of times the medication can be replenished before a new prescription is required |
| | Dispense | The total amount of medication to be administered |

| Information group | Information element | Description |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| | Facility | The facility where the prescription and dispensation took place |
| | Entered By | The name of the person responsible for writing the prescription |
| | Source | The source of the data displayed in the tooltip |
| | Comments | A free-text description of the medication prescription |
| Labs | Confidentiality | A flag to indicate information is confidential |
| | Diagnostic Service Type | The type of laboratory test (for example, blood gases) |
| | Laboratory Test | The name and code of the test |
| | Specimen Type | The specimen used for test |
| | Specimen Site | The site of the specimen collected |
| | Specimen Received Date | A date when the specimen is received at the lab |
| | Collection Date | A date of a lab event being undertaken |
| | Organisation | The organisation / health service that performed the collection |
| | Collection Location (Unit) | The unit that performed the collection |
| | Ordered By | The clinician who ordered the lab |
| | Status | The lab result status code |
| | Result Date and Time | The date of test results |
| | Result Value and Unit of Measurement | The Result Value and Unit of Measurement |
| | Abnormal Indication | An indication for abnormal results |
| | Interpretation | The interpretation code of the result |
| | Range | A range value defined for the result by the source |
| | Responsible Observer / Technician | The technician performing the test |
| | Comments | Result comments |
| Pathology Report | A pathology report is likely to include: <ul style="list-style-type: none"> the patient’s name, identifier and contact details provider details, including the requester and performer findings and results a commentary, including diagnoses | |
| Pathology | Confidentiality | A flag to indicate information is confidential |
| | Diagnostic Service Type | The type of pathology test (for example, anatomical pathology) |
| | Pathology Test | The name and code of the test |
| | Ordered By | The name of the person who ordered the test |
| | Ordering Facility | The facility/campus where the test was ordered |
| | Collection Comments | The reason the test was ordered |
| | Performing Facility | The laboratory that performs the test |
| | Specimen | The specimen on which the test is performed |
| | Specimen Site | The site where the specimen was collected |
| | Specimen Received Date | The date and time the specimen was taken/received |

| Information group | Information element | Description |
|---------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Collection Date | The date that the specimen was collected |
| | Result Date | A date when the result is provided |
| | Status | The lab event status |
| | Diagnoses | Diagnoses done for the pathology test |
| | Diagnoses Type | The type of the diagnoses |
| | Conclusions | Conclusions entered for the pathology test |
| | Result code / Test code | The pathology test results |
| | Result Date | The date when the test was resultted |
| | Pathology Finding Code | The pathology finding code, name and coding system |
| | Pathology Finding | The pathology finding description |
| | Interpretation | The interpretation code of the pathology result |
| | Responsible Observer / Technician | The name of the technician performing the test |
| | Pathology Report | A pathology report is likely to include: <ul style="list-style-type: none"> the patient’s name, identifier and contact details provider details, including the requester, and performer findings and results commentary, including diagnoses |
| | Radiology | Study |
| Date and Time | | The study date and time |
| Modality | | The type of imaging study |
| Status | | The status of the image study (active, cancelled and so on) |
| Ordered By | | The name of the person who ordered the image |
| Ordering Facility | | The name of the facility that ordered the study |
| Performing Facility | | The name of the facility that conducted the study |
| Source | | The data source system |
| Clinical Questions | | Image request comments (a free-text field) |
| Imaging Links | | A list of one or more picture archiving and communication links |
| Procedures | Procedure Name | The name of the procedure |
| | Type | The type of procedure |
| | Date | The procedure date and time |
| | Status | The status of the procedure |
| | Performed By | Person who performed the procedure |
| | Code | The procedure code and coding system (baseline) |
| | Source Code | The code as received in the message |
| | Priority | The priority value |
| | Facility | The name of the facility where the procedure was documented |

| Information group | Information element | Description |
|-------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Performing Unit | The name of the unit where the procedure was performed |
| | Service | The functional type of the place or site where the procedure was performed |
| | Source | The source system that sent the procedure |
| Documents | Confidentiality | A flag to indicate that information is confidential |
| | Document Type | The type of document |
| | Title | The title of the document |
| | Facility | The facility/campus that produced the document |
| | Author | The author of the document |
| | Creation Date | The date the document was created |
| | Update Date | The date the document was updated |
| | Status | The completion status of the document |
| | Discharge Summary Event Summary Specialist Letter Pathology Reports Radiology Reports | Documents can include: <ul style="list-style-type: none"> • patient information • provider information and the name of the treating facility • pathology tests • problems and diagnoses • diagnostic investigations • procedures performed • clinical overview(s) • current and ceased medications on discharge / medications and reviews • allergies and adverse reactions • recommendations. |

Appendix C: The consultation process to inform the Privacy Management Framework

This Privacy Management Framework (PMF) for CareSync Exchange was developed through four rounds of consultations with consumers, clinicians, advisory groups and advocacy organisations. They commenced in August 2023 and were completed in February 2024.

1. In the first stage, health consumers, clinicians and advocacy representatives participated in focus groups and interviews to understand health consumers' privacy concerns and identify data themes that may raise additional, specific privacy concerns.
2. The second stage of consultations comprised workshops with consumer and clinician participants to identify solutions to address health consumers' privacy concerns identified in the first stage. Solutions were explored using fictional patient scenarios and developed through discussion of technical controls and measures in the PMF.
3. Solutions to privacy concerns were validated in a third round of consultations with the following groups to ensure that they were feasible and appropriate:
 - a. advisory groups (Clinical Design, Technical Design, Consumer Reference Group)
 - b. advocacy organisations
 - c. legal, technical, policy and design roles within the department,
 - d. health services and vendors .
4. In the fourth stage, the PMF underwent a public consultation process to take feedback from government agencies and regulators, health services, clinical employee groups, a privacy advocacy group and organisations and peak bodies who could provide insight into categories of sensitive information.

Index

- Aboriginal and Torres Strait Islander people
 - acknowledgement of 2
 - consultation with 42
 - data sovereignty of 10, 47
 - information on status of 24, 30
- aged care 10, 51
- Agent Hub **10 (Figure 1)**, 19, 22, 37, 46
- Ahpra (Australian Health Practitioner Regulation Agency) **18 (Figure 6)**, 29, 45
- alcohol and other drugs 24, 30, 51
- alerts 23
- Alfred Health 51
- allergies 23
- allied health professionals 9, 20, 45
- ambulance services 9, 19, 51
- audiologists 45
- auditing 6, 8, 19, 20–1, 25–7, 35, 38, **40 (Figure 10)**
- Auditor-General 41
- Austin Health 51
- Australian charter of healthcare rights* 29
- Australian Commission on Safety and Quality in Health Care 45
- Australian Digital Health Agency 10, 48
- Australian Health Practitioner Regulation Agency. *See* Ahpra
- Australian Signals Directorate 34n6, 47
- authentication and authorisation 34

- 'break glass' (additional security protection)
 - 24–6, **26 (Figure 7)**, 29, 35–6
 - definition of 25, 47
 - monitoring of **36 (Figure 9)**
 - reporting on 37

- CareSync Exchange (Victorian Electronic Patient Health Information Sharing System) 23
 - access to 19–20, 51
 - application of **11 (Figure 2)**
 - benefits of **12 (Figure 3)**
 - consultation about 43, 58
 - and consumer rights **14 (Figure 4)**, 15–18, **40 (Figure 10)**
 - definition of 5, 49
 - description of 9, 52–7
 - establishment of 7, 8, 49, 58
 - exclusions from **12 (Figure 3)**, 23, 27, 51 (*see also* 'break glass')
 - governance of 13, 25, 41–2
 - implementation of 9, 19, 41, 51
 - improvement and review of 43–4
 - information collected by 52–7
 - and My Health Record 10, 48
 - permitted and non-permitted uses of 19
 - rollout of 7, 15, 41, 52
 - supporting materials for 41–2
 - users of 46
- children and young people in out-of-home care 24, 26, 30, 42
- chronic and complex conditions 24, 30
- clinicians 45
 - access to CareSync Exchange by 20, 26
 - definition of 9
 - training for 28
- cognitive bias 28, 29
- communication
 - and collaboration **40 (Figure 10)**
 - resources for 13, 41–2
- complaints and concerns 13, **14 (Figure 4)**, 15, 18, **18 (Figure 6)**, 37, 38, **40 (Figure 10)**
- compliance 28, 41, 43–4
- consent 9
- consultation 43, 58
 - between clinicians 39
- consumer notification **40 (Figure 10)**
- consumer rights **14 (Figure 4)**, 15–18, **40 (Figure 10)**
- continuity of care 9, **12 (Figure 3)**, 39
- criminal offences 39
- cultural safety 30, 31
- cyber threats **14 (Figure 4)**, 47, 49
- cybersecurity 33–4

- data
 - analysis of 44
 - breaches of 36–7, 39, **40 (Figure 10)**, 43 (*see also* incident management)
 - definition of 47
 - management of 21–2, 50
 - preventing loss of 22, 33–4
 - retention or destruction of 50
 - storage and security of 33–4
- date of birth 10, 17, 20–2, 23
- decision making, timeliness of 6, 7, **12 (Figure 3)**
- definitions. *See* glossary on pages 45–50
- delegations 41
- dentistry and dental clinics 45
- Department of Health
 - access to CareSync Exchange by 21–2
 - and break-glass events 35–6
 - and governance 41
 - and monitoring 35–8

- and policies and procedures **40 (Figure 10)**
- and reporting 38
- and review of PMF 43
- and security 33–4, **40 (Figure 10)**
- and training 28
- and user activity logs 49
- disability 24, 30
- discharge summaries 23, 25, 31
- discrimination 29
- doctors 9, 20, 45
- domestic violence. See family violence
- drugs and alcohol 24, 30, 51
- duplication, avoidance of **12 (Figure 3)**

- Eastern Health 51
- electronic medical record. See EMR
- emergency department letters 23
- emergency situations / care **36 (Figure 9)**, 46, 48
- EMR (electronic medical record)
 - definition of 5, 8, 47
 - and the PMF 13
- encryption 34
- escalation of complaints or issues **18 (Figure 6)**, 28, 29, 36
- expert panel 6, 43–4

- family violence 24, 25–6, **26 (Figure 7)**, 30, 42
- feedback 6, 37, 38, 58
- file servers 33, 34
- First Nations Australians. See Aboriginal and Torres Strait Islander people
- Freedom of Information Act 1982* (Vic) 16, 49
- freedom of information requests 16, **16 (Figure 5)**, 49

- gender and identity 24, 30
- general practice and practitioners 9, 10, **12 (Figure 3)**, 19, 45, 48, 51
- genetic conditions 24, 30–1
- glossary, purpose of 5
- governance 41–2

- HCC. See Health Complaints Commissioner
- Health Complaints Commissioner (HCC) 18, **18 (Figure 6)**, 37, 40, 45
- health consumer, definition of 9, 45
- health information, definition of 47
- Health Information Sharing Legislation Reform 15, 18
- Health Information Sharing Management Committee 6, 13, **40 (Figure 10)**, 41, 43

- Health Legislation Amendment (Information Sharing) Act 2023* (Vic) 5, 6, 13, 24, 35, 41, 49–50
- Health Privacy Principles 8, 39, 50
- Health Records Act 2001* (Vic) 5, 6, 8, 15, 29, 39, 49
- Health Sector Cyber Security Assessment 34, 47
- health services
 - administration of 8
 - definition of 8, 9
 - executives of 41
 - number of 8
- Health Services Act 1988* (Vic) 5, 8, 15, 41, 48–50
- hospital transfers 9, 10, 39
- human rights 44

- identity
 - protection of **14 (Figure 4)**, 17, 20–2
 - recording of 23, 30
- inaccuracies, correction of **14 (Figure 4)**, 17, 20
- incident management 20–2, 37, 39, **40 (Figure 10)**, 43.
 - See also data: breaches of
- Indigenous Australians. See Aboriginal and Torres Strait Islander people
- Indigenous Data Sovereignty and Governance 10, 47
- infectious diseases 24, 31
- information
 - collection of **10 (Figure 1)**, 23, 47
 - consumer access to 15, **16 (Figure 5)**
 - management of 24–7
 - misuse of 13, 24
 - security of 33–4
 - sensitivity of 13, **14 (Figure 4)**, 23, 24, 29–30
 - types collected 23, 52–7
- Information Privacy Principles 29, 39, 50
- Information security manual* (Cwth) 34n5, 47, 48
- information sharing
 - consent for 9
 - process for **11 (Figure 2)**
 - usefulness of 7
- investigations 17, 21, **40 (Figure 10)**, 44.
 - See also Ahpra

- Keeper of Public Records 27, 46

- lab reports 23
- legislation 49–50
- logins 19, 22, 37, 46, 48

- malicious acts and actors 33, 39, 49
- matching of records 10, 17, 19, 20–2
- Mayam nairi Wingara* 47
- medical students 20
- medications 5, 23, 25
- mental health 24–5, 31, 48, 51
- Mental Health and Wellbeing Act 2022 (Vic)* 24, 25, 48, 50
- metrics 37
- midwives and midwifery 20, 45
- Minister for Health 6, 8, 41, 43–4
- misdiagnosis 24, 30
- Monash Health 51
- monitoring and security measures 6, 21, 33–4, 35–8
- multicultural communities 24, 31
- My Health Record 9, 10, 48

- National agreement on closing the gap* 10
- National Safety and Quality Health Service Standards 28
- near misses 39
- neurodivergence 24, 31
- Northern Health 51
- nurses 9, 20, 45

- Office of the Victorian Information Complaints Commissioner (OVIC) 18, **40 (Figure 10)**, 46
- orthotists/prosthetists 45
- out-of-home care 24, 26, 30, 42
- outpatient letters 23

- paramedics 9, 20, 45
- pathology reports 23
- patient visits 23, 48
- patient-centred care 6, 28, 29
- patients
 - definition of 9, 46
- penalties 6, 39
- performance metrics 37
- Peter MacCallum Cancer Centre 51
- pharmacies 19, 45, 51
- physical and ergonomic controls 22
- physiotherapists 9, 20, 45
- PMF (Privacy Management Framework)
 - application of 7
 - definition of 5, 48
 - exclusions from 13
 - improvement and review of 43–4
 - purpose of 6, 13
- policies, procedures and guidelines 13, 27, **40 (Figure 10)**, 42

- Portal **10 (Figure 1)**, 37, 46, 48
 - security of 34, 36
 - users of 21–2
- primary care 10, 48. *See also* general practice and practitioners
- printing, copying or emailing health information 22, 33
- privacy
 - breaches of 17, 20–1, 24
 - importance of 6, 7
 - principles of 39, 50
 - safeguards for 13
- Privacy and Data Protection Act 2014 (Vic)* 39, 50
- Privacy Management Framework. *See* PMF
- private hospitals and providers 9, **12 (Figure 3)**, 19, 45, 51
- Protective security policy framework (Cwth)* 34n5, 49
- pseudonyms **14 (Figure 4)**, 17
- public health service, definition of 46
- public hospitals 9, 19, 51
- public records 27, 46, 50
- Public Records Act 1973 (Vic)* 27, 50
- public-profile individuals 24, 26, 31, 39

- radiographers 45
- radiology reports 23
- recommendations for improvement 37, 43–4
- records, matching of 10, 17, 19, 20–2
- referral letters 9
- reporting requirements 35–8
 - annual 6, 37
 - public-facing 38
- reproductive health 24, 31
- research 19, 51
- residential care and services 51
- rights for consumers **14 (Figure 4)**
- rollout. *See* CareSync Exchange: rollout of Royal Children’s Hospital 51
- Royal Commission into Victoria’s Mental Health System 25, 50
- Royal Melbourne Hospital 51
- Royal Women’s Hospital 51

- Secretary of Department of Health 6, 7, 13, 20, 41, 43
- security testing 34
- senior responsible officers (SRO) 20, 37, 46
 - and ‘break glass’ events 35, **36 (Figure 9)**
- sexual and reproductive health 24, 31
- sexual assault or harm 24, 26, 31
- social workers 9, 20, 45
- SRO. *See* senior responsible officers
- stigma 13, 24, 29, 30–1

- students 20
- supported residential services 51
- Supported Residential Services (Private Proprietors) Act 2010 (Vic)* 51

- Targeting Zero review (2016) 8
- Thomas, Mary-Anne 6. *See also* Minister for Health
- timeout feature 22
- training 13, 28–32, 43
- transfer of patients 39
- transparency 7, 15, 49

- unauthorised access **14 (Figure 4)**, 17, 49
 - detection of 36
 - reporting on 37
- unusual activity 37
- updates and customisations 37, 43, 51, 52
- user access reviews 34
- user activity reports and logs **16 (Figure 5)**, 17, **26 (Figure 7)**, 27, 35, 46, 49
 - retention or destruction of 50

- Victorian Aboriginal affairs framework 2018–2023* 10
- Victorian Auditor-General 41
- Victorian Electronic Patient Health Information Sharing System. *See* CareSync Exchange
- Victorian Health Incident Management System 37
- Victorian Protective Data Security Standards 34, 50
- Victoria’s cyber strategy 2021* 34n5
- violence. *See* family violence
- vulnerable people 25, 42

- Wallace, Euan M 7. *See also* Secretary of Department of Health