Personally controlled electronic health record system – participation:
Frequently asked questions
This frequently asked questions document provides guidance about the participation agreement for healthcare organisations participating in the personally controlled electronic health (eHealth) record system.

**Purpose and interpretation of the participation agreement**

Why do healthcare organisations need to enter into a participation agreement to use the eHealth record system?

Healthcare organisations must enter into a participation agreement with the System Operator in order to register to participate in the eHealth record system. The System Operator – the Secretary of the Department of Health and Ageing – is responsible for establishing and operating the eHealth record system.

The terms of the participation agreement include rights and obligations of both parties the System Operator and the healthcare organisation. Including these terms in a participation agreement instead of legislation provides flexibility for the agreement to evolve over time to reflect the changing needs of the eHealth record system and healthcare organisations.

The participation agreement also provides for information to be uploaded to the eHealth record system (and to individuals’ eHealth record) and shared with authorised users without breaching intellectual property rights.

Why do healthcare organisations need to appoint an authorised contact person for the participation agreement?

Healthcare organisations need to appoint an employee to be their authorised contact for administrative purposes. For example, if the System Operator needs to contact an organisation about the terms of the agreement, the System Operator will directly contact their nominated authorised contact person.

Who can be an authorised contact person?

It is recommended that the authorised contact person be the person assigned as the responsible officer for the purposes of the Healthcare Identifiers Service.

If disagreements arise between the System Operator and a healthcare organisation, what mechanisms are available for resolution?

Neither the System Operator nor the healthcare organisation can begin legal proceedings until it has taken certain steps (outlined in clause 10 of the participation agreement) which include notifying the other party of the dispute (in writing) and participating in some form of mediation.

If a disagreement arises between a healthcare organisation and an individual healthcare professional regarding obligations under the participation agreement, what mechanisms are available for resolution?

Any disagreement must be managed between the healthcare organisation and healthcare professional concerned.
Using the eHealth record system

How do I, as a healthcare organisation, participate in the eHealth record system?

To participate in the eHealth record system, your healthcare organisation must:

- have a Healthcare Provider Identifier—Organisation, which is also known as an HPI-O. An HPI-O is allocated by the Healthcare Identifiers Service (operated by Medicare) on application by an organisation;
- have an eHealth record system compliant digital credentials which can be obtained from Medicare;
- be registered with the System Operator. Your organisation must apply to the System Operator who will determine if your organisation meets all participation requirements;
- not discriminate against a consumer because they do not have an eHealth record or because of their access control settings;
- tell the System Operator within 14 days if your organisation ceases to be eligible to be registered (e.g. your organisation’s software is no longer eHealth record system conformant);
- tell the System Operator if you know or suspect there is an error in a record your organisation has downloaded or accessed, or that the security of the system has been compromised by one of your employees (including contractors);
- tell the System Operator when there is any change to the name or details of your organisation’s authorised contact person;
- give the System Operator reasonable assistance in relation to any inquiry, investigation or complaint regarding the eHealth record system;
- develop, maintain, enforce and communicate to staff written policies relevant to the eHealth record system to ensure that use of the system is secure, responsible and accountable. The policies your organisation developed need to deal with a range of matters, including authorising persons within the organisation to access the system, training, and physical protection of IT system;
- provide your organisation’s policies to the System Operator upon request;
- ensure your IT system uses conformant software when connecting to, and interacting with the eHealth record system; and
- comply with the eHealth record system rules that apply to healthcare organisations.

What is an individual healthcare provider?

An individual healthcare provider is someone who provides, or will provide, healthcare or is someone registered by a registration authority as a member of a particular health profession.

For the purposes of the supporting material the term individual healthcare provider is referred to herein as a healthcare professional.

How do healthcare professionals access the eHealth record system?

Once a healthcare organisation has been registered in the eHealth record system, healthcare professionals (and other staff members whose duties require them to access the eHealth record system, such as a practice manager) who have been authorised to access the system on behalf of that organisation will be able to do so. Authorised healthcare professionals will be able to access, and in some circumstances upload information to, their patient’s eHealth record.

Authorised healthcare professionals will be able to access the system via either a conformant clinical information system with a secure individual logon, or via the provider portal (read only) using an individual PCEHR compliant digital credential.
What does a healthcare professional need to do to participate?

For a healthcare professional to access the eHealth record system via a conformant clinical information system, the healthcare organisation they are employed by will undertake the work to establish access. Individual healthcare professionals will be authorised by their organisations, may undergo training, and will access the eHealth record system using their organisation’s clinical information systems.

For a healthcare professional to access the eHealth record system via the provider portal, they will need to obtain from Medicare an individual eHealth record system compliant digital credential. This digital credential will authenticate the healthcare professional’s identity each time they access the provider portal. To obtain an individual eHealth record system compliant digital credential the healthcare provider must first have been assigned a Healthcare Provider Identifier – Individual (HPI-I) number by the Healthcare Identifiers Service. In addition, the healthcare professional’s organisation will need to inform the System Operator that the healthcare provider has been authorised by the organisation to access the provider portal via or on behalf of the organisation.

To register for an HPI-I, or to find out what your HPI-I is, and to obtain an individual eHealth record system compliant digital credential, please go to the HI Service page on the Medicare Australia website and download the appropriate application forms.

If you are a sole practitioner in your own organisation, you will need to register your organisation, and if accessing the provider portal, notify the System Operator that you have been authorised by your organisation.

For more information and training on how to use the eHealth record system, visit www.ehealth.gov.au and follow the link to the Learning Centre or call the helpline on 1800 723 471.

How is the system protected?

The eHealth record system is protected by a combination of regulatory and technical mechanisms, and:

• provides an information communication technology system including firewalls, gateways and portals to ensure only authorised users can access the system;
• stores data in transit in line with Australian Government standards;
• ensures data stored in the eHealth record is encrypted to the same Australian Government standards;
• uses software currently used by a wide range of financial institutions to detect and prevent fraudulent activities. This is closely monitored and supported by systemic and manual compliance checks;
• ensures the integrity of information transmitted and stored by providing digitally signed clinical documents;
• prevents changes to clinical documents or records once they are uploaded to an eHealth record – this means that healthcare professionals and consumers can only view information in the eHealth record. Healthcare professionals may choose to upload replacement documents and consumers may choose to effectively remove documents;
• establishes an audit trail for consumers to check when their eHealth record was accessed and by whom – this is also supported by eHealth helpline – 1800 723 471;
• detects, analyses and reports inappropriate access and enables the overall improvement of security systems through transaction logging capabilities; and
• ensures ongoing education for users to understand risks and be able to mitigate them, increasing the safety of their records. Education and risk management is being dealt with through various agencies.

What information is displayed to the consumer in the audit log?

A patient’s eHealth record will have a view showing the activity history related to their record. This will show when information has been added or removed as well as the organisation that viewed their record and when. Healthcare professionals will be able to see an audit log of their own activity on the eHealth record system. The purpose of the audit log view is to provide consumers with transparency that will encourage confidence that their record has been accessed appropriately.
What happens when the system is unavailable?

The System Operator aims for a high level of system availability. However, there will be times when the system is unavailable, for example, for scheduled system maintenance periods and upgrades.

The eHealth record system does not replace existing clinical records. It is an additional tool that provides a summary of patient information entered by healthcare professionals from different healthcare organisations. This enables a single summary view of a patient’s key health information, but does not replace the primary records held by healthcare organisations about a patient, discussion with patients, or direct communications between healthcare professionals.

Service availability notifications are provided in the footer section of www.ehealth.gov.au

What are the clinical assurance and safety processes built into the system?

Only authorised healthcare professionals can enter information in the clinical record component of a patient’s eHealth record, helping to ensure clinical relevance and accuracy. However, if you or a patient finds an error in a clinical document, you or the patient must notify the healthcare organisation from which the document originated. That organisation can then upload an updated document with the correct information included.

The Department of Health and Ageing and its partners actively test and monitor the eHealth record system on an ongoing basis to detect and fix any bugs before they impact users. The National E-Health Transition Authority also assesses clinical safety of the system elements with oversight from the Australian Commission on Safety and Quality of Healthcare.

What information can the System Operator correct or remove from the eHealth record system?

The System Operator may request that a healthcare organisation correct personal information contained in an eHealth record. If the organisation refuses to do so, the System Operator may request that the organisation upload a note prepared by the consumer in relation to the personal information, to the eHealth record.

The System Operator may effectively remove documents from the system if they are defamatory or affect (or may affect) the security or integrity of the eHealth Record System.

What consent has the patient provided to organisations to upload their information? Does the healthcare professional have to give the consumer an opportunity to provide consent at each consultation?

When a consumer registers for an eHealth record, they give standing consent for healthcare organisations to upload the consumer’s information to the eHealth record system.

It is important to note that this consent is subject to the parts of the Public Health Acts of New South Wales, Queensland and the Australian Capital Territory that prohibit the disclosure of certain sensitive information (such as in connection with AIDS or HIV) without the express consent of the consumer.

You must not upload information if the patient asks you not to.

There is no requirement for you to obtain consent from your patient on each occasion prior to uploading their information to the eHealth record system. However, medical professional organisations recommend that you should advise the patient that you will upload their information and you should record this advice in your patient records.

What am I allowed to download from a patient’s eHealth record?

Healthcare organisations are authorised by the personally controlled electronic health record system legislation to collect, use and disclose health information included in a consumer’s eHealth record if it is for the purpose of providing healthcare to the consumer. Healthcare organisations are also authorised to:

• disclose health information to the consumer or the consumer’s authorised or nominated representative;
• collect, use or disclose health information for any purpose with the consent of the consumer; and
• collect, use and disclose health information for purposes relating to the provision of indemnity cover for a healthcare professional.

Any collection, use or disclosure of health information must comply with the consumer’s access control settings of their eHealth record, except in certain circumstances such as where the healthcare organisation reasonably believes that it is necessary to lessen or prevent a serious threat to an individual’s life, health or safety or a serious threat to public health or safety.

Downloading information from the eHealth record is a form of collection and use that is authorised by the personally controlled electronic health record system legislation. However, you should only download information that is necessary.

Information downloaded to your local information system, whether you’ve downloaded a report directly into your system or copied the information into your local record, will be subject to local health information and privacy laws and professional obligations, just like other health information in your system.

Healthcare organisations must take reasonable steps to ascertain whether information accessed through the eHealth record system is accurate, up to date and fit for purpose.

Healthcare organisations are not authorised to collect, use or disclose health information included in the consumer-only notes of the eHealth record.

What if I, as an organisation, am contracted to provide IT services to another healthcare organisation?

Some healthcare organisations may choose a third party service provider (known as contracted service providers) to provide IT services. In some cases those contracted service providers may be healthcare organisations.

If you are contracted to provide IT services to a healthcare organisation to enable access to the eHealth record system, you:
• must be registered to participate in the eHealth record system as a contracted service provider;
• must have entered into a contracted service provider participation agreement with the System Operator; and
• will be allocated an identifier by the System Operator.

Frequently Asked Questions about contracted service providers will be made available by the System Operator before the registration of contracted service providers commences.

**Intellectual property**

Why are intellectual property rights an issue for the eHealth Record System?

Intellectual property rights in the form of copyright may exist in a number of elements in the eHealth record system including reports, specialist letters, diagnostic images and shared health summaries.

If someone does something that is an exclusive right of the copyright owner – for example, they make a copy of a record available online – without permission of the copyright owner, there will be a breach of copyright.

The participation agreement will help reduce the risk of a copyright breach.

What kind of information does the participation agreement apply to and how far does it extend?

The participation agreement applies to all data and information uploaded to or accessible through the eHealth record system.
Through the participation agreement, a healthcare organisation grants a licence to the System Operator to use materials in the eHealth record system and to license other healthcare organisations to use material in the system.

Also through the participation agreement, the System Operator grants a licence to healthcare organisations to use materials uploaded to the eHealth Record System by other healthcare organisations.

Under this licence the information can only be used for the purposes of providing healthcare and for other eHealth record system purposes. The licence will apply in perpetuity and cannot be revoked.

If a healthcare organisation downloads materials from the eHealth record system, the licence will continue to operate for as long as the information is used for the authorised purpose. This allows, for example, downloaded records to be stored in the organisation’s clinical information system and shared within an organisation for the purpose of providing healthcare.

What assistance is provided to healthcare organisations in managing the intellectual property in information to be uploaded?

Agreements between healthcare organisations and their employees (including contractors) may state who will own the copyright in materials created by the employee.

Healthcare organisations may wish to develop arrangements to deal with the intellectual property rights of other providers or organisations. Suggested words have been developed that may be used in communications with other healthcare organisations or as a part of the record for non-participating organisations to grant a healthcare organisation permission to upload to the eHealth Record System information created by that other organisation, and to license the System Operator to use, publish and communicate that information.

The suggested words are:

“I agree to this record (or, if relevant, the attached records) being uploaded to the personally controlled electronic health (eHealth) record system. I authorise the person uploading the record(s) to grant the System Operator (within the meaning of the Personally Controlled Electronic Health Records Act 2012, a perpetual, irrevocable, royalty-free and licence-fee free, worldwide, non-exclusive licence (including a right to sub-license) to use, reproduce, copy, modify, adapt, publish and communicate the record(s) for the purpose of providing healthcare and for other purposes of the eHealth record system,

Healthcare professionals are not under any obligation to upload records to the eHealth record system and must exercise their own discretion about whether it is appropriate to upload a record.”

Healthcare organisation obligations

Will I need a legal arrangement with my organisation’s healthcare professionals to allow them access through my organisation’s system?

A formal agreement is not required by the System Operator but it may constitute good corporate governance to establish clear arrangements with the healthcare professionals employed by your organisation.

What sort of errors should healthcare professionals notify the System Operator about?

In general, non-clinical system errors such as data mismatches and transposition errors (for example, demographic errors) should be notified to the System Operator.
What are the responsibilities of healthcare organisations in relation to the quality and content of records they upload to the eHealth record system?

The eHealth record system does not change the current obligations of healthcare professionals to maintain their own detailed and accurate clinical records for consumers.

Healthcare organisations are responsible for the information that is uploaded from their clinical systems.

When uploading a record to the eHealth Record System, healthcare organisations must:

• not upload a record that contains defamatory material;
• only upload a record if it would not infringe another person’s intellectual property rights or moral rights;
• only upload shared health summaries for a patient if the summary was prepared by that patient’s the nominated healthcare professional;
• not upload a record unless it was prepared by a person who has been allocated a Healthcare Provider Identifier—Individual, also known as an HPI-I;
• only upload records on registered consumers to the eHealth record system’s National Repositories Service or a registered repository;
• not upload information about a consumer if the consumer has advised that the information is not to be uploaded;
• take reasonable steps to ensure the quality of the content of the records; and
• understand that uploading a record to the eHealth record system does not relieve your organisation of its obligations to keep clinical records about a consumer or any other obligations that may apply (for example, to communicate health information to a consumer).

What is an eHealth record protocol document?

It is recommended that a healthcare organisation put in place protocols to guide employees (including contractors) in their use of the eHealth record system.

What subjects, issues and processes should be included in an eHealth record protocol document?

The personally controlled electronic health record Rules 2012 require healthcare organisations to develop and maintain policies that reasonably address (at a minimum):

• how they will authorise employees (including contractors) to access the eHealth record system and how this list will be kept up to date;
• the training that will be provided;
• how the organisation will communicate to the System Operator the identity of each person accessing the eHealth record system using the healthcare organisation’s IT system;
• the physical and information security measures that are to be established and adhered to by the healthcare organisation and people accessing the eHealth record system via or on behalf of the healthcare organisation, including systems that employ reasonable user account management practices; and
• mitigation strategies to ensure eHealth record-related security risks can be promptly identified, acted upon and reported to the healthcare organisation’s management.

This is also a professional record keeping standards issue. An example of how healthcare organisations may address this matter is provided in the AMA Draft Guide to using the personally controlled electronic health record system (www.ama.com.au/node/7676) which provides guidance to healthcare organisations about the clinical use of the eHealth record system.
How will healthcare organisations report to the System Operator who their users are each time they access the eHealth system? Will clinical practice software do this?

Healthcare organisations will not need to maintain duplicate records to identify their users.

Compliant clinical software will identify to the System Operator each person within a healthcare organisation when they seek access to the eHealth record system. This information will be recorded in the audit logs maintained by the System Operator.

What are the obligations of a healthcare organisation to provide the System Operator with reasonable assistance in relation to any inquiry, investigation or complaint?

A healthcare organisation must provide reasonable assistance at the request of the System Operator, to help respond to an inquiry, investigation or complaint about the eHealth record system. The System Operator must give a healthcare organisation reasonable notice to provide information. Requests for assistance may, for example, relate to the setting of access flags by an organisation, the accuracy of a record, or the policies that healthcare organisations need to maintain about security and user account management.

What are access flags?

Access flags are a key component of the eHealth record system's access control mechanisms, supporting the consumers' ability to restrict the healthcare organisations that can access their eHealth record. The level of detail for this is established when a healthcare organisation sets access flags. Access flags are set by healthcare organisations in the personally controlled electronic health record system, not in local IT systems.

When a healthcare organisation is involved in the care of a consumer, and, as a result, is added to the access list for the consumer's eHealth record, access flags determine if any other associated healthcare organisations are also added to the access list for the consumer's eHealth record.

For example, if an access flag is associated with a hospital, a consumer who has chosen to restrict access to their eHealth record is able to allow access to authorised users within that particular hospital. Similarly, if an access flag is associated with a group of facilities (for example, a group of mental health institutions) then the consumer would have the capability to limit access to authorised users within that group.

In the case of a GP practice, an access flag, for example, may be associated with the practice. This enables consumers who have chosen to restrict access to their eHealth record to allow access to that practice, thereby enabling access by authorised users within that practice.

What does my organisation need to do to meet the requirements for setting access flags?

The Healthcare Identifiers Service provides a system for establishing a network hierarchy for healthcare organisations participating in the eHealth record system, consisting of a seed organisation (the head organisation of the network) and network organisations (subordinate to the seed organisation).

It is the responsibility of the seed organisation to ensure that the network hierarchy supports the setting of access flags in accordance with the principles set out in the personally controlled electronic health record Rules 2012. In general, these principles require that the setting of access flags balance reasonable consumer expectations about the sharing of information as part of providing healthcare and arrangements within the organisation for access to health information collected by the organisation.

The seed organisation must regularly review the access flags of their network hierarchy and adjust them as necessary to remain consistent with the principles. If the System Operator considers that access flags have not been set in accordance with the principles or are otherwise inappropriate, the System Operator will consult with the seed organisation and may require the organisation to change its access flags.

Guidance material will be made available to healthcare organisations to assist in setting access flags.
How does a healthcare organisation ensure it has appropriate insurance cover for liabilities that may arise for individual healthcare professionals or the organisation itself?

Healthcare organisations may need to discuss insurance cover with their indemnity provider. The participation agreement has been developed in close consultation with several major indemnity insurers.

If a provider accesses the eHealth record system and asserts they are linked to my healthcare organisation, when in fact it is not my organisation that is providing care to the patient, what protection do I, as an organisation, have?

If the individual provider is not authorised to collect, use or disclose information in the eHealth Record System, the individual, rather than the organisation, may be liable.

However, if a healthcare professional accesses a consumer’s eHealth record by mistake, they will not breach the legislation and will not be liable for a civil penalty.

What measures do I, as an organisation, need to take to ensure that the security of the eHealth record system cannot be compromised by providers in my organisation?

Healthcare organisations must comply with the technical specifications and requirements in the personally controlled electronic health record Rules. Among other things, the personally controlled electronic health record Rules require healthcare organisations to develop and maintain robust security policy on the physical and information security measures that are to be established and adhered to by the healthcare organisation and people accessing the eHealth record system via or on behalf of the healthcare organisation.

All information in this publication is correct as at August 2012.