RACGP

Royal Australian College *of* General Practitioners

Practice Incentives Program (PIP)

Digital Health Incentive resources

2016

www.racgp.org.au

Healthy Profession.
Healthy Australia.

Practice Incentives Program (PIP) Digital Health Incentive resources

Disclaimer

The information set out in this document is current at the date of first publication. It is provided for general guidance only and is intended to be an overview of the Practice Incentives Program (PIP) Digital Health Incentive requirements, as revised and effective from 1 May 2016.

This document is not and does not seek to be an exhaustive assessment of the subject matter. The contained material is tailored toward general practice, and reviews only a portion of the relevant law.

Persons implementing recommendations contained within must always exercise their own independent skill or judgement and obtain appropriate professional advice prior any decision or action concerning the PIP Digital Health Incentive. Compliance with recommendations does not guarantee discharge of any law, or duty of care owned to patients and others coming into contact with the health professional and the premises from which the health professional operates. Nor does it guarantee the satisfaction of any legal or regulatory requirement.

Accordingly The Royal Australian College of General Practitioners and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in these resources for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of any person using or relying on the information contained in this publication and whether caused by reason of any error, negligent act, omission or misrepresentation in the information.

The Royal Australian College of General Practitioners
100 Wellington Parade
East Melbourne, Victoria 3002 Australia

Tel 03 8699 0510
Fax 03 9696 7511
www.racgp.org.au

Published April 2016

We recognise the traditional custodians of the land and sea on which we work and live.

Contents

Introduction

The Practice Incentives Program (PIP) Digital Health Incentive (formerly the PIP eHealth Incentive Payment or ePIP) eligibility criteria has been revised. In addition to the existing criteria, general practices are now required to upload a specified number of shared health summaries (SHS) to the My Health Record (formerly the Personally Controlled Electronic Health Record [PCEHR]).

Because the new PIP Digital Health Incentive mandates practitioner participation in the My Health Record, significant new risks and responsibilities for the practice and its staff have been identified.

General and individual practitioners need to carefully consider these risks and responsibilities before participating in the PIP Digital Health Incentive.

The RACGP does not support the revised eligibility criteria for the PIP Digital Health Incentive, and had advocated for incentives that support data accuracy and quality. Nevertheless, the RACGP has developed a number of resources to support members to make an informed choice about participating in the PIP Digital Health Incentive and the My Health Record.

The RACGP has developed the following resources:

- General advice
- My Health Record policy template for general practices (Appendix 1)
- Access agreement template for individuals authorised to access the My Health Record (Appendix 2)
- Assisted Registration for the My Health Record template for general practices (Appendix 3)
- My Health Record checklist

In addition to these resources, the *My Health Records Act 2012*, My Health Records Rule 2016 and the Australian Privacy Principles are essential reading for practice owners and individuals responsible for the governance of their organisation.

It is important to be aware that there are significant fines for individual healthcare providers and healthcare provider organisations for inappropriate use of the My Health Record:

1. Health practitioners who breach the My Health Record privacy provisions may be fined up to $108,000 for each offence.
2. Health practitioners could incur civil fines of up to $540,000 for a single breach.
3. Criminal penalties of up to two years jail may apply for privacy abuse of the My Health Record.
4. Provisions in the Privacy Act 1988 may also have an impact on the use of the My Health Record and include penalties of up to $360,000 for individuals or up to $1.8 million for corporations for serious or repeated breaches.

The Office of the Australian Information Commissioner (OAIC) has recently audited access security controls of seven healthcare provider organisations in the My Health Record. The OAIC report outlined a number of issues that may provide useful information for practices considering involvement in the My Health Record.

The information in these resources is intended only as general guidance to assist practitioners when considering the use of My Health Record and application for the PIP Digital Health Incentive. An internal risk analysis should be conducted before deciding to participate in the My Health Record to meet the PIP Digital Health Incentive requirements. Advice should also be sought from your medical defence organisation (MDO).

General advice on the PIP Digital Health Incentive and My Health Record

Introduction

The PIP Digital Health Incentive (formerly the PIP eHealth Incentive or ePIP) eligibility criteria has been revised. In addition to the existing criteria, general practices are now required to upload a SHS to the My Health Record (formerly the Personally Controlled Electronic Health Record [PCEHR]) for 0.5% of the practice's standardised whole patient equivalent (SWPE) to be eligible for their PIP Digital Health Incentive payment.

The revised eligibility criteria are effective as of 1 May 2016. The size of the PIP payment is dependent on the size of the practice and is a maximum payment of $12,500 per quarter. Practices must comply with all five eligibility criteria to continue to receive the PIP Digital Health Incentive payments. The RACGP recently surveyed a number of practices involved in the PIP and most received only a portion of this maximum payment.

The Commonwealth advises that the revised PIP Digital Health Incentive requirement equates to the upload of approximately five SHS per full-time equivalent GP per quarter (ie for a practice with five full-time equivalent GPs, this would equate to approximately 25 SHS uploads per quarter). However, this SHS upload requirement is likely to increase over time.

The RACGP does not support the revised eligibility criteria.

My Health Record

The My Health Record is voluntary for both patients and healthcare professionals. The My Health Record is primarily a vehicle for consumers to share key pieces of their health information with healthcare providers of their choice. The My Health Record is a shared document and data repository, where a document is sent from a local clinical information system and can be accessed across the healthcare sector by registered users of the My Health Record.

The My Health Record is not a replacement for local clinical information systems, it does not replace or substitute for communications which occur directly between providers and it does not replace a practice's normal clinical records system.

My Health Record access controls

The documents and information stored in the My Health Record are under the patient's control and provider access is controlled by the patient. Consent to view any documents or information in the My Health Record is established through the patient's personal access controls. The default setting is for general access which allows any healthcare professional participating in the My Health Record to access the patient's record.

Patients have the option to restrict access by healthcare organisations to their entire My Health Record or to particular documents or information within their My Health Record.

Patients can:

- choose not to have a record at all
- ask healthcare providers not to add information to their record

- remove a document from view so that it is not available to healthcare providers but will continue to be stored by the System Operator and can be added back to the record at any time
- choose which healthcare organisation can access their My Health Record (eg a patient can authorise their general practice to have access but restrict access for their physiotherapy practice). Patients can also remove access and add new access controls if they change general practices
- limit access to the entire or part of their My Health Record by setting the appropriate access controls. If this is done, patients will need to provide an access code to those healthcare organisations they wish to permit to access their My Health Record.

Patients cannot:

- restrict access to their SHS, personal health summary or advance care planning information; they can, however, request information not be included when the SHS is uploaded and they can remove these documents from view
- alter clinical records (the patient can remove a document from view but cannot change the uploaded clinical content).

When registering for a My Health Record and setting their access controls (or choosing not to opt out of a record in the two national opt-out trial areas), patients provide 'standing consent' for healthcare organisations that provide them care to upload clinical information to their My Health Record.

With this standing consent, other than for the creation of an SHS, there is no requirement for a healthcare provider to obtain further consent prior to uploading clinical information to an individual's My Health Record, unless the patient expressly forbids this to be done. A healthcare provider must not upload information if the patient asks them not to do so.

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. Specific consent is also required for the creation and sharing of an SHS.

Consent is given to the entire healthcare organisation, enabling individuals who are authorised to access the My Health Record in that organisation to access the record. Individuals who are authorised to access the My Health Record in the organisation can access a patient's My Health Record in the delivery of healthcare to that patient, regardless of the patient's presence, subject to the patient's access controls.

A limited document access code (LDAC) may be used by a patient to restrict access to specific documents within their My Health Record. A patient can provide this to their healthcare provider for a one-time use.

A record access code (RAC) is a code that can be used to restrict access to a patient's My Health Record. The code is provided to a healthcare provider for all providers in the linked healthcare organisation to grant access to the patient's My Health Record.

Practitioners should have a policy and procedures in place to manage the destruction of the LDAC and RAC codes once they have been used and they should understand how their software and system handle these codes.

A healthcare professional can allow emergency access. Allowing emergency access may be warranted where the healthcare professional believes that access to the information is necessary to lessen or prevent a serious threat to an individual's life, health or safety and the patient's consent cannot be obtained. Access to the record this way will release restricted documents and will also trigger an audit log. Patients can create settings to be notified by email or SMS if this occurs.

Providers participating in the My Health Record must not discriminate against a patient who does, or does not, have a My Health Record or because of their access control settings. Providers must not upload a record that contains defamatory material. Providers may only upload a record if it does not infringe on another person's intellectual property rights or moral rights. Providers must take reasonable steps to ensure the quality of the content of the records.

My Health Record content

The My Health Record may contain a number of document classes. There may be documents from healthcare professionals, documents from the patient and documents from the Australian Government Department of Human Services – Medicare Services.

Documents provided by healthcare professionals may include:

- SHS – a clinical document summarising a patient's health status and including important information such as allergies/adverse reactions, medicines, medical history and immunisations. These fields are mandatory for an SHS
- event summary – a clinical document that may be uploaded to an individual's My Health Record summarising one or more episodes of care
- discharge summary
- referrals to specialists
- specialist letters
- diagnostic test results
- prescribing and dispensing information through electronic transmission of prescriptions (eTP).

Patient entered data[1] includes:

- personal details and emergency contact details
- personal health summary – a document created by the patient that includes medications and allergies/adverse reactions. This section of the My Health Record is accessible by healthcare professionals (unlike the personal health notes)
- personal health notes – an area of the My Health Record that allows individuals to store private notes about their health. This can be considered their private health diary. This section of the My Health Record is not accessible by healthcare professionals
- the contact details of the custodian of a patient's advance care directive.[2]

When registering for a My Health Record, the patient can choose to have their Medicare data included in the record. This can include the past (two years) and future Medical Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) (and Repatriation PBS) claims information, their organ donor status and, if relevant, details from the Australian Childhood Immunisation Register records. This data is visible to individuals authorised to access the record. There are, however, restrictions on the number of documents a My Health Record can hold. Extensive MBS and PBS data has been noted to prevent the upload of clinical documents.[3]

Shared health summary (SHS)

The SHS includes information that would often be found in a GP health summary; however, there is no requirement that the creator of the SHS be a GP.

A patient's SHS represents a summary of a patient's health information at a point in time and contains the patient's:

- past and present medical conditions
- current medications
- allergies and adverse events
- immunisations that have been recorded.

An SHS is created by a 'nominated heathcare provider' which is a term defined in legislation. Under the *My Health Records Act 2012* a healthcare provider is a nominated healthcare provider of a patient if:

- there is an agreement in force between the healthcare provider and the healthcare recipient that the healthcare provider is the nominated provider
- a health identifier has been assigned to the healthcare provider
- the healthcare provider is either
  - a medical practitioner
  - a registered nurse
  - an Aboriginal or Torres Strait Islander health practitioner with a certificate IV in Aboriginal and/or Torres Strait Islander Primary Health Care (Practice).

A patient may request to not include particular information in their SHS. If the provider creating the SHS agrees that the particular information may be too sensitive, it can be left out of the SHS. If, however, the patient requests to exclude something the provider creating the SHS feels is important for other healthcare providers to know, the provider may decline to upload the summary. An SHS should not be uploaded without the patient's awareness of content and their consent.

If a nominated healthcare provider wishes to change the information in a patient's SHS (eg the medications listed), the provider will need to upload a new SHS with the updated information, which is subject to the same consent obligations. There is no legislative requirement for healthcare providers to regularly update a shared health summary.

There is no requirement for a nominated healthcare provider to update an SHS outside of a consultation with the patient.

Provider access to the My Heath Record

Authorised healthcare professionals are able to access the system either via a conformant clinical information system with a secure individual logon, or via the provider portal (read-only) using an individual My Health Record compliant digital credential.

Provider portal

The provider portal is the interface through which healthcare provider organisations can access the My Health Record and view a patient's My Health Record without having to use a clinical information system. The provider portal is a view-only service.

To access the My Health Record via the provider portal, healthcare providers are required to have:

- a Healthcare Provider Identifier – Individual (HPI-I)
- a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate (for example a USB key or smart card) that identifies them as an authorised healthcare provider.

The registered healthcare provider organisation (one or more) where the healthcare provider practices then needs to provide authorisation to access the My Health Record via the provider portal by linking the HPI-I with their Healthcare Provider Identifier – Organisation (HPI-O).

Once registered, individuals authorised by the organisation will be able to access the My Health Record via the provider portal using a NASH PKI certificate for individual healthcare providers.

When individuals who are registered to access the My Health Record via the provider portal log into the system, they will see a list of all organisations they are authorised by and need to select the healthcare provider organisation they are representing. Healthcare provider organisations who choose to authorise access via the provider portal need to consider the risks associated with healthcare providers accessing patient records via the provider portal while acting as a representative for an organisation that is not directly involved in a patient's care.

Indemnity coverage

Indemnity coverage from 1 July 2013 includes a My Health Record specific clause. However, every MDO will have its own policies related to the My Health Record. Providers and practices should contact their MDO for specific advice.

Privacy and security

The *My Health Records Act 2012* and My Health Records Rule 2016 create some new obligations; however, GPs and practice staff already have a responsibility to ensure each patient's health information is kept confidential and secure.

The RACGP *Computer and information security standards* (2nd edition) further information and recommendations that will raise awareness of contemporary security issues.

The OAIC provides advice on how to manage personal information and also the required documentation for practices to comply with the Australian Privacy Principles.

The RACGP has developed a privacy policy template and provides other resources to ensure general practices can meet their privacy requirements.

PIP Digital Health Incentive requirement 5 checklist

This checklist is designed to help general practices meet the eligibility criteria for Requirement 5 of the PIP Digital Health Incentive in relation the upload of shared health summaries (SHS). This checklist is a guide only and does not describe the complete list of activities that should be undertaken.

Practice staff

The practice team should be aware of their responsibilities with regard to information security and each team member has a role to play when ensuring that patient and business information is protected.

Responsible Officer (RO) and Organisation Maintenance Officer (OMO)

The My Health Record legislation requires two designated roles in relation to computer and information security. These are the Responsible Officer (RO) and the Organisation Maintenance Officer (OMO).

- ☐ The RO and OMO have received training and understand their roles and responsibilities.
- ☐ The RO and OMO access training annually and when any new material or changed risks are identified.
- ☐ The System Operator has been notified of the contact details of the relevant staff undertaking these roles in the practice. The My Health Record System Operator is the secretary of the Department of Health and is responsible for the My Health Record.

Training

All staff who use the My Health Record should receive at least annual training and when any new material or changed risks are identified as required by the *My Health Records Act 2012* to ensure they are aware of their privacy and security obligations. Practices may choose to also document confirmation from relevant staff that they have received adequate training prior to their being allowed access.

- ☐ Staff have access to at least annual training.
- ☐ A record is kept of all training accessed and the names of attendees are documented.

Useful resources

Staff roles and responsibilities	RACGP Computer and information security standards – Standard 1: Roles and responsibilities
Responsible Officer and Organisation Maintenance Officer	RACGP Computer and information security standards: Compliance indicator 1.4 Responsible officer and organisation maintenance officer
Australian Government Department of Health	My Health Record
NEHTA – Getting started with eHealth for healthcare providers	eHealth Roles and responsibilities
NEHTA – eHealth training resources	eHealth Guides
My Health Record updates	*My Health Record News* – a digital bulletin for providers

IT systems in the practice

Information security requirements will be different for all general practices. It is therefore important for all practices to understand their information security needs, and to document the policies and procedures that the practice team needs to follow. This ensures the availability, integrity and confidentiality of all information held within the practice's clinical and business information systems.

Access to clinical and business information

Access to clinical and business information in the practice should be managed so that only authorised users can access information. The practice team should receive training on the relevant software and hardware and about the potential privacy and security risks before access and passwords are provided.

- ☐ Access rights are set up so practice staff only have access to the system functionality they require to carry out their day-to-day roles.
- ☐ A password policy is implemented, which determines password complexity, frequency of required password changes, individual and unique login and password requirements for all users.
- ☐ Staff have received training on the relevant software and hardware and about the potential risks before access and passwords are provided.
- ☐ Guest accounts and remote access are managed to ensure patient information is protected.
- ☐ System access is suspended in the incidence of a data breach, and notifications are made as per the OAIC Data breach notification – A guide to handling personal information security breaches.
- ☐ When a person ceases working at the practice their access is terminated.
- ☐ The software has auditing requirements to identify who has accessed the practice systems.

Protection of personal information

- ☐ Hardware, software and operating systems are physically protected and maintained to minimise and prevent unauthorised and accidental viewing of patient information.

Useful resources

Information security policies and procedures	RACGP Computer and information security standards: Compliance indicator 3.1 Policy content
Access rights	RACGP Computer and information security standards: Compliance indicator 4.3 Access rights
Passwords	RACGP Computer and information security standards: Compliance indicator 4.4 Password maintenance and 4.5 Password management
Permissions management	RACGP Computer and information security standards: Compliance indicator 4.9 Initial definition and permissions management
Computer screen confidentiality and the use of screensavers	RACGP Computer and information security standards: Compliance indicator 11.6 Confidentiality
Practice staff access agreement template	Appendix 2

My Health Record legislation requirements

The My Health Record is supported by a legislative framework that includes governance arrangements, a privacy and security framework and a registration process for both providers and patients. General practices using the My Health Record must ensure they comply with these legislative requirements.

Compliance with the *Privacy Act 1988* and the Australian Privacy Principles in relation to the protection of health information

The Privacy Act requires healthcare providers to comply with 13 Australian privacy principles (APPs), which set out how personal information must be handled and protected. Personal information should be managed in an open and transparent manner and practices need to implement procedures and systems to deal with privacy enquiries and complaints.

Patients that come to the practice:

- ☐ know why and how their personal information is collected
- ☐ know how their personal information is used
- ☐ know who will have access to their personal information
- ☐ have the option of not identifying themselves or of using a pseudonym
- ☐ have access to their personal information
- ☐ can opt out of receiving unwanted direct marketing. Direct marketing is covered under APP 7 and involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. More information on direct marketing can be found at the Office of the Australian Information Commissioner (OAIC)
- ☐ can ask for their personal information to be corrected
- ☐ can make a complaint if their personal information is mishandled
- ☐ can access the practice privacy policy which addresses all privacy breaches and complaints not just those that relate to accessing My Health Record. The RACGP has developed a privacy policy template to support practices in meeting these requirements.

Compliance with the *Healthcare Identifiers Act 2010* to protect individual healthcare identifiers (IHIs)

Compliance with the *Healthcare Identifiers Act 2010* to protect IHIs ensures that:

- ☐ reasonable steps have been taken so they are not lost, modified, disclosed or accessed by an unauthorised person.
- ☐ they are only collected from the healthcare identifiers (HI) service by authorised users who need this information as part of their everyday work activities
- ☐ they are only collected to manage a patient's healthcare or to communicate information as part of providing healthcare
- ☐ patients know the practice is collecting IHIs as part of providing healthcare. This should be included as part of the practice privacy policy.

Compliance with the My Health Records Rule 2016

A written policy is required, which reasonably addresses how users are authorised to access the My Health Record within your practice. There are a number of specific requirements for this policy and the RACGP has developed a policy template (refer to Appendix 1).

Useful resources

Frequently asked questions regarding the *Privacy Act 1988*	OAIC FAQs for agencies and organisations – Health service providers
Obligations in relation to the handling of individual healthcare identifiers (IHIs) by healthcare providers	OAIC Privacy business resource 1: Individual Healthcare Identifiers – Compliance obligations of private healthcare providers

Data quality

Uploading shared health summaries (SHS) means your practice is sharing local practice information with other healthcare providers. General practices uploading SHS should be mindful of data quality.

Useful resources

Content of patient health records	*RACGP Standards for general practices* (4th edition)

Appendices

Appendix 1 – My Health Record policy template for general practices available at www.racgp.org.au

Appendix 2 – Agreement to access the My Health Record template for general practices available at www.racgp.org.au

Appendix 3 – Assisted registration policy template for general practices available at www.racgp.org.au

RACGP

Healthy Profession.
Healthy Australia.