Overview of policies required to participate in digital health

This document provides an overview of the policies that are required for healthcare organisations to participate in digital health.

Directory Name	Objective of the policy	Sample Policy
My Health Record system Policy	To govern the use of the My Health Record system, the My Health Record system Rule state that in order to participate in the My Health Record system, your organisation needs a written policy in place to address the following: a) the manner of authorising persons accessing the My Health Record system via or on behalf of the healthcare provider organisation, including the manner of suspending and deactivating the user account of any authorised person: (i) who leaves the healthcare provider organisation; (ii) whose security has been compromised; or (iii) whose duties no longer require them to access the My Health Record system; b) the training that will be provided before a person is authorised to access the My Health Record system, including in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the My Health Record system and the consequences of breaching those obligations; c) the process for identifying a person who requests access to a consumer's My Health Record and communicating the person's identity to the System Operator where required; d) the physical and information security measures that are to be established and adhered to by the healthcare provider organisation and people accessing the My Health Record system via or on behalf of the healthcare provider organisation, including; i. restricting access to those persons who require access as part of their duties; ii. uniquely identifying individuals using the healthcare provider organisation's information technology systems, and having that unique identity protected by a password or equivalent protection mechanism; iii. having password and/or other access mechanisms that are sufficiently secure and robust given the security and privacy risks associated with unauthorised access to the My Health Record system; iv. ensuring that the user accounts of persons no longer authorised to access the My Health Record system via or on behalf of the healthcare provider organisation prevent access to the My Health Record system; and v. suspending a user account that enables access to the My Health Record system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised; and e) mitigation strategies to ensure My Health Record-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management. f) where the healthcare organisation provides assisted registration: (i) the manner of authorising employees of the organisation to provide assisted registration; (ii) the training that will be provided before a person is authorised to provide assisted registration; (iii) the manner of recording a consumer's consent and how that record will be handled for retention purposes; and (iv) the process and criteria for identifying a consumer for the purposes of assisted registration.	**Download a sample policy**

Directory Name	Objective of the policy	Sample Policy
National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) Certificates	Healthcare Organisations accessing the My Health Record system via a conformant Clinical Information System requires a NASH PKI Certificate for Healthcare Organisations. The NASH PKI Certificate for Healthcare Organisations Terms and Conditions require the healthcare organisation to have a set of policies and procedures in place governing use of the NASH PKI Certificate.	**Download a sample NASH PKI Certificate policy**

The following policies are not mandatory for digital health. However they are a requirement for General Practice eligibility for the PIP eHealth Incentive:

Directory Name	Objective of the policy	Sample Policy
Secure Message Delivery (SMD) Policy	Requirement 2 of the PIP eHealth Incentive Guidelines states that practices must have a written policy in place encouraging use of Secure Messaging. Practices may wish to keep a record of secure messaging use to measure and assess progress against this policy. Most products are able to keep a record of messages sent and/or received and should be installed with this function activated.	**Download a sample SMD policy**
Clinical Coding and Terminology Policy	Requirement 3 of the PIP eHealth Incentive Guidelines state that practices must ensure that where clinically relevant, they are working towards recording the majority of diagnoses for active patients electronically using a medical vocabulary that can be mapped against a nationally recognised disease classification or terminology system. Practices must provide a written policy to this effect to all General Practitioners within the practice. Developing a clinical coding policy for your practice achieving consistent disease coding requires the entire clinical team to be on board, so it's important to get all staff engaged in the process. A practice policy for clinical coding will need to address the roles and responsibilities of each team member.	**Download a sample Clinical Coding and Terminolgy policy**