APPENDIX 1

Overview of IPPs & HPPs

An overview of the **12 Information Protection Principles (IPPs)**

Collection	1. Lawful – We only collect personal information for a lawful purpose that is directly related to our functions and activities 2. Direct – We collect personal information from the person concerned 3. Open – When collecting personal information, we inform people why their personal information is being collected, what it will be used for, to whom it will be disclosed, how they can access and amend it and any possible consequences if they decide not to give it to us 4. Relevant – When collecting personal information, we ensure it is relevant, accurate, not excessive, and does not unreasonably intrude into people's personal affairs
Storage	5. Secure – we store personal information securely, keep it no longer than necessary, destroy it appropriately, and protect it from unauthorised access, use or disclosure
Access	6. Transparent – we are transparent about personal information that is stored, what it is used for and people's right to access and amend it 7. Accessible – we allow people to access their own personal information without unreasonable delay or expense 8. Correct – we allow people to update, correct or amend their personal information where necessary
Use	9. Accurate – we make sure that personal information is relevant and accurate before using it 10. Limited – we only use personal information for the purpose it was collected for unless the person consents to the information being used for an unrelated purpose
Disclosure	11. Restricted – we will only disclose personal information with people's consent unless they were already informed of the disclosure when the personal information was collected 12. Sensitive – we do not disclose sensitive personal information (such as ethnicity or racial origin, political opinion, religious or philosophical beliefs, health or sexual activities, or trade union membership) without consent.

Schedule 1 of the HRIP Act provides a similar set of privacy standards for health information. They are the health privacy principles (HPPs), and they are largely the same as the IPPs, however without an equivalent to IPP 12 (Sensitive) and with other additional obligations and standards instead.

Below is an overview of the **12 Health Privacy Principles (HPPs)**

Collection	1. Lawful – We only collect health information for a lawful purpose that is directly related to our functions and activities 2. Direct – We collect health information from the person concerned unless it is unreasonable or impractical to do so 3. Open – When collecting health information, we inform people why their health information is being collected, what it will be used for, to whom it will be disclosed, how they can access and amend it and any possible consequences if they decide not to give it to us 4. Relevant – When collecting health information, we ensure it is relevant, accurate, not excessive, and does not unreasonably intrude into people's personal affairs
Storage	5. Secure – we store health information securely, keep it no longer than necessary, destroy it appropriately, and protect it from unauthorised access, use or disclosure
Access	6. Transparent – we are transparent about health information that is stored, what it is used for and people's right to access and amend it 7. Accessible – we allow people to access their own health information without unreasonable delay or expense 8. Correct – we allow people to update, correct or amend their health information where necessary
Use	9. Accurate – we make sure that health information is relevant and accurate before using it 10. Limited – we only use health information for the purpose it was collected for unless: a. the person has consented to its use for another purpose, b. it is being used for a purpose directly related to the purpose it was collected for, c. we believe that there is a serious threat to health or welfare, d. it is for the management of health services, training, research or to find a missing person, or e. it is for law enforcement or investigative purposes.
Disclosure	11. Restricted – we will only disclose health information for the purpose it was collected for unless: a. the person has consented to its disclosure for another purpose, b. it is being used for a purpose directly related to the purpose it was collected for, c. we believe that there is a serious threat to health or welfare, d. it is for the management of health services, training, research, compassionate reasons or to find a missing person, or e. it is for law enforcement or investigative purposes.
Other	12. Identifiers – we do not use unique identifiers for health information, as they are not needed to carry out DCITHS's functions

13. Anonymity – we allow people to stay anonymous if it is lawful and practical for them to do so

14. Transborder – we do not usually transfer health information outside of New South Wales

15. Linkage – we do not currently use a health records linkage system and do not anticipate using one in the future. But if we were to use one in the future, we would not do so without people's consent.