Checklist: How can you ensure accuracy?

How can you ensure that the biometric information you hold, and the operation of your biometric system, is accurate?

What is reasonable in the circumstances to avoid accuracy errors will change depending on your overall risk profile (the type of information you hold, what it is being used for, your context, and the potential harm that individuals may experience).

Example steps to ensure accuracy:

- ✓ Ensure the biometric system is using sufficiently high-quality samples e.g. photos, audio recordings.

- ✓ Keep biometric samples up to date as required and generate new biometric templates when needed (for example, due to aging, surgery or injury).

- ✓ Where necessary, implement manual (human) review of matches by the biometric system before taking action based on the biometric system. You also need to ensure the staff involved have appropriate training and are effectively equipped to challenge the accuracy of results if needed. This is sometimes called having a "human in the loop". Having a human in the loop will be essential for some uses of biometric information – for example, if you are operating a biometric watchlist or any other context where people could be negatively impacted by the use of their biometric information.

- ✓ Regularly review and refine the sensitivity and specificity settings of the biometric system to ensure the rate of any false positive or false negative matches is appropriate for the use case and not leading to adverse outcomes for individuals.

- ✓ Select a biometric system with appropriate accuracy for your privacy risk and overall context. Some systems show better performance in certain contexts or

for certain uses than others, especially in different conditions (i.e. in the wild versus controlled environments). You should refer to independent evaluations (e.g. by NIST) of the accuracy where possible.

- ✓ Train staff and any other users of the biometric system about what a match means, so that they better understand the results of a biometric system and can respond appropriately. For example, a match resulting from a verification process is not a definitive determination of a person's identity – it reflects the statistical likelihood that this person is same as the identity they are claiming.

- ✓ Have a process or audits in place to identify and resolve errors and issues related to the biometric system, including understanding and mitigating any bias in the system (such as the system being less accurate for a particular demographic group or skin tone). The risk of inaccuracy from bias needs to be addressed both with human review (e.g. training, two person check before acting on an alert) and system checks. Unaddressed risk of bias may compromise the accuracy of the system.

- ✓ Ensure individuals can raise concerns about the accuracy of the system and you have a process in place to respond (see also our guidance on rule 7 – correction of biometric information).

- ✓ Conduct due diligence when choosing or procuring a biometric system or service provider and consider the suitability for the setting the system will be used in and the New Zealand demographic.