Digital, Data and Technology Services – minimum requirements

The health and disability sector uses a wide range of digital, data and technology services (digital services) from many suppliers. Services, and the suppliers that provide them, continually evolve through innovation and as new capabilities and uses of technology emerge.

An individual health organisation will typically contract with multiple suppliers of services to support their business functions. While each service will provide a unique set of capabilities there are common requirements that need to be met by all digital services to ensure they are safe, secure, integrated, reliable and provide appropriate access to data and information.

The following describes the baseline common requirements that all health organisations are expected to meet. It is not an exhaustive list and should be considered a minimum level of practice. The Ministry of Health will update the requirements annually.

The baseline requirements are:

General

1. All new digital services and the data they collect and hold must be conformant, and in some cases compliant[1], with Ministry of Health published HISO standards, roadmaps and architecture guidelines and integrate with Ministry of Health mandated national digital services (such as the National Health Index).
2. Digital services should be integrated to support a consistent, and where possible seamless, user experience and avoid unnecessary duplication of data and functions. Application Programming Interfaces should be used where possible to support integration with and by others.
3. Digital services and supporting infrastructure must be maintained and regularly upgraded to stay within agreed supplier support thresholds as a minimum.
4. Cloud delivery should be considered for all digital services in preference to locally hosted and configured technology, and an assessment of risk undertaken prior to their use.

Security

5. Health organisations must regularly assess their conformance with the Health Information Security Framework and ensure that all new digital services are conformant using guidance such as the Government Chief Digital Office Cloud Risk Assessment framework.
6. Security processes must be consistent with industry good practice such as that described in the Health Information Security Framework, including applying security patches in a time frame proportionate to the assessed risk.
7. Digital services should be regularly independently security tested in a time frame proportionate to their criticality and the type of data they process and evidence provided that any deficiencies or vulnerabilities identified have been rectified.

[1] **Conformance** describes the need to demonstrate that the outcomes of a certain standard are being met even if the standard itself may not be partially or fully followed (for example, a different standard may be in use that achieves or exceeds the required outcomes).
Compliance prescribes the adherence to a certain standard and requires that a particular standard is adopted in order to achieve specified outcomes.

Data

8. Data must be governed consistent with industry good practice and guidance including consideration of data protection and use, privacy, social license and Māori data sovereignty. Health organisations should consider their conformance with the Health Information Governance Guidelines. Health organisations must clearly define the data assets they hold and who is responsible for their stewardship.
9. Data must be available for sharing, transfer and access with appropriate authorisation to other digital services, organisations and stakeholders, including the consumer. Access to data must not be unreasonably withheld or onerous and supplier contracts must not impose technical or commercial barriers.

Commercial

10. Supplier contracts must not include exclusive commercial arrangements that incentivise or require aggregation of services.
11. Suppler contracts must include provisions for service retirement or exit, for example maintaining data access or reconfiguring integration design, in the event that supplier contracts are terminated.