Ministry of Health
PO Box 5013
WELLINGTON 6140

Department of Internal Affairs
PO Box 805
WELLINGTON 6140

12 April 2017

The Chief Information Officer
District Health Board

Changes to the Ministry of Health's policy on cloud computing

The Ministry of Health and the Government Chief Information Officer (GCIO) are writing to advise you of changes to the Ministry of Health's cloud computing policy.

Background

The Ministry's policy has been that personal identifiable health information cannot be stored or processed offshore by a public cloud service unless the health provider has first been granted an exemption to do so by the Ministry. In early 2016, the Ministry allowed health providers to use public cloud services without obtaining an exemption provided that they have been reviewed and accepted by the Ministry as fit for purpose.

The use of public cloud services is now more commonplace and the Ministry's earlier concerns about the privacy and security of personal health information stored or processed offshore have been greatly allayed. In July 2016, Cabinet moved to actively promote the use of public cloud services for government agencies.[1]

For these reasons, the Ministry has made a major revision to its cloud computing policy.

Revised Ministry of Health policy

The following policy takes effect from the date of this letter.

1) For all health providers

- The Ministry's existing exemption process for offshore-hosted public cloud services is discontinued.
- The Ministry will no longer review and accept individual public cloud services as fit for purpose. The list of accepted public cloud services on the Ministry's website will therefore be removed.

[1] See SEC 16 MIN 2006 which was confirmed by Cabinet – CAB 16 MIN 0316

- Health providers remain responsible for the security and integrity of personal health information that is stored or processed by public cloud services. All health providers wanting to store personal health information in a public cloud service may do so provided they first undertake a formal risk assessment. The outcome of the risk assessment must be signed-off by the health provider's senior management prior to using the services. Public cloud services should be considered on a case by case basis.
- Guidance on how to manage risk assessments can be found on the GCIO's website at https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/
- Where the risk assessment identifies areas of significant concern, the health provider may wish to discuss these matters with the Ministry of Health (email cloudcomputing@moh.govt.nz) before making its decision. Particular areas that may generate concerns are summarised in section 18 of the Health Information Security Framework.[2] They include sovereignty, governance, confidentiality, provider integrity, availability, and incident response/management.

2) Additional requirements for DHBs (for all other health agencies this is optional but recommended)

DHBs must:

- forward a copy of completed risk assessments to the GCIO. A copy is also to be provided to the Ministry of Health prior to the commencement of the cloud service use
- record each individual public cloud service utilised within its application portfolio management system.

Next steps

The Ministry will shortly be updating its website to reflect this change in policy. If you have any questions about the revised policy please email cloudcomputing@moh.govt.nz

Yours sincerely,

(Signed)
Ann-Marie Cavanagh
Chief Technology and
Digital Services Officer
Ministry of Health

(Signed)
Chris Webb
General Manager Commercial Strategy and Delivery
on behalf of the GCIO
Department of Internal Affairs

[2] Refer HISO Standards - http://www.health.govt.nz/publication/hiso-100292015-health-information-security-framework