133 Molesworth Street
PO Box 5013
Wellington 6145, New Zealand
T +64 4 496 2000
W www.medsafe.govt.nz

William Francis

By email: fyi-request-12804-07dbf89e@requests.fyi.org.nz
Ref: H202003113

Dear Mr Francis

Response to your request for official information

Thank you for your request for information under the Official Information Act 1982 (the Act) on 7 May 2020 for:

> *"(A) Methodology and regularity of HISF audits*
> *Please provide current documents and reports that detail the methodology and regularity of HISF audits that are conducted upon the following types of agencies:*
> *1. New Zealand Public Service Agency*
> *2. New Zealand State Sector Agency*
> *3. New Zealand Health Agency*
> *If no such audits are carried out, please provide explanation and/or justification as to why, with reference to the Health Information Privacy Code 1994.*
>
> *Agency obligations for the holding and disclosure of medical and health information*
> *I refer to the Health Information Privacy Code 1994 and the Health Information Security Framework:*
> *https://scanmail.trustwave.com/?c=15517&d=v7Sz3jhBTjB3l7tj5aivMwErlQ2sAL1mM5E-_zkWww&u=https%3a%2f%2fwww%2eprivacy%2eorg%2enz%2fthe-privacy-a*
> *https://www.health.govt.nz/publication/hiso-100292015-health-information-security-framework*
>
> *(B) Please compare and contrast the differences between the obligations and legislative responsibilities that each of the following types of agencies must adhere to when collecting, holding, disclosing, and sharing medical and health information:*
> *1. New Zealand Public Service Agency*
> *2. New Zealand State Sector Agency*
> *3. New Zealand Health Agency"*

On 5 June 2020 the Ministry of Health (the Ministry) decided to extend the period of time available to respond to your request under section 15A of the Act as further collation and research and consultation was required.

In response to part A of your request the Ministry of Health (the Ministry) does not undertake Health Information Security Framework (HISF) audits, so this part of your decision is refused under 18(e) as the information does not exist.

For your reference, Appendix 1 sets out the authority for the HISF and the requirements that are imposed on district health boards (DHBs) to comply with this standard. This mandate is a direct quote from advice provided to all DHBs on 15 December 2016. While the HISF has authority over health agencies, there is no authority over Public Service or State Sector agencies. The Ministry is not resourced to undertake HISF audits.

DHBs have been reminded of their obligation under the operation policy framework (OPF) to comply with Health Information Standards Organisation (HISO) standards (in particular, the HISF). The Ministry undertook a survey of all DHBs in March, June and December 2016 to assist DHBs assess their level of HISF compliance.

In response to part B of your request; the Health Information Privacy Code 1994 (the Privacy Code) applies to agencies in the health sector and covers health information collected, used, held and disclosed. Further information about the Privacy Code can be found on the Privacy Commissioner's website: www.privacy.org.nz. Where the Privacy Code does not apply to a particular agency, the Privacy Act 1993 will apply. Information about the Privacy Act 1993 can also be found on the website above.

You have the right, under section 28 of the Act, to ask the Ombudsman to review any decisions made under this request.

Please note that this response, with your personal details removed, may be published on the Ministry website.

Yours sincerely

Gaynor Bradfield
Manager, Office of the Deputy Director-General
Data and Digital

Appendix 1: Extract from advice provided to all DHBs on 15 December 2016

The mandate that all DHBs operate under is based on the terms of the Crown Funding Agreement (as formally signed off between the Minister of Health and DHBs) through which the Crown agrees to provide funding in return for the provision of specified services: http://nsfl.health.govt.nz/accountability/crown-funding-agreement

These services are set out in the Operation Policy Framework (OPF) - the set of business rules, policy and guideline principals that outline the operating functions of DHBs. The 2016/17 OPF can be found at the following link: http://nsfl.health.govt.nz/accountability/operational-policy-framework-0

The 2016/17 OPF (section 11.2.3c, page 75/76) states

" ...each DHB must take the following actions...

c. Proactively support the development and adoption of Health Information Standards Organisation (HISO) standards by:

- adhering to and meeting the requirements of all published HISO standards ..."

There are lots of other conditions contained within the OPF. Section 11 in particular covers Information Technology.

These rules also apply to any wholly owned DHB agency (e.g. health alliance) and to any contract that a DHB has with an eternal agency/supplier – i.e. any agency that a DHB works with must meet the conditions imposed on the DHB. This then will apply to PHOs and others down the line as contracted providers of service to the health and disability sector.

In respect of the question about the interaction of the NZISM and the HISF (and of course the PSR - Protective Security Requirements), these are requirements imposed on Government Information generally. All information held by DHBs fits into this category. They come from the Government Communications Security Bureau (GCSB), the SIS, the Government Chief Information Office (GCIO), and Protective Security Requirements New Zealand. Other agencies also have an input – e.g. the Officer of the Privacy Commissioner. You will find links to all of these agencies in Appendix D of the HISF.

The HISF does take in to account the requirements of the above agencies and their documents - see HISF section 1.6 - and does not contradict any specialist requirements.