Overall comments

1. Do you have any general feedback on the core framework (all sections excluding appendices)?

The Hauora Health Privacy Working Group acknowledges the considerable work that will have been undertaken in revising the HISF. Health information security is a rapidly developing and increasingly complex matter.

However, after careful scrutiny of the draft core framework the Group has concluded that the document is poorly constructed and muddled in its approach. It is too loosely, or in at least one place, carelessly written; it needs more attention to detail in places. There is inadequate definition of terms as well as inconsistent use of terms. This is confusing. We struggled to understand a number of the Figures so they didn't add any value. As presented, we do not believe the core framework is fit for purpose. It doesn't meet our expectations regarding the security of our personal health information. This is disappointing and deeply concerning.

We suggest the core framework be rearranged. It needs to begin with an Introduction or similar that adds more than the present Background. It needs to include a statement about the following matters:

- the importance of health information security to the patient/health service consumer in the course of using health services;
- the importance of confidence and trust in using health services, which will be undermined if patients/consumers aren't confident their information will be held and shared securely;
- that the harms that can be done to individuals in the event of a data breach can be significant.

We acknowledge there are harms to provider organisations as well but in a technical document such as this it is easy to lose sight of the individual. The significance of having good security in relation to personal health information of individuals in a healthcare context is heightened, when we consider recent cybersecurity attacks in NZ's health sector and in Australia.

The Introduction could be followed by HISF development, and then Māori Co-design objectives. While the latter are not specifically tailored to the HISF, having them to the fore of the document reflects their importance in the reformed health environment. They may need to be amended.

Purpose and Scope could follow in the form of two statements that aren't muddied /muddled by additional information that is not a neat fit.

Then HISF approach, which we recommend **renaming Key Definitions** or similar. Further comments are provided in Sections 5 and 6.

The core framework needs a comprehensive Glossary, along the lines of 2015 HISF.

2. Is the framework too wide or too narrow in its scope?

a) Too wide

b) Too narrow

c) Just right

d) Other – please comment in the box below:

Insufficient clarity to reach a conclusion, but our concerns and comments point to it being too narrow. We believe the scope should reflect a more holistic/comprehensive approach.

(continued over the page)

Section-specific comments

Please provide any comments or feedback you have about the following sections.

3. Section 1 – Purpose

As written, we don't believe the core framework provides guidance and requirements that can be easily understood, noting that requirements are met, not adopted.

We suggest the 2nd and 3rd paras be incorporated in an Introduction.

We query if the four points in para 3 are also expected to be the (key) objectives that need to be met by this framework. i.e. in the event of uncertainty or conflict between requirements, what are the overarching requirements/objectives to guide users?

4. Section 2 – Scope

Health information:
Needs to be defined further; suggest it also includes information which may 'reveal or infer' health or medication information and conditions, similar to the GDPR. Health information/data relating to health, genetic data, and biometric data are all afforded stronger protection in the GDPR.

It would seem useful to include who/which agencies are expected to comply as this brings in the segmentation approach. Will it cover NZ's bio/health tech start- ups and clinical trials environments? The point is particularly important, as we are seeing an increase in biotech and health tech start-ups. A good example here is the wearable tech sector. Many companies that develop wearable tech have been involved in clinical trials, but outside of clinical trials, their products and services are not subject to the same oversight that might apply in a medical context.

As more products that collect and share data come to market, there is some level of future risk. What we mean is that it is not possible to know all the ways that personal health information/data can be used in health research and other research in the future, as well as by businesses. Given the trend for entities to share data in order to compile sophisticated profiles about individuals, some more thought should be given to this. We acknowledge this is not easy, but it is important to be prepared for future problems.

Does HISF also need to clarify that it is not intended to cover personal health information held by electricity retailers, telcos, NZTA?

Anonymised personal health information not necessarily subject to the same sharing restrictions:
This is vague, and suggests there may be no guidance. We assume it is being suggested that anonymised information can be subject to a varied, or lower, form of security. If this is the case, we don't agree with this as a rule – anonymised information may increase scope for use and sharing, but appropriate security and confidentiality should still be applied as necessary. Information which looks 'anonymised' as an output may actually refer to identifiable data in the backend. This is particularly true if we use the example of genetic information/data, where several studies have demonstrated that re-identification of individuals is possible with access to very little information relating to the individual.

'Anonymised' should also be defined.

Patient identifiable health information classified as 'IN-CONFIDENCE', 'MEDICAL IN-CONFIDENCE' or 'SENSITIVE' – these need to be defined.

5. Section 3 – Background

We suggest this section be incorporated in an Introduction or similar as per our feedback in Q6.

It could briefly outline why 2015 HISF is no longer fit for purpose and how 2022 HISF will address this. In particular, how did 2015 HISF not cater for Māori health and how is it expected that 2022 HISF will achieve this?

We would expect equal security protections to be provided to all types of data. Is this potentially being confused with collection/purpose/management/use of data? Particularly for secondary public good purposes? (We would expect the latter is all out of scope?). To the extent applicable, we recommend that:

- it needs to be clear that Māori health information/data should be subject to equivalent or greater protection with regards to their specific objectives/concerns;
- and that further thought be given to allow for lower levels of security for certain groups to achieve objectives. It is concerning and maybe counter-productive in the event of a data breach that could have been prevented had safeguards been tighter.

We also have a concern about health information that may relate to justice investigations, migrants or asylum seekers that could be at additional risk due to additional transfer or accessibility implications.

6. Section 4 – Development

ISO has many very specific frameworks and standards for different industries etc, so it would be useful if 2022 HISF reflects why there is a move from ISO to NIST Cybersecurity Framework-style model. Is it because NIST is being adopted by Te Whatu Ora Health NZ, or is NIST generally more popular in NZ? We are not sure what ISO standards would be the 'baseline'. There is also the issue of ensuring that users are applying the latest version of any sections from a standard originating from another body.

While ISO and NIST have differences they have been of equally good standing globally, provided they are used in a holistic way as intended. They should both have good coverage; they also provide a baseline; and there is certainly a lot more that will be done in any program than what they define. In this regard, they give minimum assurance that certain minimums are provided for that conform to a consistent perspective.

Further, we have noted that in February 2022 "NIST began the process of updating the Cybersecurity Framework." It has been "suggested more detailed guidance for the health care industry is required."

We would like an explanation about why NIST is preferred, and what is actually meant by NIST-"style model". We have interpreted this as being NIST inspired, but not conforming. It is too loose and potentially problematic with respect to interpretation and expectations around compliance.

We suggest many technical IT professionals may find this challenging. How can they communicate security gaps to management if it's all interpretative; and 'translate' SME content to ensure it is understood by key decision makers?

Patients/consumers have expectations that their personal health information is held securely, consistent with industry-based best practice. They will be seeking substantiated assurances

that their health providers comply. The move to the NIST-style model may not deliver as it appears to be more 'shades of grey' than 'black and white'.

The core framework goes on to create confusion by using a hybrid of NIST and ISO. e.g. the Principles are based on the NIST framework and Assertions are grounded in ISO 27001-2 standards.

This raises the question, "Are we following ISO or NIST requirements?" If we are using both, then we need to acknowledge the core framework is a jumble of both so users can do an appropriate gap analysis if they need to. We may be happy to support cherry picking the best of both, so long as this is made abundantly clear. Otherwise, there may be assumptions made by an agency if NIST is used already, that the organisation is already covered. Or, that following this framework provides more assurance than it actually does. This may include misunderstandings that following this framework is effectively equivalent to NIST or ISO assurances, which we doubt, based on our review of this draft.

7. Section 5 – ~~Approach~~ Key Definitions

Do you have any feedback on the approach adopted in the creation of the updated HISF?
As this covers HISF sections 5.1 to 5.6, please clearly identify the section number and sub-heading related to each of your comments.

Personal health information (PHI) and patient identifiable information (PII) need to be defined in a/the Glossary.

We note 5.1-5.6 are definitions of the key sections within the framework. We don't know if/where our comments on these definitions fit within the framework but we expect them to be given due consideration.

Recommendation – rename this section Key Definitions. See additional comment in Section 6. Key Definitions should include the foundational building blocks as per Section 6. They should be listed/appear in the same order in sections 5 and 6 to avoid confusion.

5.1 Principles
We note these are based on the current NIST framework, and further note in the current drafting of 2022 HISF the Principles are :
(1) not aligned / the same as NIST, and
(2) missing important elements provided by NIST.

We expect closer alignment to provide assurance on the robustness of this framework, although we would still caveat these are intended as a guide and so should be further scoped and defined for the intended context of the 2022 HISF.

Additional concerns are outlined below.

At the outset, we note that the Principles don't appear to incorporate the lifecycle of information and managing over time i.e. updates to information/records, merging, transfers between systems, system changes.

'Change Management' is an SME information area of expertise and security is relevant here too. This, for example, may cover risks relating to practices and habits in the testing and development of new software/databases/ analytics which use copies of existing, real datasets and sharing this with a wide cohort in the process. Likewise, it's not uncommon to make sure the live system still produces the same outcomes, once the change is added/completed. There should be an approach about how to do so safely. You don't want the live system to have the best security and fail to secure your test environment.

Quoting from NIST (in italics),

Identify – *Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities*. We consider that systems, people, assets, data and capabilities need to be set clearly as scope requirements. Cyber security is not only a technology/online thing, although it's usually considered in this way. Failing to consider the eco-system of information will leave gaps and vulnerabilities, i.e. exposing risks.

The activities in the Identify Function are foundational for effective use of the Framework. It includes *Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs*. Examples of outcome *Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.*

'Understand the risk' is vague, and not often understood/evaluated in a meaningful way on its own. We suggest that clarifying risks according to the assets' threats and vulnerabilities is preferable. If there is a recommended standard that should be applied to guide this (and standards do exist for information risk management, such as FAIR), this should also be identified to reduce subjectivity in risk management and provide greater assurance in the consistency of this framework.

Protect – *Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology*

In addition to the above, the framework should add: system, third party procurement (procurement is too narrow), online / internet of things (not the same as "technology").

Detect – *Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.*

Respond – *Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.*

Recover – *Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.*

Notably, the Principles don't include an equivalent for the NIST Principle, 'Recover'. We think they should, to aid recovery of personal data in the event of loss (from theft or other failures) and forensics, at minimum.

5.2 Assertions

Noting these are grounded in ISO 27001-2 standards

Refer to comments in Section 4 Development

5.3 Controls

Correction: *Controls are also risk reduction measures with associated compliance requirements.*

We have reservations around the adequacy of the description for an information security framework. We suggest it be reviewed and/or strengthened bearing in mind:

- The many types of information controls that are appropriate for different contexts, and

- Who are the expected users? What will they do with it? Is it for security and information risk professionals? Or is it to guide a senior management/executive level?

5.4 Requirements
There needs to be greater clarity around the difference between 'Assertions' and 'Requirements'.
We would expect all "must" statements are/can be matched to a requirement.
A requirement is typically a specific capability that must/should/could be met to support a user need, business need or compliance need.

Control compliance – We are unsure how this is meant to be interpreted. Controls tend to be effective or non-effective. Requirements are met/satisfied, or not.

5.5 Guidance
Correction: *Guidance ~~are~~ involves detailed level "should" statements outlining….*

5.6 Outcomes
Correction: *There are different methods to achieve compliance with an assertion. The guidance suggests one method, but as long as the desired control objectives or outcome are /is achieved, there is ….*

The reference to outcomes is confusing here without the outcomes or the specific 'desired control objectives' being listed in this section. We are unsure how this all fits together within the core framework. What are the actual key outcomes for the Framework? The table on page 7 talks about outcomes, or are the outcomes the ones that are referred to in the bullet points under section 1 Purpose? Further, the Outcomes aren't mapped to Appendix B, and are not described for each information security domain topic and/or control area.

Clarity is necessary ~~to~~ so that those implementing the actions and controls under the guidance know what they are working towards and why.

We strongly recommend the details on outcomes are further particularised and consistently referred to in the document. They should link back to opening content in the Purpose section.

Some requirements / requirement categories are also likely to have some expected outcomes, so this Framework will be a useful and pragmatic tool to aid direction where there may be conflict, if done well.

8. Section 6 – Framework

Do you have any feedback on the framework outlined in the updated HISF?
As this covers HISF sections 6.1 to 6.1.9, please clearly identify the section number and sub-heading related to each of your comments.

Reword: *The 2022 HISF framework is an approach rather than a 'yes' and 'no' standard. It is more about how we think and less about compliance,…*

As written a layperson could interpret this as, so long as we get our thinking right, compliance doesn't/may not matter. It doesn't inspire confidence in the 'approach'. Consumers/patients expect that organisations will work towards achieving industry best practice and compliance.

……..which will be worked through as part of the developing Te Whatu Ora operating model.

While page 1 of the Framework refers to Te Whatu Ora-Health New Zealand it could be easily overlooked. It would be useful to have a statement in an Introduction that Te Whatu Ora is being used throughout 2022 HISF as the preferred terminology for Te Whatu Ora-Health New Zealand.

6.1 HISF strategy map (pg 7 and part of pg 8)
This section, before it breaks into further sub-sections e.g 6.1.1, would benefit from sub-headings. It contains various information that is linked to other sections but this is not made clear. It is difficult to see how things fit together.

Define ‘Health sector’ and ‘user’

Fig 1 HISF Strategy Map

Correction: Outcomes sought: 3rd bubble – *Build trust and confidence in the ~~sectors~~ sector’s ability to secure information*

Desired behaviours of health sector participants: who are ‘participants’? Are they the same as ‘users’?

Reword: Monitoring and measurement – *Capability to capture compliance data, ~~and~~ assess sector readiness* and ongoing continuous improvement (or similar). ‘Readiness’ implies status at the outset; we believe it must extend to the long term.

Associated Table

Outcomes sought
Correction: *Build trust and confidence in the ~~sectors~~’ sector’s ability to secure information*

We will observe this by…

Who is doing the observing and measuring? Te Whatu Ora? The collective ‘we’? Will this be specified in the segments? This needs to be clarified. The public has an interest in knowing. We suggest this is ultimately a Te Whatu Ora responsibility at either national or regional level.

- *Enable data sharing and collaboration/ Improved patient wellbeing and clinical outcomes*

We believe there is insufficient alignment between these points to demonstrate a direct cause/effect which can be objectively identified and assessed. How do you measure/attribute this as an outcome of a security practice? An intermediate measure needs to be developed to accommodate for this in order to reliably observe this.

- Correction: *Build trust and confidence in the sector’s ability to secure information/ Improved engagement and wide adoption*

There may be an increase in confidence through reduced data and security breach incidences; and effective mitigating and handling of information risks in the event they occur. However other factors are at play, particularly the digital divide. Again, should an intermediate measure be developed?

Pg 8

Successful implementation

- *use the HISF as a key mechanism for assessing and improving information security maturity, and manage the organisation’s risk profile*

Will private organisations be expected to use HISF? Would they be in error or a weaker position if they used another guiding framework for health security or information risk management? Agencies should select the framework that best caters to their activities. It is possible a stricter use of NIST (or ISO etc) is a better fit. The scope, intended use and objectives of this framework continue to be unclear with this statement.

- *acknowledge their obligations, assess themselves and share their level of maturity allowing Correction: ~~the~~ Te Whatu Ora / Health New Zealand and other key stakeholders such as Primary and Secondary Health Care, to measure and manage security uplift.*

We are unsure of the interaction/scope with the above. This needs to be clarified.

HISF’s development pathway consists of the following seven foundational building blocks.

We note four of the 'building blocks' have been defined in the HISF approach section. We think there would be benefit in having the other key concepts/terms defined and set out early on. The way this has been structured/presented is too complicated making it difficult to understand how everything fits together.

Recommend: Section 5 be re-named Key definitions (instead of 'HISF approach' which muddies the water), with Section 6 HISF Framework being the application of the definitions. This would be more straightforward and might save some unnecessary confusion and duplication between Sections 5 and 6.

Fig 2 Structure of revised HISF

*Requirements Guidance as to how organisations **may** comply with each assertion*
This is a nuanced statement. While an organisation may choose to follow the guidance provided or not, in order to comply with each assertion, our expectation is that the organisation would still be required to comply using alternative guidance. Compliance should not be optional.

Foundational blocks

Fig 2 lists seven. However as we worked through the sub-sections we counted 10, including two 6.1.8s. Unhelpful and needs to be corrected.

6.1.1 HISF obligations pg 8

Te Tiriti o Waitangi – is Māori data the same as personal health information?

Confidentiality
Correction: ensure personal health information is ~~only~~ accessible only to those authorised for access.

Integrity
Correction: ensure the safeguarding, the accuracy and completeness of information, its handling and processing. (NB:100% accuracy cannot be achieved but every effort should be made to get close to it)

6.1.2 HISF principles pg 9

Add Recover as 6th principle as per earlier recommendation in Section 5

Correction: *Overall, the principles are designed to ~~reinforcing~~ reinforce the continuous nature of organisational behaviour and practice with respect to information security as well as:*

6.1.3a Segmentation with risk characteristics pg 10

These need to be clearer – definitions and more examples. As presented, Fig 4 is unhelpful/doesn't add value.

6.1.3b Segmentation with maturity characteristics pg 11

Our views differed on this. Some of us do not fully understand what may be generally intended with the use of "maturity characteristics". Although it was acknowledged these may be standardised in other standards and frameworks, we don't believe it is a common approach which is used practically or consistently over time.

Those of us who are more familiar with using maturity frameworks, questioned the appropriate use and definition supplied in the framework. We disagreed with the premise the HISF principles equate to – or infer – any type of information or security maturity, or that they could be appropriately applied vice versa with regards to the HISF principles in their current form.

Maturity tends to be reflected in whether activities are ad-hoc, repeatable, standardised, leading practice (there are some specific frameworks defining these).

We understood the maturity characteristics in Fig 5 are the 5 HISF principles with 'behaviours' added. Fig 5 doesn't add any value.

Introducing new terminology e.g. 'ideal practices' is unhelpful. Regardless, more detail is necessary to support their use and assist understanding.

More confusion arises with the introduction and reference to NHS on page 12: According to NHS[1], *these* ***categories*** *reflect…..* What categories does the framework reference, why and how? It should be transparent this is in regards to the United Kingdom's NHS organisation in the main body of the framework (not just a footnote). More importantly, clarity about what this actually refers to is necessary to understand the intended use and interpretation of this section, and its relevance.

The reference to *Framework Implementation Tiers ("Tiers*") adds further confusion.

Is this from UK NHS? If yes, we still need to understand what and why this is relevant here? It may have some useful aspects but what is its connection to the scope here, and what aspects are relevant for NZ's 2022 HISF? There needs to be some brief explanation / justification for this, otherwise we query its relevance.

6.1.4 Maturity Assessment

Correction: *The HISF maturity assessment scale rating is as defined below according to the extent ~~of~~ to which……. ……being the dominant standard ~~of~~ to which the updated HISF controls are aligned ~~to~~.*

We note this conflicts with the maturity references in the last figures? (although at least this is a maturity scale).

Pg 13

6.1.5 Cyber security assertions

Fig 7

We have reservations about Fig 7. It needs more detail so that users still consider each principle in a holistic and meaningful way. We are not convinced this is very informative from a practical perspective. We are concerned some users may assume this is a holistic assessment/mapping, which it isn't. Did the examples in the white boxes come from a particular source? We suggest Fig 7 be reviewed/revised, further defined and explained for guidance.

The term assertion in this context is simply a checklist to ask the participants how they comply to a set standard. It is about an intent. We ask how organisations comply with the intent versus current outcomes

This is a duplicate. It seems confusing to have to try and distinguish the term here.

Confirmatory evidence for each assertion may be used for compliance, reporting and future planning purposes.

The evidence is used by the individual agency doing the self-assessment or Te Whatu Ora or both?

Correction: *According to NIST, such a framework is designed to provide a listing of functions, categories,..*

Pg 14 Approach

[1] UK National Health Service

Correction: 6.1.6 Requirements - duplicate

6.1.7 Controls – duplicate

6.1.8 HISF mappings to control catalogues

There is some mixed language and phrasing. We understand the intention, but we are not sure this is a standard phrase or term (at minimum within this framework). It may be more appropriate to say “other information frameworks, standards and regulations.” These don’t however, all target security; they are mostly information management. This also needs a definition.

6.1.8 Guidance – duplicate

6.1.9 Tools and templates – 10th building block?

9. Section 7 – Māori Co-design Objectives

Do you have any feedback on the co-design objectives and the approach taken to meeting these aims as outlined in the updated HISF?

As previously stated, we expect Māori Co-design Objectives to appear earlier in the document, preceding the body/detail of the core framework.

We note Māori co-design approach is currently being developed to incorporate Te Tiriti obligations into the revised HISF. When this is completed should we anticipate it replaces, or augments the Māori Co-design Objectives as presented in this draft 2022 HISF; that its place would be earlier in the HISF as we expect?

We assume these form part of the requirements of this framework.

There needs to be further consultation and very specific guidance about how this would look in practice across all segments, and in each segment respectively – it will likely be quite different across private, public, Non-Government Organisation and/or Not For Profits (including charity and community services).

10. Appendix A – Cyber Security Assertions for Districts

Is this appendix easy to read and understand? Y/N

We set out our comments on specific points as follows:

PL-A01 – Governance can be defined in a number of ways that may be broad. This needs to be better specified here. “Senior Executive” should be defined.

PL-B01 – In the absence of some indications or context on what a “clear Information Security Policy, Acceptable Use Policy, and standards” should look like and entail, this is very broad and difficult to measure.

11. Appendix B – Controls and Guidance for Districts

Is this appendix easy to read and understand? Y/N

We set out our comments on specific points as follows:

PL-B03 – We suggest that a "security incident violation" is defined, recognising that there may be some variance based on sector segmentation and that organisations outside of district level may have differing approaches based on size and individual risk profile.

PL-B05 – This appears to mix references such as health devices, health information assets, medical devices, and corporate devices which leads to confusion on scope. We suggest the intent here is at a level that is more aligned with information management/governance than security, and so the content should be reworked.

As part of this reworking, we suggest that the guidance would benefit from sub-headings or breaking up at an assertion/requirement level.

We do not consider that medical devices should be bundled in this control area. The risk profile is different, and they come to market in a controlled manner with other regulatory oversight and assurance. This is distinguished from IT assets which agencies can buy and implement with more discretion.

We suggest moving the final section of the Guidance ("*It is important to note that while many information assets can be owned by in the conventional sense, the notion of ownership of health information is fraught with legal, ethical, and policy-based issues…" through to* the final bullet point) up to the start of the guidance. The inventory content should be set out as standalone content from the overall asset management process wording, to emphasise its importance.

References to data/asset inventories in the guidance should then be scoped to be kept simple and allow for flexibility, recognising that whilst an inventory is absolutely critical, the reality is that from a practical perspective these can be extremely difficult to implement and maintain.

The guidance section later includes commentary on the concepts of ownership and custodianship. We recommend that this section also refers to and ties back to the co-design objectives.

PL-B06 – There may be some overlap between this control area and the earlier area of PL-B05, as media equipment could generally be thought to be included in assets. It is suggested this content is changed to target decommission and disposal for assets and/or data generally.

PL-B07 – Something appears to have become confused here, and it seems the guidance from PL-B07 and RE-AO4 need to be read together. New guidance then needs to be inserted for RE-A04 that specifically addresses the testing element.

PR-A02 – "Confidential information leakage" should be included in the glossary/definitions section.

PR-B02 – Instead of focusing on personnel, it would be better to centre this assertion, requirement and guidance around processes. Rather than a specific people focus, what is key is to have a clear process and a simple tool(s) that enable the reporting.

DE-B01 – We suggest a degree of caution is required in setting out the requirement, in that these need to reflect the uncertainty of possible vulnerabilities or reoccurrence that could happen. In some cases, nothing further may be able to be done or is appropriate – e.g. in the event of human accident; you can't assume more training or awareness is the answer to prevent occurrence or that processes need change (in fact, training or changes may increase short term vulnerability while people re-learn).

RE-A03 -We observe that the guidance comment that the Office of the Privacy Commissioner must be notified of all P1 and P2 incidents within 24 hours places a different obligation on districts from the expected 72 hour timeframe directly stated by the Commissioner in privacy breach guidance.

We also recommend that P1 and P2 incidents are defined.

RE-A04 – We do not understand how this differs from the assertion already under ID-B05. The current guidance seems to fit better under PL-B07. We therefore recommend that the guidance is reframed to specifically focus on the testing element.

RE-A05 – The guidance needs to be refocused on the communication/notification aspects that are sought be addressed here with the requirement. The existing content of bullet points feel like a better fit under PL-B07.

RE-A08 – This guidance again needs to be refocused to emphasise and detail the communication aspects that need to be addressed here. Cross referencing to apply the guidance under RE-A06 has no relevance, as that currently is about evidence gathering. The guidance needs to be consumer/patient specific, not just a re-do of what appears under RE-A05 which relates to customers, suppliers and interested parties. Although the Framework excludes privacy considerations, when discussing notification the mandatory breach notification regime under the Privacy Act 2020 cannot be ignored.

12. HISF Guidance

Should the framework provide guidance for specific health segments, either as:

a) one document (Framework and guidelines together)

b) two documents (Framework in a separate document and all guidelines in one separate document)

c) multiple documents (Framework, guidelines for specific segments in separate individual documents)

d) Other – please comment in the box below:

Multiple documents with the Framework to accompany each set of guidelines for specific segments