[redacted]

From: enquiries@website.privacy.org.nz
Sent: Friday, 18 September 2020 8:31 am
To: Enquiries
Subject: Enquiry form submission (202009180831)

Categories: sent to policy team

* PGP Signed by an unmatched address: 18/09/2020 at 8:31:07 am, Decrypted

Enquiry form submission

First name: Dr Russell
Surname: Wills
Email: russell.wills@hbdhb.govt.nz
Phone: [redacted]

Question:
Email below sent to Sebastian Morgan Lynch 12th August not responded to, see below. Children's Commissioner also has inquired.

Additional comments:
Hi Sebastian, It's been awhile. I trust you are well. Andrew I'd be grateful for your thoughts on this too please.

I have read the new draft Health Information Privacy Code: https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Draft-Health-Information-Privacy-Code-for-consultation-V2.pdf

My interest as you might imagine lies in information sharing when children are at risk. Three rules apply: Rules 10(1)(d) and 11(2)(d), and Rule 5(1)(a) and (b).

Rules 10(1)(d) and 11(2)(d) still has the threshold of "serious threat". This is different to the information sharing provisions of the Oranga Tamariki Act S66 (where the threshold is "wellbeing") and the Family Violence Act. As we've discussed previously, DHB lawyers default to safety, i.e., "No, you can't share that information doctor". I am afraid you are missing an opportunity to put their concerns to rest when it comes to information sharing to keep child and adults victims of family violence safe.

I recommend that the information sharing provisions of the OT Act and the FV Act be added to Rule 10 (1)(d) and Rule 11(2)(d).

I like rule 11(5). Hospitals must have the ability to refuse to disclose information about a child when parents request it, and we believe it to not be in the child's best interests. Good work.

Rule 5, storage and security, also causes us some difficulty. What do "such security safeguards as it is reasonable in the circumstances to take" (5.1.a), and "everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information" (5.1.b) mean? What happens in practice is that we use unsecured/ unencrypted email to share children's personal information with parents, caregivers, schools, NGOs and other ministries all the time. We seek parents' permission and sometimes briefly discuss that it is unsecured. The commonest area it goes wrong is putting the wrong person in the addressee pane, though that is rare. I've never heard of our emails being hacked. The MOH however appears to interpret this section as "Thou shalt never send personal data by unsecured email". This could be clarified by a practice note (your interpretation) or adding a paragraph defining what we mean by "reasonable", i.e., that electronic transmission of personal data should be encrypted wherever possible. Where this is not possible, unencrypted transmission is permitted but the

person whose information is being shared should be informed about how the information is to be transmitted and any risks to that.

Happy to discuss: [redacted].

Viv, FYI. Viv is our HBDHB privacy officer.

Ngā mihi

Russell Wills
Paediatrician
HBDHB

* Privacy Website <website@privacy.org.nz>
* 0xF0CA0E85