**Greater Transparency Needed Around Handling of Patient Data after Hack**

The Privacy Foundation believes lessons should be drawn from revelations that the Wellington, Kapiti and Wairarapa primary health organization (PHO) Tu Ora Compass Health has experienced a large scale hack with potential compromise of patient data. More information on the incident is available at www.compasshealth.org.nz

"While we caution against panic the latest incident is a timely reminder that privacy and security ought to be at the forefront when data sharing platforms are designed and not simply a box to be ticked", says Gehan Gunasekara, the Chair of the Privacy Foundation.

"There is an assurance no clinical records held by GPs have been hacked. This is encouraging but may be insufficient guarantee that patient's personal information is safe.

"For example, PHOs hold enrolment data of patients (such as names, ethnicity, age) and additionally collect and analyse selected data that is sourced from their affiliated general practices such as smoking status, alcohol intake, diabetes checks, screening, depression, immunisations and so forth. This is helpful in improving services but they are also performance measures which inform incentive payments. In the wrong hands, however, they could lead to discrimination, blackmail and even identity theft.

"This is serious, especially as investigations into the most recent hack have revealed historic cyber-attacks and security breaches. It is premature to speculate as to why it was not discovered earlier but these will no doubt be the subject of investigation. Privacy Foundation believes regular monitoring and retention of audit trails ought to be normal practice. It is heartening to see the involvement of the National Cyber Security Centre, Ministry of Health, police, GCSB and the Privacy Commissioner and that there will be a smartening up around security mechanisms across all PHOs and DHBs.

"I understand officials intended to disclose the hack later this month. This also raises questions as to the implications of recent updates to the Privacy Act which, when in force, will require individuals to be informed of privacy breaches involving their personal information 'as soon as practicable'. The present case may provide lessons as to when is soon enough.

"But I believe the breach may well trigger interest from patients about what happens to their personal health information when they attend a GP and/or a health service provided by a PHO. Who has access to their identifiable health/clinical information? Can they get a print out of each access to their information and by whom? There needs to be clarification of what data is extracted from the General Practice Patient Management System for PHO purposes

and whether it has been de-identified or not. Reports suggest it could still be linked to identify individuals.

“The information available to individuals/patients about what happens to their personal health information collected by their general practice is limited and needs to be significantly improved.

“I think we should also expect further updates from the Ministry of Health, Compass Health etc. They need to provide details, to the extent possible, about changes that have been made to strengthen security across DHB, PHO and GP information systems, not just glib assurances that all will be well going forward.”

Gehan Gunasekara

Chair, Privacy Foundation

Contact for media enquiries: Gehan Gunasekara phone 09 923 5218, (021 0743419 mob.); or email: g.gunasekara@auckland.ac.nz

Further information on Privacy Foundation NZ is available on its website: http://www.privacyfoundation.nz