Special: Data Security - Privacy
Proactive Release : 27 July

13 July 2018

[redacted]
Reporter - Investigations
NZ Herald

E-mail: [redacted]

Dear [redacted]

Official Information Act (1982) Request

I write in response to your Official Information Act request dated 19 June. You requested the following information:

- **A list of incidents (since January 1 2016) that your organisation is aware of, in which documents, reports or other materials have been mistakenly left unaccompanied in public** (such as a staff member leaving a folder of material in a café or taxi).

- **For each of the above incidents please provide the following details:**
  - **what material was involved and whether this included any information about members of the public and an overview of such details** (i.e. people's names, addresses, photographs),
  - **the date of the incident,**
  - **where the material was left,**
  - **whether it was recovered and how, and**
  - **what actions took place as a result.**

- **For each of the incidents, please provide copies of any summary reports, documents or correspondence.**

For context, Counties Manukau Health Services provide health services to more than 540,000 people residing in South Auckland, both in hospitals and community settings. We employ over 7,000 staff, and are constantly working to create an environment that respects and manages the privacy of information.

Any incident related to a breach or possible breach of privacy at Counties Manukau is reported via our Incident Reporting System (IRS). It is our expectation that irrespective of the nature and severity, all breaches of individual privacy will be logged in the IRS, and then investigated. We take all reports of incidents affecting any individual's privacy very seriously, and they are all investigated by the service. Staff log an incident report, and self-select from the specific incident type pre-defined for these types of incidents as '*Breach of confidentiality' or 'Breach of privacy'* or where the outcome/ consequence of the incident is classified as a *'possible Breach of Privacy'*. Further narrative detail of the incident is

captured within free-text fields. Under these broad privacy breach categories, there will be a wide range of incidents logged, which reflect a variety of events; for example a toilet-door being opened, photography in clinical areas, or documents mistakenly sent to the wrong recipient. Most of the incidents relate to events within the hospital campus, as part of direct health care delivery. These incidents are typically identified within a relatively short space of time, are reported by a staff member and then investigated.

In the 30 months from January 2016 to June 2018, there were eight incidents that specifically involved unattended documents/ information inadvertently left in public by staff. We have summarised the incident report notes, and the follow-up actions in **Table 1** below.

Incident Date	Incident details (summary)	Response (summary)	Investigation: Contributing Factors	Type of Corrective Actions Taken:	Date of Closure
17/08/2016	**Patient Handover List** found in hospital carpark - contains patient detail and health status/ summary plan for daily care information.	Found by DHB staff member and returned/ destroyed	procedure/ policy not followed	communication process enhanced	19/08/2016
30/09/2016	**Anaesthetic / Surgical data sheets** (8) lost between sites on staff shuttle - contained patient details.	Documents not recovered/ found. Paper records to be replaced by PCIMS electronic data in 2017.	inadequate securing	Areas searched. Staff questioned. education/ training provided	19/10/2016
08/11/2016	**Patient Therapy notes** (3) left unattended in community gym while a therapy session underway with patients.	Notes retrieved after 2 hours unattended - do not appear to have been viewed/ moved in absence. Notes recovered, patients affected informed of breach and complaint process.	[not specified]	[not specified]	21/11/2016
29/12/2016	**USB stick (DHB Research Team)** found by member of public – who contacted the DHB. Contained research staff names/ titles (5), training presentations and meeting minutes/ templates etc.	USB returned to DHB and reviewed.	inadequate securing	education/ training provided	22/05/2017
19/06/2017	**Patient (1) Blood results** report stapled to copy of a training handout - and left at a community health provider setting.	Document found by a Nurse, and destroyed. Letter sent to patient informed of breach and complaint process.	procedure/ policy not followed	education/ training provided	10/07/2017
21/06/2017	**Patient Handover List** found in at hospital entry - contains patient detail and	Found by DHB staff member and returned/ destroyed	inadequate securing	[not specified]	30/06/2017

Incident Date	Incident details (summary)	Response (summary)	Investigation: Contributing Factors	Type of Corrective Actions Taken:	Date of Closure
	health status/ summary plan for daily care information.				
09/10/2017	**Smoke Free referrals** (13) left on train – contain patient referral information (contact details and health)	Documents found by Train Manager and returned in original condition. No indications of public viewing, tampering or any loss of documents. Affected patients contacted by phone & letter - advised of breach and DHB actions taken.	inadequate securing; monitoring inadequate; procedure/ policy not followed;	education/ training provided; Lost property found and returned; process modified/ enhanced	27/10/2017
13/02/2018	Patient Handover List found in at Middlemore train station - contains patient detail and health status/ summary plan for daily care information.	Found by DHB staff member and returned/ destroyed.	inadequate securing	education/ training provided	20/02/2018

Table 1

As context, all details of the incidents are recorded and managed via the Counties Manukau DHB IRS system, and follow the standard procedures, as outlined in the 'Management of Privacy Breach' Procedure document **(attached as appendix 1)**. This aims to reduce the occurrence of these types of breaches, and to conistently manage the notification, response and mitigation steps which are undertaken for any reported (and potential) breaches of privacy arising from the loss of documents.

We take a proactive stance in responding, and for high-risk scenarios take a conservative and comprehensive approach, actively working to notify affected individual(s), where appropriate, and inform them of steps taken in our response to the breach. When an incident is logged in the IRS, the report is automatically sent to the immediate service manager to investigate; and also to Risk and Privacy Manager for review. The service involved will initially investigate each incident, and then implement appropriate remedial action. In all cases, the incident is evaluated to assess the risks to the individual(s) involved/ affected.

Where the risk is considered to be high for affected individual(s), the following scenarios are examples of risk factors that are taken into account in our response:

- whether the information has been found, or is unlikely to be retrieved
- where the breach occurred, within hospital facilities, off the property
- if the information is of a sensitive (clinical) nature, or business (commercial) related
- when and how long the information has been in the public domain
- the number of people who have or could have had access to the information
- the ability of the individual to mitigate or further manage their risk

In most instances, our notification process to affected individual(s) is by either face-to-face or direct telephone contact with all parties involved, followed by written formal notification of the incident and the actions taken to mitigate future similar breaches. The standard template for the notification letter to individual(s) is defined in our 'Management Privacy Breach Procedure' (attached). Our approach may include notification to the Office of the Privacy Commissioner and Ministry of Health, as appropriate.

In March 2016, we appointed a Risk and Privacy Manager, who has focussed on rolling out consistent privacy training to all CM Health staff, creating awareness through increased communication and updating procedures, with the objective of creating a privacy culture of transparency and openness.

One of the key messages has been to improve the visibility of privacy breaches and near misses, using improved and more complete reporting to strengthen our processes. The programme rollout has allowed CM Health to improve both our everyday practice, and the processes required to securely manage and respect personal information. As a consequence of greater awareness, we have seen an increase in the number of breaches reported through the IRS, which has supported greater visibility and the ability to improve our privacy culture.

I trust this information satisfactorily answers your query. If you are not satisfied with this response, you are entitled to seek a review of the response by the Ombudsman under section 28(3) of the Official Information Act.

Please note that this response or an edited version of this may be published on the Counties Manukau DHB website.

Yours sincerely,

Gloria Johnson
Chief Executive (Acting)