Privacy Management Annual Report
July 2014 – June 2015

Central Coast Local Health District (the District) meets its privacy obligations through appropriate governance and the provision of privacy information, training and support to staff. Compliance with privacy legislation continues to be provided by the Privacy Contact Officer (PCO).

The District has taken action in complying with the requirements of the Privacy and Personal Information Protection Act 1998 and the Health Records and Information Privacy Act 2002 by:

- Updating the privacy intranet website.
- Providing privacy information to the public on the new District internet site (went live December 2014).
- Completion of mandatory training through Health Education Training Institute (HETI) Online, Privacy Module 1.
- Providing privacy training, which is available to staff on a one-to-one and group basis.
- Distribution of memos via area communication to educate and reiterate staff’s obligations under privacy legislation.
- The availability of key privacy resources, including the NSW Health Privacy Manual for Health Information, NSW Health Privacy Internal Review Guidelines, Information and Privacy Commission fact sheets, links to legislation via the intranet and the Privacy Information for Patients Leaflet (currently being updated).
- Participating in the yearly Privacy Awareness Week (3-9 May 2015).
- Processing privacy internal review requests within the required timeframe.
- Implementation of a privacy prevention action plan for a proactive approach to prevention of privacy breaches.
- Development of a privacy risk matrix to clearly define processes in regard to the management of alleged privacy breaches.
- The availability of a generic privacy email account and contact number to provide advice on privacy matters for both staff and the public.

The District’s PCO has continued to provide policy and compliance support to the District staff, particularly in relation to electronic medical records (eMR) and access to, and disclosure of, personal health information.

Privacy complaints and issues are addressed as required, either via the complaint management guidelines, the internal review process under privacy law or reviewed and actioned as appropriate.

Internal Review

Privacy law governs all aspects relating to the management of personal and health information held by an agency in NSW. The Health Records and Information Privacy Act 2002 governs personal health information and the Privacy and Personal Information Protection Act 1998 governs all other personal information and provides a formalised structure for managing privacy complaints relating to these acts.

During July 2014 - June 2015, the PCO received two applications for privacy internal review.

- **Date received:** 8 January 2015
- **Privacy principles breached:** Nil
- **Details:** The applicant submitted a privacy internal review request alleging a staff member had accessed and disclosed health information to mutual friends. The applicant alleged that they received telephone calls from mutual friends relaying information about their medical conditions. The applicant had not disclosed this information to the mutual friends and the mutual friends advised the applicant that the staff member was discussing the applicant’s medical information at social events.
The review determined there was no evidence to support unauthorised access or disclosure had occurred regarding the personal health information of the applicant. No further action was taken on the matter.

Further review: Nil

- **Date received:** 6 May 2015  
  **Privacy principles breached:** Nil  
  **Details:** The applicants applied for a privacy internal review as their request for access to medical records for a family member was denied. There were a number of factors that contributed towards this decision including guardianship orders, complications in relation to capacity, opinions of the treating team, and meeting the Districts obligations in complying with the Health Records and Information Privacy Act 2002. The review determined the original decision was accurate and there was no breach of privacy, however this matter is currently with the Information and Privacy Commission for review and comment.  
  **Further review:** N/A

### Privacy Breaches

When the District identifies an alleged privacy breach, the matter is investigated and if substantiated, recommendations are made to prevent similar matters from occurring in the future.

During July 2014 – June 2015, the PCO identified the following breaches of privacy via complaints, internal systems and processes. The nature of these matters and outcomes are as follows:

- **Date received:** 8 July 2014  
  **Details:** Numerous breaches of privacy, in relation to use and disclosure of health information, were identified in relation to a staff member by their manager. An investigation was commenced by Workforce Services and the PCO. The majority of privacy breaches were substantiated. The outcome resulted in the staff member being issued with a first and final warning. Issues were identified in regard to department processes and education and these were included in the recommendations at the outcome of the investigation.

- **Date received:** 15 July 2014  
  **Details:** A staff member was alleged to have looked up their ex-partner and child through eMR. An eMR report was requested and a meeting was held with the staff member. It was determined that the staff member had used eMR to look up their ex-partner and child for non-work related purposes. The staff member was issued a first formal disciplinary warning and was requested to read and sign the NSW Health Code of Conduct and the District Values and Behaviour Charter. The staff member also completed HETI Online privacy training modules 1 and 2.

- **Date received:** 22 July 2014  
  **Details:** An Out of Home Care (OOHC) referral form was placed in the incorrect patient’s blue book. The OOHC referral form contained personal information of a child, their carer’s, birth parents and reasons for coming into care. As a result of this, processes were amended to prevent a similar breach of privacy from occurring. A desktop printer was attached to the workstation of the OOHC Coordinator, secure print folder functions for the multi-function device (MFD) were installed and a hyperlink to immunisation schedules on the desktop of computers were installed to print to the local printer not the shared MFD.

- **Date received:** 4 August 2014  
  **Details:** A staff member inappropriately accessed pathology results through the eMR system for a patient. The staff member admitted to the inappropriate use and apologised. The staff member received a formal warning and was required to read and sign the Code of Conduct and internet policy. The staff member also completed HETI Online privacy training module 1.

- **Date received:** 14 August 2014  
  **Details:** A staff member within Workforce Services sent two different letters of offer (for employment) to the incorrect recipients. It was determined that this breach occurred due to an administrative error which resulted in the letters being sent to the wrong recipients. As a result of the privacy breach, a privacy in-service was conducted with Workforce Services to go through the District’s obligations in relation to the Privacy and Personal Information Protection Act 1998.
• **Date received:** 28 August 2014  
  **Details:** A patient presented to the Emergency Department for treatment and was later contacted by another service of the District. The patient was unhappy as they had not been notified or consented to this service contacting them. This service was unrelated to the reason the patient came into the Emergency Department. Systems were reviewed in regards to this issue and it was determined that better processes in relation to notifying patients that this service may contact them needed to be implemented. A pamphlet regarding the service is in production.

• **Date received:** 1 September 2014  
  **Details:** A complaint was received in regard to a staff member using eMR to look up their late ex-husband’s personal health information. An eMR report was requested and it identified that the staff member had looked up their late ex-husband on numerous occasions. The report also indicated that the staff member had looked up other patients that were not required for work related purposes. The investigation resulted in the staff member receiving a first formal warning, re-reading and signing the Code of Conduct, re-reading and signing the District Values and Behaviours Charter and completing privacy module 1 and 2 through HETI Online.

• **Date received:** 3 September 2014  
  **Details:** Staff reported to their manager that they had witnessed an employee using eMR to look up past patients. Workforce Services, in liaison with the PCO, investigated the matter and substantiated the breaches of privacy. The staff member was issued with a formal warning.

• **Date received:** 3 September 2014  
  **Details:** A previous staff member removed research paperwork (hard copy and electronic) from the District, which included patient health information. The matter was reported to the police. After a lengthy investigation, the hard copy files were returned to the District and the electronic information was located on an electronic database at the District.

• **Date received:** 11 September 2014  
  **Details:** It was reported to the PCO that a personnel record had gone missing from a department within the District. The manager conducted various searches to locate the personnel record however, it could not be located. The staff member was notified their personnel record was missing and could not be located. Advice was provided to the manager from the PCO and Senior Records Officer in relation to the appropriate storage and security of personnel records.

• **Date received:** 26 September 2014  
  **Details:** A claim and Incident Information Management System (IIMS) report was sent to the incorrect manager. The matter was in relation to a sensitive issue regarding a staff member. In order to prevent similar issues from occurring, the process for sending claim and IIMS reports to managers was reviewed and amended.

• **Date received:** 30 September 2014  
  **Details:** Two patients with the same surname attended one of the District’s services and one of them was required to return to the District for test results, however the wrong patient was called back and when they arrived they were given medical information for the other patient. An IIMS report was completed, Open Disclosure occurred between the two patients and they were advised of their right to make a complaint.

• **Date received:** 1 October 2014  
  **Details:** A Nursing Manager advised the PCO that a critically ill child came into the Emergency Department and it was reported that a staff member was inappropriately discussing the patient. It was also alleged that another staff member had looked the same patient up on eMR for non-work related purposes. The staff member who was accused of inappropriately discussing the patient was issued with an informal warning and advised to complete their HETI Online module 1 privacy training. The other staff member, who accessed the patient’s health information via eMR for non-work related purposes, was issued with a first formal warning and advised to complete their HETI Online module 1 privacy training. The staff member advised they accessed the information out of professional curiosity and admitted their error in judgement and understood they had breached privacy.
• **Date received:** 23 October 2014  
**Details:** A Manager provided a reference check for an employee. During the reference check the Manager released personal and health information regarding the staff member's life and health issues. Workforce Services investigated the matter in liaison with the PCO. The manager was issued with a first formal warning and they were required to re-read and sign the NSW Health Code of Conduct, re-read and sign the District Values and Behaviours Charter and undertake HETI Online privacy training module 2 in addition to the mandatory completion of HETI Online privacy training module 1.

• **Date received:** 29 October 2014  
**Details:** A staff member was alleged to have made an inappropriate comment about sexual assault information located within a patient file to a Nurse Unit Manager. Workforce Services investigated the matter and determined the staff member would be issued with a first formal warning. The staff member also read and signed the NSW Health Code of Conduct, undertook the HETI Online Code of Conduct Training and undertook HETI Online privacy training module 1 and 2.

• **Date received:** 17 November 2014  
**Details:** A family member of a patient called the hospital to advise they were unhappy with some of the patient's details being provided to their partner. The family member requested a note to be placed on the patient's file that no information be released. Feedback was received from the NSW Ministry of Health who advised details should not be released to members of the public for patients who have been discharged. Further guidance was provided by the NSW Ministry of Health to assist staff with enquiries on 8 September 2015.

• **Date received:** 2 January 2015  
**Details:** A complaint was received from a member of the public advising a staff member had released their home address to their ex-partner when the ex-partner brought their child into the Emergency Department. An investigation was conducted by the PCO. Registration processes were reviewed to ensure compliance with privacy legislation and the staff member who released the address was identified. The Nursing Manager advised they would follow-up this issue with the staff member when they returned from leave. Current policies and procedures around the registration of patients comply with privacy legislation. It was recognised at the outcome of the investigation that education and improvements to processes would assist with accurate and efficient registration of patients. The recommendations from the PCO were aimed at improving these areas. The recommendations were allocated to the appropriate areas for action.

• **Date received:** 10 February 2015  
**Details:** A staff member identified through their work that another staff member had accessed eMR to look up their child. An eMR report was completed and the staff member was interviewed. The breach of privacy was confirmed and the staff member was issued with a first formal warning. The staff member advised they understood the Code of Conduct and their obligations in relation to privacy. Confidentiality was discussed with the staff member and how they should obtain health information in relation to their child in the future.

• **Date received:** 18 February 2015  
**Details:** A patient contacted the Complaints Department to advise they had been given two different patient's documents, a discharge summary and a radiology result. The matter was investigated however, it couldn't be determined who had provided these documents to the patient. Staff from the relevant area were reminded to check documents when preparing discharge paperwork.

• **Date received:** 25 February 2015  
**Details:** A staff member accessed their relative's health information numerous times via eMR. The staff member advised they felt they weren't getting answers in relation to their relative's care so they accessed eMR to obtain the information for themselves. The staff member was investigated and the privacy breaches were confirmed. The breach of privacy legislation and Code of Conduct was discussed with the staff member and the outcome resulted in the staff member receiving a first formal warning.

• **Date received:** 4 March 2015  
**Details:** A staff member was given the incorrect payroll number and they were able to log into stafflink for another staff member with the same name. It was determined this was an administrative error. HealthShare advised they are investing in automated processes to ensure errors of this nature don't occur in the future.
• **Date received:** 2 April 2015  
**Details:** A staff member found Emergency Department assessment paperwork, for a patient, on the ground in a public car park near the hospital. The staff member who printed this document was identified and the manager advised they would be spoken to regarding the importance of security of personal health information.

• **Date received:** 2 April 2015  
**Details:** The District received a complaint from a member of the public in regard to a family member’s privacy being breached by a staff member at the hospital. The staff member is alleged to have looked up the patient’s health information and spread the details to other staff and relatives. This privacy complaint was investigated and the staff member was interviewed. A breach of privacy was not substantiated in relation to this complaint.

• **Date received:** 7 April 2015  
**Details:** A critical incident occurred in the community involving two seriously injured patients who presented to the District. The incident was posted on Facebook via a community feed and a staff member posted a comment stating they worked at the District and the patients involved in the accident had died. The NSW Ministry of Health were notified. The staff member admitted to writing the Facebook post and Workforce Services issued the employee with a first formal warning. Recommendations for the staff member included; re-read and sign the NSW Health Code of Conduct, undertake privacy training with the PCO and undertake HETI Online privacy training module 2 in addition to the mandatory completion of HETI Online privacy training module 1.

• **Date received:** 8 April 2015  
**Details:** A Nursing Manager produced a FirstNet report on staff that had accessed FirstNet for patients who presented to the Emergency Department involved in a critical media incident. Five staff members were alleged to have used FirstNet for non-work related purposes. The matter is still currently under investigation. The investigation determined 2 staff members accessed FirstNet inappropriately. These staff members were consulted and referred to Workforce Services for disciplinary action.

• **Date received:** 8 April 2015  
**Details:** A Nursing Manager produced a FirstNet report on staff that had accessed FirstNet for a patient who had presented to the Emergency Department involved in a critical media incident. 10 staff members were alleged to have used FirstNet for non-work related purposes. The investigation determined 3 staff members accessed FirstNet inappropriately. These staff members were consulted and referred to Workforce Services for disciplinary action.

• **Date received:** 5 May 2015  
**Details:** A staff member attended the District as a patient and when they received a discharge summary in the post it was for a different patient with the same surname. The staff member was concerned their discharge summary may have been posted to another patient. The matter was investigated and it was believed the administrative error occurred due to staff looking up the patient on the 72 hour list on FirstNet and they found one person with that surname and presumed it was the correct patient. It is unlikely the staff member’s discharge summary was posted to another patient. A process change was implemented where discharge referrals are now only sent electronically to GP’s.

• **Date received:** 13 May 2015  
**Details:** A staff member self-reported to their manager that they used eMR to look up a family member. The employee was appropriately counselled and educated and they completed HETI Online privacy training module 1 and 2.

• **Date received:** 20 May 2015  
**Details:** A patient handover list was discovered by a staff member on a walkway near the hospital. The document included details such as patient names, DOB, medical record numbers (MRN’s) and reason for visit. The area this document came from was identified and the manager spoke to staff about the appropriate handling of patient documents and sent them an email reiterating this.
• **Date received:** 27 May 2015  
**Details:** A patient list was discovered unattended in the conference centre. The document included patient names, MRN's and some medical information. The owner of the list was identified and the document was returned to them. The staff member was reminded they need to keep documents secure especially if they contain identifiable patient information.

• **Date received:** 9 June 2015  
**Details:** A patient claims their ex-partner, who is a staff member, has looked them up on eMR to obtain information for legal proceedings. An investigation commenced and the staff member was interviewed. There was no evidence to suggest the staff member had looked the patient up on this occasion, however the eMR report showed there had been instances in the past when the staff member had accessed the patient’s health information. The staff member admitted to these breaches of privacy. Privacy was discussed with the staff member and the appropriate process for requesting access to a relative’s health information. The outcome for the staff member was for a formal counselling session to occur, for them to re-read and sign the Code of Conduct and complete HETI Online privacy module 2 training. The staff member was issued with a first formal warning.

---

Janine Bell  
Manager  
Date: 1/10/15

Matt Hanrahan  
Chief Executive  
Date: 1/10/15