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 provides ongoing privacy information and support to its staff through:

- The privacy intranet website
- Provision of 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 the privacy legislation
- Availability of a generic privacy email account and contact number to provide advice on privacy matters
- Availability of key privacy resources, including the PD2005_593 NSW Health Privacy Manual - Version 2, NSW Health Privacy Internal Review Guidelines, and the Privacy Information for Patients Leaflet
- Participation in the yearly Privacy Awareness Week
- Resources from the NSW Information and Privacy Commission website
- Mandatory online privacy training through HETI Online

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

Privacy complaints and issues are addressed as required, either as informal complaints handled through existing complaints handling processes, or as formal complaints under privacy law, via the internal review process.

**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 2013 - June 2014, the PCO received four applications for Privacy Internal Reviews.

- **Date received:** 12 March 2014
  - **Privacy principles breached:** Nil
  - **Details:** The applicant made a privacy internal review request because they were not satisfied with the information they received via their application for clinical notes for their deceased partner and because they didn’t receive an answer to their Health Care Complaints Commission (HCCC) complaint. Timeframe had elapsed for a privacy internal review. Matter was managed by releasing a copy of the HCCC response to the applicant and providing another copy of the clinical notes under the clinical notes application process.
  - **Further review:** Nil
• Date received: 6 November 2013  
Privacy principles breached: Nil  
Details: The applicant applied for a privacy internal review as they alleged their employment records had been released to a third party without their consent. The disclosure of the records was in line with privacy legislation, however an apology was offered to the applicant for the misunderstanding and for any distress caused due to the limited communication surrounding the process. The District’s Workforce Services will review its processes around the release of employee information to ensure staff are properly informed about the District’s obligations to communicate with this particular third party.  
Further review: Applicant made an application to the NSW Civil and Administrative Tribunal but this was later withdrawn.

• Date received: 9 October 2013  
Privacy principles breached: Health Privacy Principle 5 and 11  
Details: The applicant applied for a privacy internal review after open disclosure occurred regarding a letter intended for the applicant from the District that was sent to the wrong address. The letter contained health information. The incident occurred due to a typographical error. The letter was returned to the District by the resident at the incorrect address. An apology was offered to the applicant. The District has processes in place for checking correspondence prior to dispatch and communication occurred between stakeholders reiterating the importance of ensuring a client’s privacy, in particular clearly identifying the correct address when producing correspondence.  
Further review: Nil

• Date received: 17 July 2013  
Privacy principles breached: Nil  
Details: The applicant applied for a privacy internal review as they alleged a staff member accessed their dependent’s medical records to determine if the dependent was in hospital. No evidence to substantiate the allegation. The investigation revealed systems are in place to monitor access and security of patient information, however staff were still reminded of their privacy obligations.  
Further review: Nil

Privacy Breaches

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

During July 2013 – June 2014, the PCO identified the following alleged breaches of privacy via internal systems and processes. The nature of these matters and outcomes are as follows:

• Date received: 29 April 2014  
Details: Applicant telephoned the Complaints Department with a complaint regarding their grandchild’s discharge summary. The applicant stated they had been provided incorrect discharge summary as it contained Department of Community Services carer information. The Complaints Department determined that an old discharge summary had been printed prior to the patient being reviewed by the Emergency Department Registrar and it was this document that had been provided to the applicant. The Complaints Department were unable to determine who provided the discharge summary to the applicant. The Complaints Department advised that staff were reminded to be mindful when distributing discharge summaries.

• Date received: 22 April 2014  
Details: HCCC complaint regarding an alleged breach of a patient’s health information during their stay at Gosford Hospital. The patient alleged that their health and sexual health information was discussed inappropriately and that their information was being distributed via staff laptops and mobile devices. The patient was advised that staff do not have access to sexual health information via eMR, however, staff were reminded to be aware of patients proximity when discussing care and treatment to ensure confidentiality is maintained at all times. The patient was advised that the use of personal laptops and mobile devices is prohibited.

Matt Hanrahan  
Chief Executive  
Date: 27/7/2018