Digitising public hospitals

Report 10: 2018–19

Queensland Audit Office
Better public services

Managing data access and security

Data exchange

The ieMR enables information to be exchanged between systems within digital hospitals and with other statewide systems. This allows clinicians to access clinical data recorded outside of the ieMR system. If a patient moves between hospitals with an ieMR (within an HHS or to hospitals in other HHSs), clinicians can easily access their medical records.

eHealth Queensland has designed sufficient operational controls to ensure data can be reliably exchanged between the ieMR and other systems within Queensland's public hospitals.

Monitoring clinician and staff access to patient data

The department has provided clinicians and staff with easy access to patient information in the ieMR (that is, without placing additional restrictions on what clinical records they can access), in accordance with the approved design.

HHSs mitigate the risk of unauthorised access through monitoring and disciplinary processes. This is a reasonable approach, because the risk of denied access could contribute to an adverse patient outcome—even death—while a data privacy breach has far less potential for adverse impact.

The HHSs that have implemented the ieMR have a process for monitoring potential breaches of user access to clinical records and for taking disciplinary action against staff who use their ieMR access to view clinical records not relevant to their clinical duties. However, this process is not fully effective, because there is a gap in the monitoring process. The HHSs do not have a process to ensure the staff appointed to review the user access records complete their review of potential breaches of user access to clinical records.

Each month, eHealth Queensland generates a report for each HHS that shows potential breaches of user access to clinical records. eHealth Queensland sends this report to the HHSs to send to staff to whom they assign responsibility for reviewing the report. If these staff find a potential security breach, they refer it to the HR Workforce Solutions section of the HHS which then investigates the matter and, if necessary, enforces disciplinary action. However, the HHSs do not have processes for following-up with staff who do not review their report of potential access breaches. The process relies on the staff referring matters to the HR Workforce Solutions section.

Preventing unauthorised access to clinical records

Password controls

We found weaknesses with the department's password controls for preventing unauthorised access to the ieMR. While the department offers guidelines to staff on best practice for creating passwords in its Information Security User Responsibilities document, it does not enforce this through preventative technical controls. It relies on detective controls (an internal control mechanism).

eHealth Queensland's detective control alerts it when an ieMR user attempts to guess a password through a high number of unsuccessful attempts. While this reduces the likelihood that an account could be misused, which reduces the risk to the department and patients, the department needs to address the residual risk. Unauthorised access to a clinician's account (through a successful password guess) could have significant adverse impacts.

We are aware that the department is progressively implementing other forms of user authentication. It needs to roll out the more sophisticated authentication approaches with more complex passwords to strengthen security.

Removing user access after employment termination

We found weaknesses with HHSs' employee termination processes for ieMR users. While users of the ieMR system can only access it if they have physical access to a hospital, there is a risk that dormant user accounts created through staff movements (which also have weak password settings) could be exploited by internal users.

The department has a compensating control (if a HHS does not remove a user's access upon termination) to de-activate user accounts after three months of inactivity. As these accounts are linked to clinical data, HHSs should not depend on the department's compensating control. They need to implement a more timely and effective control to terminate user access for employees who no longer require access.