

GPO Box 3123
Brisbane QLD 4001

Level 2
North Tower Green Square
515 St Pauls Terrace
Fortitude Valley QLD 4006

Tel.: 07 3360 6060
Toll-free: 1800 061 611
(in Queensland outside
Brisbane)

Fax: 07 3360 6333

mailbox@ccc.qld.gov.au
www.ccc.qld.gov.au

ABN 32 164 714 360



Crime and Corruption
Commission

QUEENSLAND

Your Reference:
Our Reference:
eDRMS:
Contact Officer:



2 April 2019

TO BE OPENED BY ADDRESSEE ONLY


Chief Executive Officer
Gold Coast Hospital and Health Service

Via email: 

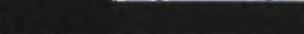
Dear 

**RE: COMPUTER HACKING AND RECENT INVESTIGATIONS AND
DISCIPLINARY OUTCOMES**

I refer to recent correspondence from Gold Coast Hospital and Health Service (GCHHS) to the Crime and Corruption Commission (CCC) detailing the recent investigations and disciplinary findings in relation to two (2) matters involving authorised access to confidential information by staff.

Both matters were subject to oversight from the CCC by way of *Merit and Compliance Review* and were investigated by CSI Specialist Solutions on instruction by GCHHS. The recommendations were accepted and the same disciplinary action taken against each subject officer. Both matters have now been finalised by GCHHS.

The purpose of this correspondence is to address the outcomes of both matters and bring your attention to some concerns of the CCC.


The matter involved allegations against , an Administration Officer in the Gold Coast University Hospital (GCUH)  that  had inappropriately accessed the electronic Medical Records System (eMR) between 1 June 2017 and 27 June 2018.

The investigation found that  had accessed  own medical records as well as that of  two dependents on a minimum of seventy-seven (77) occasions during this period.

 openly admitted to the access, stating the only reason was to see if test results and referrals for  and  dependents were on the file. The reason given by  for requiring this information was to reduce  anxiety levels.

██████████ was aware of confidentiality provisions, policies and procedures and claims ██████████ did not disclose any information to other persons.

The allegations were substantiated and following the show cause process ██████████ was disciplined by way of a pay point reduction (AO3 ██████████ to AO3 ██████████) and reprimanded.

The investigator, ██████████ recommended that GCHHS continue to be proactive in this area of concern and remind staff of their obligations pursuant to the Code of Conduct relating to the use and disclosure of information.

Comment

Separate to the criminal considerations which will be discussed below, we note that the access was only identified following the implementation of the 'P2 Sentinel' software in June 2017, which allows GCHHS to audit who logs on to the eMR system. Potentially the unauthorised access by ██████████ may have been greater than the occasions identified, hence reference by ██████████ that the amount was at 'minimum' 77 times.

Further, the access occurred in spite of the activities conducted by GCHHS to promote awareness about unauthorised access to information by staff. These activities included the 'Privacy Awareness Week' in May 2018 which included warning messages displayed on computer screens to staff.

While at all times this was a disciplinary investigation we do wish to caution ██████████ ██████████ about leading the subject officer during interviews along with the need to maintain impartiality at all times.

██████████ This matter involved allegations that ██████████, also an Administration officer at GCUH had inappropriately accessed the medical records of a child patient between 20 November 2017 and 28 February 2018.

The investigation found that ██████████ had accessed ██████████ grandson's medical records on the Hospital Based Corporate Information System (HBCIS) on 19 June 2018 and separately on the eMR on ten (10) occasions between 20 November 2017 and 28 February 2018. It was also found that ██████████ scanned or uploaded documents to ██████████ grandson's file through the eMR on various dates (x4) between 27 November 2017 and 28 February 2018.

Further it was found that ██████████ accessed ██████████ granddaughter's medical records on the eMR on 7 December 2017 and that ██████████ scanned or uploaded documents on even date.

██████████ reasons for the unauthorised access was due to ongoing health issues experienced by ██████████ grandson, requests by ██████████ daughter and ██████████ desire to ensure reports were uploaded for the use of a treating specialist.

██████████ was aware of the confidentiality provisions, policies and procedures along with the activities promoted during the 'Privacy Awareness Week'.

The allegations were substantiated and following the show cause process ██████████ was disciplined by way of a pay point reduction (AO3 ██████████ to AO3 ██████████) and reprimanded.

██████████ recommended that GCHHS consider implementing the message displayed on the computer screens during 'Privacy Awareness Week' on a full-time basis, to ensure members acknowledge privacy principles upon logon to GCHHS records. The CCC concurs with this recommendation.

Comment

The investigation referred to consideration and corrective action taken by GCHHS against ██████████ Unit Manager ██████████ (UM) ██████████ following allegations arising from this matter. When interviewed

██████████ said that ██████████ had requested ██████████ to access the eMR rather than doing it herself. An audit confirmed that ██████████ did access the records of ██████████ grandson on multiple occasions.

In the show-cause letter to ██████████ it was put to ██████████ that ██████████ had accessed eMR without authorisation. ██████████ admitted that ██████████ incorrectly accessed the medical records on request by ██████████.

The conduct does not appear to have been assessed or considered by GCHHS as constituting corrupt conduct. ██████████ was issued with a warning, which was not considered disciplinary action but a warning against future inappropriate behaviour. No notification has been made to the CCC and it is unclear on what basis GCHHS has made this assessment.

On our view of the records provided ██████████ accessed confidential medical records of a patient in circumstances where ██████████ was not authorised to do so. More concerning is ██████████ did this on the personal request of a work colleague. From ██████████ interview it would appear that ██████████ not only accessed the confidential records but further that ██████████ disclosed information to ██████████.

In our view the conduct does constitute 'corrupt conduct' within the meaning of section 15(1) of the *Crime and Corruption Act 2001*.

We have therefore recorded two (2) allegations of corrupt conduct against ██████████, being of unauthorised access as well as unauthorised release of confidential information. We will record a finding of substantiated on both.

Computer Hacking and Misuse

The consideration and outcome of both these matters has highlighted a concern for the CCC as how GCHHS is dealing with matters which involve unauthorised access of confidential information. This form of corrupt conduct is a continuing area of focus for the CCC.

It is our position that on the evidence the conduct of ██████████ and ██████████ would constitute criminal offending and should have been referred by GCHHS to the Queensland Police Service for consideration. There is no mention of any such considerations on either matters, either in the Terms of Reference to the investigator or in the disciplinary process.

Section 408E (1) of the Criminal Code makes it an offence for a person to use a restricted computer without the consent of the controller. The systems accessed in these matters satisfy the definition of 'a restricted computer' and it is not in dispute the access for the reasons given would not have been authorised. Both officers were aware of the confidentiality provisions, policies and procedures of GCHHS.

Section 408E (2) aggravates the offence in circumstances where the access was intended or done to gain a benefit (or cause a detriment). Benefit is not required to be tangible and there is sufficient authority that mere knowledge would satisfy the element of benefit. That is, where an officer accesses information on a restricted computer simply to gain some knowledge of that information and then does nothing with it they have benefited. Recently we have seen the Queensland Police Service (QPS) prosecute its own officers in such circumstances for the offence of Computer hacking/ misuse.

██████████ has admitted to accessing the eMR system to obtain specific information (test results and referrals for ██████████ and ██████████ dependents). In other words ██████████ gained a benefit, namely knowledge.

██████████ conduct is more concerning in that not only did ██████████ access a restricted computer for a particular purpose, namely knowledge, ██████████ then relied on the information to upload certain records onto that restricted computer. ██████████ intentions appear 'noble', however this is not a defence to ██████████ conduct and would be a matter for consideration by the QPS and/or by the courts.

Moving forward

There has been a recent reduction in relation to the number of corruption allegations received by the CCC relating to misuse of information however it remains an area of focus. Prevention material is available on the CCC website to assist agencies to ensure private and confidential information is secured.

The CCC has recently make specific reference to the misuse of information in the Matters Assessed Report (MAR) provided to agencies and we have requested that where evidence is obtained during any disciplinary investigation which would support the offence, the matter should be referred to the QPS for consideration.

While this reference was not included by the CCC in the MAR for the current matters, it is concerning that GCHHS has classified the conduct as 'inappropriate access'¹. This downplays the seriousness of the conduct, including the potential criminality. We therefore suggest that where appropriate this language be amended to 'unauthorised access'.

We appreciate the recent implementation by GCHHS of the auditing software. However we strongly recommend GCHHS ensure the warning message displayed on the computer screen upon access is permanent. While the recent correspondence does not indicate any acceptance or implementation of this recommendation from [REDACTED] I should note that many agencies, including the CCC, have implemented a warning on their databases.

In the CCC's case all CCC officers have to agree to the following terms at logon before access to the database is allowed:

Access to... is for work related purposes only. Improper access may result in disciplinary/criminal proceedings against you. All access is recorded and auditable.

A further step that the CCC recommends is the issuing of a directive to all staff that such conduct will not be tolerated and may constitute criminal offending. A directive makes is clear to staff that such conduct is not simply a breach of the Code of Conduct but may result in criminal prosecution. This is in line with community expectations and the provisions of the Criminal Code.

The QPS Commissioner has issued such a directive to staff which explicitly states that discipline sanctions for inappropriate access of QPS information that have applied in the past will no longer apply into the future. In other words, a 'line in the sand' has been drawn and it is now the expectation of both the QPS and the CCC that a criminal prosecution is the first consideration before any disciplinary investigation or action is contemplated.

The directive should further make it clear that 'curiosity' or 'personal interest' is not an acceptable reason for accessing confidential information held by GCHHS. There is a level of both trust and responsibility associated with being able to access confidential information and staff are only to access or use such information for an official purpose and that is associated to their duties.

Other agencies that hold private and confidential information, such as Queensland Corrective Service have moved to issue similar directives to staff. The CCC intends to request that all agencies follow this initiative.

Finally, I note that [REDACTED], Director of Integrity Services has had some preliminary discussions with [REDACTED] of GCHHS at the end of last year around similar matters. During those discussions [REDACTED] provided recommendations including how to manage the potential increase in unauthorised access complaints following the implementation of the auditing software, the

[REDACTED]

implementation of the directive mentioned above along with guidance on how to deal with referrals to the QPS and how these allegation types may be dealt with in GCHHS's section 40 directions.

██████████ indicated that the advice from ██████████ would be raised with his Executive for consideration.

Conclusion

With regards to ██████████, ██████████ and ██████████ we have no further requirement of GCHHS and intend to close our files. We would request that this correspondence be brought to the attention of the Statutory Compliance and Conduct Unit for their records.

With regards to the other matters we would appreciate your consideration of the prevention items mentioned and confirmation of the implementation of the recommendations made by the CCC and ██████████. Should a directive be issued we would request a copy be provided for our records.

Of course should you or the Statutory Compliance and Conduct Unit require any further assistance or clarification please feel free to contact me on ██████████ or ██████████

Yours sincerely



A/Assistant Director
Auditor and Monitoring
Integrity Services