CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

CONDUCTED AT LEVEL 2, NORTH TOWER, 515 ST PAULS TERRACE, FORTITUDE VALLEY WITH RESPECT TO

File No: CO-19-1209

OPERATION IMPALA
HEARING NO: 19/0006

DAY 3 - WEDNESDAY 13 NOVEMBER 2019
(DURATION: 1 HRS 16 MINS)

LEGEND

PO Presiding Officer – ALAN MACSPORRAN QC
CA Counsel Assisting – JULIE FOTHERINGHAM
HRO Hearing Room Orderly – KELLY ANDERSON
W Witness – HANNAH BLOCH
LR Legal Representative – N/A

HRO All stand.

PO Thank you.

CA Good afternoon, Chair. I call, Hannah BLOCH.

PO Ms BLOCH, would you prefer to take an oath or affirmation?

W Affirmation, thank you.

HRO Would you stand and repeat after me. I solemnly affirm and declare.

W I solemnly affirm and declare.

HRO That the evidence given by me.

W That the evidence given by me.

HRO Shall be the truth.

W Shall be the truth.

HRO The whole truth.

W The whole truth.

HRO And nothing but the truth.

W And nothing but the truth.

HRO Thank you. Have a seat.

CA Good afternoon, Ms BLOCH. You were provided with an Attendance Notice for today?

W I was, yes.

CA May Ms BLOCH be shown the Attendance Notice.

W Yes, thank you.

CA I tender that.

PO Exhibit 52.

ADMITTED AND MARKED EXHIBIT 52

CA Ms BLOCH, your current position is as Executive Director of People and Corporate Services at the Gold Coast Hospital and Health Services

W That's correct.

CA And your areas of expertise are human resources and industrial and employee relations.

W Yes.

CA You have been with the Gold Coast Executive Team since September 2016.

W '13. Sorry, I've been at the Health Service since 2013, yes, and the Executive team since 2016.

CA Yes. And you have been in Queensland Health for over 10 years?

W Yes, that's correct.

CA And you have partnered with Health Services to lead transformational change?

W That's correct.

CA Did you want just to go into a little bit of detail about that?

W Yes, certainly. So my experience working with Queensland Health has been as both an investigator in the Ethical Standards Unit, leading human resource functions, leading change within the organisation and then more recently at Gold Coast looking after Human Resources, Legal Services and Operational and Support Services, which includes operational areas that provide support to clinical services within the Health Service. And the changes have been both across all of the areas I've worked, but particularly around ensuring that we comply with the industrial obligations around change, designing better work practices and ensuring that we are able to deliver better services more efficiently.

CA Thank you. Has your agency prepared a submission?

W Yes, we have provided two submissions; an initial spreadsheet that detailed a range of our current IT systems and the processes in place and then some further follow-up questions that we had answered.

CA Those were the preparatory-

W -We don't have any introductory submissions.

CA Formal submissions.

W Formal submissions, no.

CA Thank you. May Ms BLOCH be shown the organisational chart for the Gold Coast Hospital and Health Services?

W Thank you.

CA I tender that document.

PO Exhibit 53.

ADMITTED AND MARKED EXHIBIT 53.

CA You are the sole representative from the Gold Coast Hospital and Health Services for the purpose of the public hearing?

W I am, yes.

CA And are you able to speak about all of the areas?

W Largely, yes. Very technical IT questions I might need to provide follow-up information, but largely I have been briefed across the full range of the scope of the terms of reference.

CA Thank you. Would you just like to speak to this organisation structure a little to explain an overview of the Gold Coast HHS?

W Yes, certainly. So Gold Coast Hospital and Health Services provide public health services to the region of the Gold Coast from the New South Wales border right through to out into Mt Tamborine and the northern areas of Coomera. We have three facilities that provide clinical services and a range of community-based services as well.

The design of our organisational structure is to run across the whole service rather than a facility-based model. So we have a layer of executives that take accountability for delivery of services across that whole health service. My role looks after, as I mentioned, Legal, Human Resources and Support Services. So I have within my purview our reporting obligations to the Crime and Corruption Commission around official misconduct, managed disciplinary processes within the Health Service as delegated to me by the Chief Executive. We have an Executive Director of Digital Transformation and CIO role, who is responsible for implementation of our information technology systems within the organisation and driving change. And it was that portfolio that led the implementation of the IeMR in the health service in April of this year, March and April. We then have a range of other portfolios as well within the organisation, so Strategy and Planning that would drive our long-term strategy for the organisation. Operations which is responsible for all of our clinical services within the organisation and Finance, etcetera.

CA Thank you. And what is the number of your staff?

W We have a workforce of slightly over 9,000 fulltime equivalents, but that represents roughly 10,300, although it fluctuates head count of staff across our facilities.

CA And in general terms the type of personal information from the public that you hold?

W So our purse is largely clinical information that we hold for members of the public. We obviously have workforce data and other financial data, etcetera, Government-related information which has various confidentiality levels as well. But largely for members of the public, it's their health information.

CA What do you see is the greatest risks and challenges to managing the private information of, the confidential information for the public?

W Yeah, I think there's two key risks. One as we move into environments that are more based on using information technology, it's managing the cybersecurity risks around that and cybersecurity is one of those issues where you never have a system that is fool-proof, you're constantly having to develop your system and improve against whatever are the latest issues in that area. So maintaining a robust cybersecurity platform. And the other issue I think is culture within the organisation. We have, as we introduce technology there's new ways that staff can access information or it brings to light ways that staff have been accessing information that we didn't necessarily know when we were using paper records. So I think keeping the importance of an ethics-based culture in the organisation where that is front and centre and we're constantly having to remind staff of the importance of maintaining confidential information and that that goes beyond simply confidentiality around patients that they see and go to using the systems in an appropriate way that links to their, you know, that it is relevant to their employment. And we're certainly seeing that emerge as we introduce programs that can audit access, we are seeing this as a new issue that we're having to address in the organisation.

CA And is there someone or a group within your agency where there's regular review of systems processes and people?

W We have a range of groups. So we recently introduced some information governance groups that are particularly looking at the way that we currently manage information within the organisation and privacy is the first principle within their mandate. So that's a group that looks at that.

We also look at it from the perspective of identifying trends in breaches. So as eventually we've, you know, through the introduction of the P2Sentinel report, which I'm sure we'll talk about, we've identified a new issue and so we've pulled together a group that included our Comms, our Legal, our Human Resources to

look at what new strategies we needed to put in place to deal with that emerging risk. And we obviously then would discuss that as an Executive team as well, about a new and emerging risk.

CA So the challenges for your agency with misuse of information primarily at the moment is getting on top of the new system?

W Yes, that's correct, yes. And the new visibility it gives us.

CA Yes, we'll talk about that shortly. Now, with privacy breaches, what impact does it have on your agency's ability to perform its functions?

W Yes, I think we have largely two types of privacy breaches equally significant. One is staff members deliberately misusing access to find information, that it may be about a member of the public or in something where they're making a deliberate act. And that very much undermines the reputation of the organisation and our obligation to the community to safeguard their health information. And the other issue is, as I mentioned, staff accessing their own or family members' information and that's a new area for us that both have the external reputational risk, but also is a challenge in our engagement with staff and the culture of the staff as we start to tackle this issue. We need to do it in a way that we bring the whole workforce on that journey.

CA And the Gold Coast Hospital and Health Services has conducted a recent survey?

W We conduct our survey every two years. Our last one was about18 months ago. We will re-conduct that staff culture survey in March next year.

CA Does it include in part the privacy issue?

W I would have to confirm if there's particular questions in regard to that for you. It does include comments about our values as an organisation. But I'd have to confirm exactly if there's privacy related questions.

CA And what sort of extent is it necessary for the Gold Coast Hospital and Health Service to share data?

W Yes, there is a particular – or there is a need to share data under particular circumstances where we're legislated to do so. Whether it be sharing information when there's been a complaint made with the Office of the Health Ombudsman or those various entities. So there's a legislative requirement to share information. There is, I think, a broader opportunity to share information that would support the delivery of health services, particularly with organisations across the public service who all collect the same type of information, but that's an area that I think is an opportunity. At the moment there's not a lot of sharing of information across those government agencies.

CA And with the new Human Rights Act in Queensland, has your agency considered the impact as of the 1st of January next year and made any modifications to your approach to privacy?

W Yes, we have considered it. There are obviously already legislative requirements to protect health information that already exists. But we are doing a review of our policies at the moment to determine where there might need to be strengthening controls. We're also reviewing our complaints management framework to ensure that consideration of privacy is appropriately represented in that. And we're rolling out training to our senior leaders in regards to appropriate government decision making to make sure that they do ensure that the requirements of the Human Rights Act are considered as part of their decision making.

CA Thank you. And for vulnerable members of the public, such as domestic violence victims, concealing their information and contact details from a former partner, are there any particular protections currently put in place around that more sensitive information category?

W Yes, so we have a social work team, who, within that team are staff who specialise in family and domestic violence and provide a support service to both the organisation and staff managing those cases, but also clients who come into the service. And we would case manage each occasion to determine what action needs to be taken to protect that individual. We're able to use either aliases in our patient administration system, which means if a member of the public was to call up, say to call switch and say please put me through to Joe Blogs in that ward, that patient wouldn't show up in that system, so therefore switch wouldn't find the patient, so they couldn't put anyone through. It wouldn't identify the patient within the service. In other circumstances if there was a particular concern about a staff member in the service then we would be able to manage the care in a way that we would protect them as much as possible.

CA Now, the Commission has collated some data from the seven subject agencies, and I'll just show you four pages of that. There's four tables.

W I think I have that one.

CA Three graphs. Yes, you have probably already been provided with a copy.

W Yes.

CA I tender that document.

PO Exhibit 54.

ADMITTED AND MARKED EXHIBIT 54.

CA And that's the information that is reported in section 38 of the Crime and Corruption Commission Act.

W Correct.

CA And on the last page we've used the annual report figures for the populations for 2018-2019. So on the first page there's an a number of allegations. We'll go to the second page which is the actual number of complaints. And you see there that from four years ago 2015/2016 there were four complaints and it has risen to 11 in 2018/2019. For those previous three years it was pretty steady, four and then five, there's been a sudden jump. Is that in direct correlation to the new system?

W That's correct. So the new report that we've provided, the P2Sentinel report, we're able to identify staff accessing their own record or a family members record and that has resulted in an increase in cases being referred to the Crime and Corruption Commission.

CA And then on the last page there's the proportional breach. Yours is 751. We've got Education way ahead in the lead there at 1,993. And then the Police are the highest, 75. And then, yes, so sort of to give you an idea where you're showing up. I just want to go to Education first of all, a little bit more detail. In your responses which you talked about earlier for our information gathering process prior to the public hearings, you said that there had been a 12 month privacy awareness campaign which started this year.

W That's correct.

CA Was that in response the sudden spike in breaches as a result of the new system which we'll talk about shortly?

W Yes, it was. And we particularly tailored the messaging around access to your own information and the potential consequences insofar as criminal referrals to the police, potential therefore imprisonment or whatever the outcome may be, disciplinary action, etcetera. So we really tailored the messaging in that program around not looking at your records just as much as treating records appropriately. We also had another instance where an administrative officer had asked someone to confirm their identity by mentioning, "Is this still your address?", instead of the reverse being, Please tell me your address." So we also tailored our messaging around the appropriate way to confirm identity. And the program also included educating patients as well around the reasons why we ask particular questions every time they enter the hospital and the importance of us confirming their identity for privacy reasons.

CA You've prepared a fact sheet for patients on privacy?

W Yes.

CA An FA?

W FAQ, yes.

CA Yes. Do you want to just talk about that briefly?

W Yes, so part of our range of tools that are available for both patients and staff include answers to frequently asked questions. Patients it was more to reduce frustration out of being asked the same question over and over again. So, yes, and to make sure our staff equally followed a consistent process in that regard.

CA And do you intend to make this a regular awareness campaign?

W Absolutely. I think at the moment while we continue to see instances of people accessing their own record coming through we will continue to do that. Our information and education in relation to patients may shift, particularly with the introduction of the Human Rights Act to more of a rights-based focus around their right to privacy and other rights, and so we may broaden that campaign. But for staff we will continue our program. We actually have a new program that we're about to release which is where the catchphrase is "Our lips are sealed", so we're going to roll out a new wave of messaging for staff around that importance of confidentiality.

CA And what format what will that take?

W So that will include posters, blogs, lip gloss for staff that has got clearly marked on it "Our lips are sealed" to hand out to staff, for any way to capture the attention, we have internal message boards, we have communication briefs that we distribute through the organisation. So we will use all of those tools to be able to remind staff of the importance of confidentiality.

CA And in relation to training, in your responses pre-public hearings, you mentioned that not all training is recorded in relation to participation.

W So some face-to-face training may not be captured if it is delivered in an information-sharing type way. So we do encourage work areas to have, you know, lunchtime tool box talks around particular topics and we may not capture that information. We do capture all of our staff who participate in the orientation program and we deliver privacy messages and the importance of privacy there. All staff undertake the ethics, integrity and accountability training and then all staff who need access to our data systems have to undertake particular training and we capture the data in relation to all of those training programs and their frequency that they're undertaken.

CA And do you have specific training in relation to information privacy called information security 101?

W Yes, we do and that's mandatory for all staff.

CA Annual?

W Yes.

CA And is it assessed?

W Yes. So after each module of the training you have to complete an assessment and complete that at 100% before you can move onto the next module of the training.

CA That's online?

W That's online, yes.

CA Is anyone monitoring compliance with the mandatory annual training?

W Yes, so we report with compliance with mandatory training as part of our divisional performance meetings to see where compliance is up to and that would then be reviewed as part of our quarterly HR. We produce a quarterly HR report for our Executive and Board around how we're tracking around a range of culture initiatives, work health and safety, and mandatory training is included as part of that.

CA Does that information privacy specific training include, as you said previously with the privacy awareness, the entire range of potential sanctions that flow?

W Yes, that is in the training. And so it's in the information privacy training and it was also included as parts of our IeMR training. So for any of our system access, so IeMR, ESM, all of the connected systems, it's the first thing that's addressed in that training with staff is the requirement for confidentiality, what that means and the potential consequences if you breach that. And we, as part of our role out of IeMR we put all our staff who have access to the system through that training from January to April this year and they weren't given access until they completed that training.

CA Just moving onto sort of a similar topic, a slightly different, prevention, specifically aimed at prevention, even though Education is, Mackay Hospital and Health Services was here yesterday, they're the other subject Health, and they have started using de-identified, quite well-structured detailed case studies as a preventative tool. Do you have that? Or have you heard about it?

W We don't currently do de-identified case studies but we do recognise that it would be a very valuable tool. There would be benefit to that being done, I think to be shared across all of Queensland Health, just due to the volume of cases and the ability to, therefore, if it is not, you know, this happened in Gold Coast Health, is also is less likely to identify a particular staff member. So that certainly would be a beneficial strategy.

CA So for the Department of Health if they would agree to initiate in that-.

W To correlate.

CA It would be welcome at your agency?

W Yes, it would.

CA Now just looking at policies and procedures, you have the IeMR, and we'll talk about what that is shortly, you have what's called the General Business Rule?

W Yes.

CA And is that regularly updated?

W It will be regularly updated. The system was only implemented in April this year, so we haven't hit a review period for that, but yes, it will.

CA I've got the General Business Rules March 2019 Version 1. That would be why it's-

W That's correct.

CA And if Ms BLOCH can just be shown the General Business Rules.

W I have a copy.

CA I tender that document.

PO Exhibit 55.

ADMITTED AND MARKED EXHIBIT 55.

CA If you just turn to pages 6 and 7. The first page talks about introduction, Code of Conduct, and then talks about confidentiality. And then the next page it says, "Prior to viewing and printing clinical information you should consider your obligations or limitations under", and then it says, "Code of Conduct, Hospital and Health Boards Act, Mental Health Act, Privacy Act, Public Health Act." Given what we've just had a discussion about when you're updating this would you have a view to putting in the Criminal Code?

W Yes, we would. That would be, yes, a positive change.

CA And then further down the page, "Consequences of a patient confidentiality breach, the consequences are severe, you could lose your job." And it says, "Mandatory reporting to the Crime and Corruption Commission." And then

further down it says the Health Ombudsman. It doesn't mention referral to the police. I take it'd be amended in that direction as well?

W Yes, definitely.

CA Thank you. Now, just turning to the information security that has caused a sudden spike. So you mentioned P2Sentinel. For the purposes of the public hearings we're focusing on the main database, the databases that hold the main, the most amount. So that's IeMR for you now since March 2019. And the way that that is audited proactively is by the P2Sentinel?

W That's correct.

CA Do you have the eHealth Queensland P2Sentinel fact sheet, or do you want us to show you a copy?

W If you've got a copy, that would be great, thank you.

CA I'll just show Ms BLOCH a copy of Exhibit 42.

W Thank you.

CA We've already heard from Mackay yesterday. I don't know if you were able to listen in?

W Yes, I was.

CA So rather than reiterating what was said then, if you have anything additional to say in relation to the workings of it at your Hospital and Health Services different from-

W Yes, so the only difference is we actually get the report on a weekly basis rather than a monthly basis. And we do that because we find it more manageable. It is a quite comprehensive report and it is a challenging process to validate the information or the access that's contained it in. And we find that getting it on a weekly basis makes that more manageable.

CA But you still have a massive back log don't you?

W We do, yes.

CA Yes. It's currently, from our information you've provided us, I'll just show you what you provided us.

W Yes.

CA So we can go through it, the table.

W Thank you.

CA I tender that document.

PO Exhibit 56.

ADMITTED AND MARKED EXHIBIT 56.

CA Is this the correct information in here?

W As at yesterday the update was for the 2017/18 approximately 1,350. So we have made some headway there, but roughly accurate.

CA So Mackay have had IeMR for about a year, I believe, more than you. And they have about 1,000 breaches. But you'd agree that it looks like quite a back log there?

W It does, yes. So we're at the point now where for new reports coming in we can finalise the assessment of those in three to five days. So we're keeping on top of the new work that's coming in.

CA And you're leaving the old work?

W That's right. And then getting to the old work as possible, but trying to keep on top of the new breaches. But, yes, there is a considerable amount of work to get through.

CA So just to read it out into the record because we're having a discussion about it. So currently there are 188 outstanding reports of potential misuses of information from 2016-2017.

W That's correct.

CA So that was before IeMR?

W Yes.

CA And then from 2017/2018, again, before IeMR, there's 1,000. So what's your current number?

W Approximately 1,370.

CA And then 2018/2019, 859. Some of those would be from IeMR.

W That's right.

CA Where does the rest of the back log come from, how is that generated?

W Prior to the introduction of IeMR we had a system called EMR. So it was a local Gold Coast Health system that was an electronic medical record. So similar to the current one, it just wasn't integrated with the rest of the State. So the P2Sentinel reporting, in my understanding, came in in June 2017, they started to be able to produce that type of reporting. So some of our breaches that we're able to report on when we introduced in the Health Service were access to the electronic medical record. As we've rolled out now the integrated electronic medical record we have breaches in that regard as well. So that's what we're working through.

CA So Mackay had said yesterday the Department of Health, they're the controller of IeMR, aren't they?

W Yes. eHealth Queensland, which is part of the Department, yes.

CA So Mackay yesterday said that to get rid of their back log an estimated one fulltime person for a year sitting there, going through it in an efficient manner, they're just there doing it, would be the solution to their back log problem if the Department of Health could provide one fulltime person to Mackay Hospital and Health Service. Do you have any estimation of how much manpower would be able to work through that?

W We haven't done any sort of calculations to try and estimate what that work would be, other than to comment that we have slightly more than Mackay Health Service. So if they've done that on a reliable calculation, then we would have slightly more. It would take us slightly longer, but, yes, we haven't done any calculation.

CA Would it be a welcome offer from Department of Health to come in to tidy up these breaches flowing from the system that they control and have given you to use?

W Look, we certainly wouldn't be opposed to any additional resources to work through the back log. It also would probably be helpful to have work done on the actual report that's provided so that it becomes more sophisticated and less complex as well.

CA I'll talk about that in a minute. I'll just talk about the back log. So with the back log that's from quite some time ago, getting on almost four years, and I'm taking it that those breaches, those staff they're still using the system?

W They are, that's correct, yes.

CA So there's a risk?

W There is.

CA Okay. Now you mentioned the reports, they're difficult to deal with, is that because they give you what's called raw data?

W Yes, so some of it is that it's a very comprehensive report because it is the raw data, but also the team who analyse it for us, the Health Informatics team have reported that there is some challenges in the way that it pulls through certain pieces of data and it doesn't necessarily connect with pay roll data, for example, very well. So when they try and validate the data that's coming through there can be missing data or data that doesn't necessarily align. So it is a very onerous process to try and go through and validate each access to determine if it was appropriate and in the course of their duties or not. And that's where they've found it quite challenging. And we have had two scenarios now where information has been sent to our HR team on the basis that they felt it was an inappropriate access and when we've issued show cause letters to the staff they actually were appropriate accesses in the course of their duties and obviously we don't want that to happen frequently. That's not a good way to treat our staff. So there is concern around the ability to validate that data accurately.

CA And Mackay talked about putting more sort of indications in the automated system so that the machine does more of the deciphering before the report issues, and that that has resulted in less reports to go through. Did you-

W -That would be very welcomed if that level of sophistication could be built into the system, as well as some type of, you know, alert so that the moment you looked up your own records you were sent an alert to say, "You're can't do that" or the ability to get that immediate action.

CA Mackay have that, they call it VIP. They've managed to put it that on their system.

W Yes, so the VIP capability is rolled out. We haven't had to test it as yet because we haven't had any VIPs. It alerts the person that they're entering an area that they, you know, a flag that it is a VIP, but unfortunately doesn't tell anyone else for us to be able to action it. So even if that functionality actually alerted someone to say, you know, this record is being accessed or gave us that ability that would be helpful.

CA But it is still an extra layer of protection-

W Yes.

CA -for the more sensitive spectrum of the public for those alerts to flash up?

W It definitely is. And we can – can audit up particular patient's file as well. So if we had a particular high-risk case where we were concerned about access, we can access a report of all the people who have accessed it and determine if that access was appropriate.

CA With the VIPs, Mackay have put in the VIP category all domestic violence cases and high-profile persons. I take it that your agency is able to do that?

W We are able to do that. And we could -- we definitely have high-profile people under our VIP. As for others, we would assess on a case-by-case basis, so it would depend on the individual's circumstances.

CA Would you agree that domestic violence victims, in particular where they have orders protecting them from their ex-partner, is a category of sensitive information that would require extra protection, such as being put in the VIP category like Mackay do?

W Yes. I think any way that we can potentially protect the people in those vulnerable situations would be positive.

CA So would you-

W To take that on board, yes.

CA -going forward from now, particularly ahead of 1st January next year, have a view that you take that back to your agency to look into?

W We would, yes.

CA Now, Mackay also have audits. I'll just check. With your auditing, how often do you do audits? Because the proactive P2Sentinel is-

W Weekly.

CA -surname only-

W Yes.

CA -so that's not to capture if they're looking up someone unrelated to them.

W So we, at the moment, the – we run the – have the P2Sentinel reports weekly, and access to anyone else's record would be done based on a complaint received by the service. So, if we received a complaint by a member of the public, or a staff member that someone had accessed their record inappropriately, then we would undertake an audit of that file as part of the management of the complaint.

CA Other agencies regularly audit -- conduct audits of the logs. Would it be possible for your agency to look into, depending upon resourcing and manpower and frequency of it, but at least starting, some type of regular audit, even if it is a random audit or, to start off with, an audit of the VIP category?

W I think the – if the capability was there. And VIPs, yes, where we have – sorry, if we have a VIP that's in the organisation and we're concerned about access,

then we will look at that. The last one that we had of that was – I had only just started in the Health Service and we had a case like that, and we undertook an audit of that particular individual's file to make sure that inappropriate access hadn't occurred.

In regards to others, I don't know the technology well enough to know how we would undertake random audits of the – of patient files given that staff members are involved in a variety of patients' files for legitimate reasons. So I think we'd have to – I think it is a positive idea, we just have to think about the practicality of how to do it, because I don't understand the system well enough to do that.

CA Yes, you're not in the ICT section, but this presumption that -- well, every access is logged, isn't it?

W Yes, that's correct.

CA So if your information technology team is able to, similar to the other agencies, including Mackay, conduct regular proactive manual audits of, other than same surname searches, then that is something-

W That is something we would take on board, yes, definitely.

CA Just moving on to discipline. We've got the response – one of the responses you talked about, the questionnaire, part 5. If Ms BLOCH could be shown that table.

W Thank you.

CA I tender that document.

PO Exhibit 57.

ADMITTED AND MARKED EXHIBIT 57

CA So it is showing -- it goes back four years, the same as every data response we've requested. So 2015-2016 nothing happened. And then there seems to be a spike in activity in 2017-2018 with 14 referrals to either the Queensland Police Service or the Commission, four terminations, six demotions and one post-separation declaration. And then 2018-2019, 13 referrals to the Queensland Police Service or Commission, one termination, three demotions.

So that's sort of – so you do proactively terminate employees when necessary?

W Yes. When appropriate, yes. In the circumstances, we do, yes, take appropriate action for when corrupt conduct is identified.

CA And make police referrals?

W Those matters, I believe, are largely referrals to the CCC. I think we've had only one matter that was a referral to the police service.

CA In what timeframe?

W Across that timeframe.

CA Which timeframe?

W I believe it was '17-'18 that we had one police referral.

CA We'll talk about that in a second.

Now, the breaches, if there is a breach discovered, either through the P2Sentinel software or a complaint leads to a reactive audit, are those breaches dealt with mainly by the line managers, or is there central ability to manage that and records taken?

W So they're all managed centrally. So if there is a breach either identified through P2Sentinel, that would amount to breach of 408E of the Criminal Code or a breach and – a breach of access and a disclosure, then they are all managed through our HR service and undertaken through a disciplinary process.

So they would first go to our statutory conduct service who would assess them for referral to the Crime and Corruption Commission, and then be sent to our HR department who would manage the disciplinary process.

CA And in relation to determinations about discipline and police referrals, do you have any factors, any thresholds that you take any consideration?

W Yes. Insofar as – I'll do police referrals first, if that's okay.

CA Yes.

W And then the discipline.

Insofar as police referrals, if there was any involvement of – any sort of malicious intent or involvement of other people outside of the organisation, then we would use that as a more likely to refer to the police, than an – if someone has accessed their own record. However, we are have had discussions in the organisation that would we consider a repeat offender as a reason to refer the matter to the police also. We haven't had a circumstance yet where that has occurred.

CA In regards to discipline?

W In regards to disciplinary action, so we would conduct a disciplinary process for any substantiated allegations of corrupt conduct. And in the course of the

disciplinary process, we would consider the seriousness of the allegations and any mitigating factors that were put forward by the individual in determining an appropriate penalty.

The general range of penalties that we have applied in circumstances of people accessing their own record have been a reprimand and a reduction in increment for a period of time has been our – has been a penalty we have consistently applied throughout. In regards to people accessing someone else's record, they've been largely the cases where termination of employment has been used. We do see a number of employees leave during the disciplinary process though in those circumstances.

CA Do you pursue post-separation?

W We do in serious cases, yes.

CA What would you classify as serious?

W We can pursue post-separation disciplinary in circumstances where it will be a demotion or termination of employment. So in those circumstances, we would pursue—

CA You do at all times?

W Yes.

CA Okay. And Mackay had quite a detailed threshold, including if, for severity, if there's disclosure.

W Yes.

CA If the records of a domestic violence victim, or – with a domestic violence order, or a high-profile person are accessed.

W Absolutely.

CA And the degree of risk to the health and safety of staff and patients.

W Yes, I would agree with all of those, yes.

CA So for consistency between Hospital and Health Services, would you be open to the Department of Health orchestrating some consistency between Hospital and Health Services with respect to the decisions to discipline and refer to police?

W Yes. I think there is a discipline policy that the Department of Health have that they could potentially include that type of information in as a guide to delegates.

CA Just moving on to a couple of case studies. I believe we let you know which ones we were going to refer to. So it is a de-identified manner we deal with them here, so we won't refer to them in detail. I have prepared redacted-

W Thank you.

CA -material to provide you. So I'll just start with giving you a letter from the Commission to the Chief Executive of your Health Service on 2nd April this year. I tender that document.

PO Exhibit 58.

ADMITTED AND MARKED EXHIBIT 58

CA We'll go through the letter in a bit of detail, but just in summary, this was an access only in relation to a family and the employee. It was an AO3 administrative officer on 77 occasions in June – sorry, over a very long period of time, from June 2017 to June 2018, so a whole year it wasn't picked up. The outcome was a reduction in pay point and a reprimand.

W Yes.

CA And it was detected through the proactive P2Sentinel when that was rolled out.

W That's correct.

CA And it was in relation to the old EMR database. Now, as you see the Commission wrote to the hospital in April this year. And just down the page, the reason given for the misuse of information was to reduce anxiety levels.

Now, here the concern at paragraph 4, on page 2, from the Commission is that the long period of misuse was picked up by the P2Sentinel, but that the misuse could have been more than that. As a result of that concern being raised by the Commission, did, as happens in some other agencies, a more comprehensive audit take place, say, dating back four years before the offending?

W We didn't – we didn't undertake a proactive audit in relation to this particular staff member or others, but we had introduced the P2Sentinel which is picking up breaches from previously. So we're using that data to be able to address circumstances where people have accessed that record – accessed records, noting, however, we do have the back log that we're trying to work our way through as well.

CA If you didn't have that back log, would you be open to the idea, like other agencies – some other agencies do of going back, say, over a period of time to see if there's further offending?

W If there was a way to do it under the technology that could be, yes, something we look at. I think resources would be challenging in that circumstance given the size of the organisation.

CA So just going on to page 3, in the middle where it says "Computer Hacking and Misuse", the Commission noted that there was a concern with your Health Service in dealing with such matters. And the second – the paragraph under that says that a position taken by the Commission was that – should have been referred to the Queensland Police Service. What did your agency do with that information?

W Yes, so we – so we did give consideration to that, and now in our assessment of matters for – when we assess whether they meet the threshold for corrupt conduct, we do make a suggestion about whether it should or shouldn't be referred to the police. We do try and gather the information in relation to the incident through the show cause process first to determine if that would be warranted, because the point of gathering the data through the P2Sentinel we still don't have a lot of information around whether it would warrant referral, and particularly in circumstances where it is a first offender. But we did take on board the feedback of the CCC in giving consideration to that and ensuring that we document in the process when that consideration has been given.

CA And on the next page 4, in the fourth paragraph, there's the suggestion of implementation of a warning message, which is the recommendation, for logon, that it is made permanent. Did that happen?

W We're very supportive of that strategy. We don't have the ability to implement that within the Health Service. So in May we escalated that to eHealth Queensland as a request. And my understanding is it is working its way through the approval and assessment processes there.

CA So when did you refer to that eHealth?

W May.

CA May of this year?

W 2019, yes. Shortly after receipt of the letter.

CA And they still haven't done anything about it?

W That's correct, yes. We do support that that would be an incredibly effective strategy to implement.

CA And two paragraphs down from that, there's a further recommendation that there be a directive issued to all staff referring to the lack of toleration and that – of such conduct and that it may constitute criminal offending. Has that happened?

W We actually put all of our staff who have access to systems through training at that point in time. So we haven't done a written directive, but we did put all staff through face-to-face training where that was made explicitly clear at the start of the training.

CA Other agencies do have their Director-Generals or Commissioners send, from time to time, directives and strong messages via email to all staff-

W We have-

CA -so from the top-down approach. Don't you think that would be a good idea for your agency?

W Yes, we are very supportive of that. We have done staff broadcasts in relation to privacy and awareness. We haven't done a written letter addressed to each staff member in relation to the issue

CA But your agency is open to sending-

W Very much so.

CA -regular emails from the CEO?

W Very much so, yes.

CA And then the next paragraph down talks about the referral to the police, and particularly that it is the expectation of the Commission that criminal prosecution be the first consideration before disciplinary investigation commences. Is that something that your agency, if it hadn't at that point in time, has now taken on board and is doing with every reported breach that you investigate?

W We do – yes, we do take that on board. We – it is challenging, as I mentioned, in regards to the quality of the information that we have at that point in time. The disciplinary process is the vehicle by which we gather a lot of the information around the access, so we have to balance those two. If the quality of the reporting and the ability to validate that information was improved, it would be a lot easier to make that assessment.

CA Now, with police referrals, you said there was one in 2017/2018.

W I believe that was the year, yes.

CA And what was the misuse of information on that occasion?

W It was accessing a patient's record and, in the course of accessing the record, also including falsified entries into the record.

CA Okay. And what happened with that referral? What was the result?

W The – there was a referral to the police. We haven't had an outcome in relation to police investigation, but the person is no longer an employee.

CA So since 2017/18, the police haven't let you know that they're going to charge?

W Not as far as I'm aware, no.

CA Have you had any issues with referring matters to the Queensland Police Service?

W Not in relation to information privacy necessarily. We have had – it has become more challenging in that there used to be a police liaison officer in the Queensland Health, Department of Health, and that really assisted in facilitating the referral of new matters, getting advice from the police on whether it was something that they felt warranted their investigation or involvement, and also getting updates. And it's – unfortunately, that role was, or that office was abolished approximately 12 months ago, so it can be difficult to get updates in relation to progress of matters without that particular liaison role.

CA Now, Mackay are taking a stronger stance in relation to referrals to police. And we had one yesterday - you might have seen when you were watching - where it resulted in termination and a referral to the police in similar circumstances to the one that we've just gone through. I'll just find that.

W My understanding is the case that was spoken about yesterday was the staff member had accessed their staff member's records, as opposed to a family member.

CA The one yesterday was - it is Exhibit 44. Yes.

W Thank you.

CA So that one, you'll see the employee was terminated and referred to the Queensland Police Service. And the facts of that, in summary, as you would have heard yesterday, where there was access only to own records, family, fellow staff and their families. And it resulted in a speedy and quite harsh for the employee, but certainly taking a strong stance. The complaint was received on 30th August 2018. Show cause on 8th March 2019. Temporary transfer and removal of IeMR access whilst the investigation was undertaken on 31st January 2019. Do you do that?

W Insofar as that process, depending on the circumstance of the-

CA The removal of access while investigation is taking place?

W Depending on the circumstances of the case. If it is accessing their own record, we don't necessarily. If it was circumstances of accessing other people's records, or a complaint about accessing a complaint from a member of the public, then, yes, we would give consideration to that.

CA And then suspension with full pay on 23rd May this year. Referral to the police on 24th May this year. Termination on 5th August this year. And referral to the Office of the Health Ombudsman. Would you agree that that is a stronger stance than your Health Service is currently taking?

W I think the factor in that case, that I would say, is almost an aggravating factor for it, is the access to the staff – other staff member's records and their family. In the circumstances where we had that type of access, then we would probably have a similar outcome. For cases where we've been implementing a penalty of a reprimand and a reduction in increment have been access purely to their own or their own family member's record. We haven't had a circumstance of accessing a staff member's record.

CA Okay. Now, just moving on to the second case study, which you were provided with. If Ms BLOCH can be shown the other letter. It is not dated – it is dated at the bottom, I think. February. You're familiar with this particular matter, we've let you know about it?

W Yes.

CA Okay. So just in summary, but then we'll go through parts of the letter.

I tender that letter.

PO Exhibit 59.

ADMITTED AND MARKED EXHIBIT 59

CA This involved access and disclosure.

W Yes.

CA It was a nurse. Looked at her own records. Her sons' records, two of them, and her ex-daughter-in-law over a prolonged period of time in varying degrees of those different types of records, from June until October last year, in relation to the ex-daughter-in-law. I won't go into the other ones. I'm particularly interested in the ex-daughter-in-law.

Now, at the time of the complaint, and again it was by a reactive audit that this information has come to pass, but you've already said that, at the moment, your Health Service doesn't conduct regular audits.

W No, that's correct.

CA From the social worker involved with assisting the ex-daughter-in-law, in an acrimonious separation, where she was [redacted], and she was attending your Hospital Health Service in relation to the [redacted] So she was [redacted]. She stopped using your service [redacted] once it was discovered that your employee, her ex-mother-in-law, had accessed her records, over that prolonged period of time, and given her address to her ex-partner, namely, your staff member's son. Wouldn't you agree that that is a serious case of offending?

W Yes.

CA And that there is a quite high risk of harm. [redacted]. Would you agree?

W Yes.

CA And that resulted in the Health Service not referring the matter to the police despite the Commission saying that there had been a consideration in the evidence and there was sufficient evidence.

W Following the investigation of the matter, yes.

CA There was sufficient evidence-

W Yes.

CA -for a section 408E misuse of information charge to be laid on that staff member by the police.

W Yes, that's correct.

CA But your agency did not refer this matter to the police despite the Commission informing your agency that we have considered it and that there was sufficient evidence. Why did that not occur?

W My understanding of the matter, without disclosing too much information, was it was a very complicated family matter, as you had described. And by the time the matter had – the disciplinary process had finalised, there had been a full reconciliation within the family unit. And that – the final letter we received from the CCC was that they understood it had been appropriately dealt with through the disciplinary process without the referral to the CCC.

I hope I'm not confusing two different matters. We have correspondence regarding that matter. I apologise if I'm confusing two different matters.

CA We'll just look at that letter. Just while we're doing that, in this letter, the redacted one, on page 3 under particulars, and this is a letter to the staff member

from your agency, under e., it says "Computer misuse is an offence and can incur penalties of up to two years."

W Yes.

CA You provide correct information from now on?

W Yes. Yes, we do. We have updated that.

CA Okay.

W Yes.

CA I'll just show you the letter from the Commission that you refer to.

W Thank you.

CA So that's the letter from 2nd May. And in the third to last paragraph, that's where the Commission is saying that there was sufficiency of evidence in their view.

W That's correct, yes.

CA Now, Mackay have initiated a matrix.

PO Can I just ask, Ms BLOCH, you acknowledge that's a letter from the CCC to the Health Service?

W That's correct.

PO Was there a subsequent letter from the CCC to you saying that, in light of the other circumstances, they understood that it was an appropriate matter to deal with only by way of disciplinary?

W It was in that particular letter that the – the follow-on of that paragraph is that "The CCC understands this has not occurred, however, we are satisfied in this particular circumstance the employee shall be adequately dealt with through the disciplinary process and now have no further requirement of the Health Service to report this matter to the police."

PO Okay. So that's what you were referring to?

W Yes.

PO Did you want to tender that letter as well?

CA I tender that.

PO Thank you. That's Exhibit 60.

ADMITTED AND MARKED EXHIBIT 60

PO That was 2 May this year, was it, '19?

CA Yes, this year. And I'll just show you, Ms BLOCH, Exhibit 48.

W Thank you.

CA Have you seen that before?

W No, I have not.

CA So it is from Mackay. They've drafted it. And it is a, sort of, triage from the overload of IeMR reporting. And as you'll see there, instead of them, sort of, turning up stumps and leaving the back log where it is and just working on new stuff, they're triaging all of it. So they've got different banners there. They pretty well speak for themselves; blue being the least serious, and then going to purple. And it talks about the way that they deal with those matters.

Now, the matters that they classify as really important, level 1, they deal with them straight away, very quickly. And you'll see there on the right-hand side, in red, that all matters involving Family Court matters, domestic violence matters, whether a benefit or a detriment, or if an Executive is involved, then that's prioritised straight away, regardless of if it is just, as you say, looking up self or immediate family.

W Yes.

CA So do you see any benefit in that type of triaging, how it would capture instances like we've just talked of where, yes, they're all in family, but they may split up and they may split up from time to time. You say they're all back together again now, but there's instances where people separate and the domestic violence woman does get harmed, severely harm, and, at worst, killed. So wouldn't you say that, as a way to deal with that sensitive information, this type of triaging would be more beneficial for the confidence of the public in the Gold Coast not only protecting their information, but also dealing with breaches in a timely manner?

W Yes, look, I think this would be a very valuable process to be able to implement. I wouldn't have thought that the manner of dealing with the blue, green – well, particularly the blue would have met our obligations for reporting to the Crime and Corruption Commission insofar as even if it is a single instance of looking at your own record, it would still require reporting to the CCC in that circumstance. But certainly a way of – a way of, you know, triaging and dealing with things in a more -- in a speedier way would certainly be welcomed, yes, and it would allow for escalation of the more serious things through an identified pathway.

CA Would you like to take this back to your agency and have some discussions about potentially implementing it in some form?

W We – absolutely. We actually have attempted to develop one ourselves, but were in working with officers of the CCC, were led to understand that we had to report everything through to the CCC and deal with it in that matter. So we would be very supportive of a way of being able to triage and deal with matters in a less formal – less formal way, or a way that allows us to directly engage with staff at a – in a less formal manner.

The other complicating factor is that the view of the Ombudsman is that all of these circumstances identified through P2Sentinel would amount to a public interest disclosure, which also requires an additional level of management around the incidents, so we would have to also engage with that department around a structure like this, and they would feel comfortable that the process adequately met their legislative requirements.

CA Would it be beneficial if the Department of Health was able to and willing to engage in the process of overseeing the implementation of a structure somewhat along the lines of this-

W Yes, I think that—

CA -that would be applicable to all Hospital and Health Services so that there's consistency?

W I think a consistent way of approaching it would be very valuable, and particularly given everyone is at different stages of implementation of the IeMR. So while P2Sentinel is around, to have a consistent method that, if it is rolled out, then across agencies as they go live with the integrated electronic medical record would be really valuable, and it would also allow a high-level conversation with the various agencies involved to ensure that we're meeting all of our requirements.

CA And just a couple of last questions: with the employment of new staff, what type of vetting procedures do you undertake?

W Yes. So our – all new staff have to go through a criminal history check. And the level and extent of that check varies depending on the role that they're going into. There can be additional checks for staff going into aged care environments, etc. We also require blue cards for certain types of staff. We review – do identification checks and checks of mandatory qualification and registration. And we undertake referee checks for all staff as well.

CA And one last question in relation to NPP 4-

W Yes, Privacy Principles.

CA -the Privacy Principles. So that's the obligation on behalf of the agency to protect the information to take reasonable steps to protect the information. And one of those reasonable steps, it could be said, to make the best use of the audit functions, so you have the ability to audit, every access is logged, but currently you don't do any manual auditing, and you've said that there's some resourcing issues.

W Yes. I think the – it certainly would be valuable if there could be a structured approach to how we could identify audits. Even if there was a way to automate, for example, if you work consistently in theatres, but have access to record for a paediatrics patient, or something along those lines, that gave us some routine flagging in the system of expected access, that would certainly allow us to make the use of any auditing function to be more targeted and, therefore, hopefully more effective. So any ability to – in the system to be able to make that more efficient would be very valuable.

And the other thing which we think would be valuable is an automatic flagging – or, an automatic alerting, sorry, that access has occurred so that we can be – particularly if there was a model, such as this framework, whereby one instance of access to your own record is dealt through a conversation. If that was automatically alerted to the individual and the line manager that "We believe you've accessed your own record", and the line manager also received an alert, that type of sophistication in the system would benefit – would benefit our ability to deal with the issues much quicker and hopefully, therefore, prevent these circumstances where people have multiple accesses because it hasn't flagged in the reporting system.

CA Just wait one second.

And with the auditing, if the software isn't able to be installed or updated, and your agency was given sufficient resources by the Department of Health to be able to conduct at least an audit on a regular basis manually, from time to time, even if it was random, even if it was, say, sensitive VIP cases, that that is something you would look to do and see as a reasonable step?

W I would, yes.

CA And also you've said taking on the potential triaging?

W Yes, definitely.

CA And then you're doing your current prevention with education, clearing up the policies and looking into doing some case studies. Is there any other reasonable-

W (Overlapping speakers).

CA -steps you think you could be taking?

W No. I think that covers the types of things that we've identified in the service, yes.

CA So just to clarify, there was a little bit of confusion with the matrix.

W Yes. Sorry, I have only very quickly glanced at it.

CA That's okay. So what it is is that that isn't what Mackay do by way of discipline for these types of misuse, that's how they triage going to look at them.

W Right.

CA This is the pre-looking at them.

W Okay. My apologies. Yes.

CA So that isn't what they actually – how they handle them and the outcomes; do you sort understand?

W Yes. Sorry. I was confused by the email sent to the employee and informal meeting with the line manager, the 'please explain' which is not a disciplinary step-

CA Yes.

W -or the-

CA But that's how they, sort of, triage—

W -they go straight to a show cause process if we believe that there has been a breach.

CA Yes. So they're dealing with the severe one-

W The pre pre, yes.

CA -straight away. And then the other ones are, sort of, put in a queue and working out how they are going to, sort of, look at them before they start really looking them.

W Yes. Right. Understand.

CA Is that clear?

W Yes.

CA Okay. All right, so I haven't got any other questions. Thank you so much.

W Thank you.

PO Mr SCHMIDT?

LR No. Thank you, Chair.

PO Thank you. Thank you, Ms BLOCH. Thanks for coming. You're excused.

W Thank you.

PO Okay, 10 tomorrow?

CA Yes.

PO You've got no-one else today?

CA No, we don't.

PO Okay, 10 tomorrow. Thank you. .

HRO All rise. This hearing is adjourned.

END OF SESSION