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 2 - TUESDAY 12 NOVEMBER 2019
(DURATION: 1HR 27MINS)

LEGEND

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

CA I call Mr FRANCISCO.

PO Mr FRANCISCO, would you prefer to take an oath or affirmation?

W Affirmation.

PO Affirmation, thank you.

HRO Can you repeat after me, please. I solemnly affirm and declare.

W I solemnly affirm and declare.

HRO That the evidence given by me.

W The evidence given by me.

HRO In these proceedings.

W In these proceedings.

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.

CA Good afternoon, Mr FRANCISCO.

W Good afternoon.

CA You were given an attendance notice to appear today?

W Yes, I was.

CA Yes. May Mr FRANCISCO be shown a copy of it?

W Thank you.

CA I tender that document.

PO Exhibit 40.

ADMITTED AND MARKED EXHIBIT 40.

CA Mr FRANCISCO, you are here on behalf of Mackay Hospital and Health Service.

W That's correct.

CA And your role at that agency is as Executive Director of People, and your areas of expertise are human resources management business management and industrial relations.

W That's correct.

CA You've been in that position since May this year?

W That's correct.

CA And previously for the previous three years you are in a similar position at a local Regional Council.

W That's correct.

CA And you've also spent – and prior to that, between 2006 and currently, all of your positions have been in similar roles?

W That's correct.

CA In addition to that, you were a casual academic lecturer at the University of Mackay from 2018 for a few-

W Central Queensland University in Mackay.

CA And you also spent many years from 1985 to 2006 as a lieutenant colonel in the Australian Army?

W That's correct.

CA Your qualifications are a Graduate Certificate Industrial Relations at Griffith University, a Master's of Business Administration degree from the University of Southern Queensland?

W That's correct.

CA A Graduate Diploma in Business from Edith Cowan University.

W That's correct.

CA And a Bachelor of Arts in Politics and History from the University of New South Wales.

W That's correct.

CA Thank you. Has your agency provided a submission?

W Yes, it has.

CA Have you got a copy of that?

W Not with me today, no. There was a number of submissions submitted earlier, responses for information. UI correct that, it was a response for information rather than a submission to the-

CA Yes, so you haven't actually provided a formal submission.

W No.

CA But you have provided information as we've requested it in preparation for the hearing.

W That is correct.

CA Yes. What is your function, if you can go into a little bit more detail at that – at your agency?

W So my responsibility is the executive function for human resources, which is recruitment, employee engagement, health and safety, HR services, which is industrial relations, employee relations, employee investigations, those types of matters. So the broad spectrum of all HR and health and safety matters.

CA And you're able to talk to issues of the workings of the database as well, you're familiar with that?

W That's correct.

CA I'll show Mr FRANCISCO the organisational chart for Mackay Hospital and Health Service.

W Thank you.

CA I tender that document.

PO Exhibit 41.

ADMITTED AND MARKED EXHIBIT 41.

CA To provide the hearing with an overview of the functions of your agency, how you perform them, the types of private information that you have, that sort of global introduction, are you able to do that by speaking to the organisational chart?

W I can.

CA Yes, could you do that?

W So in the – obviously my role I have a responsibility from the HR function side, my responsibility from a data perspective is 100% around people data, so employee data. Marc WARNER who is the Executive Director of Corporate Services he has a responsibility for our ICT systems. So our whole – our ICT systems as a whole, and sitting under that is what we call the digital hospital which has the responsibility for data systems that relate to patient information. As part of the ICT function he also has responsibility for the finance and procurement data systems as well.

The roles of Ms Terry JOHNSON and Ivan FRANETTOVICH as operations roles they have responsibility for the operational staff that utilise those systems from a clinical perspective but also from a people perspective because we have supervisors and clinical directors and so on. Ms Julie RAMPTON and Professor PHILIP REASBECK, they operate from the perspective of controlling the clinical staff. So Ms RAMPTON has the nursing staff. And Mr REASBECK has the doctors. And from a clinical perspective. So not a direct operational line, but managing their technical aspects and how they perform their technical aspects of their duties and how they then interact with the systems that primarily are patient data systems from that process. So globally that's how it works. It doesn't sound very neat, but it works quite neatly from an operational perspective.

CA And the type of information that's confidential for the public that you hold is health information?

W That's correct. So we will hold health information for patients, for the public. We'll also hold confidential information about employees, so things like bank details. We'll also hold confidential information about people who with whom we engage on a commercial basis, so contracts and their banking details and so on. So and then also the last part will be the ICT has a number of infrastructure type information that's protected from the public to secure the security of the system overall.

CA And how could you describe the structure of Mackay Hospital and Health Service in terms of the responsibilities for privacy being one section, information technology, security and information management another, and then another area being ethical standards and discipline?

W So the Chief Executive has overall responsibility for the privacy aspect and

that's executed primarily through myself as the Executive Director People, but each of the executive leads has a responsibility for ensuring that staff that work in their areas have acknowledgement of specific privacy and confidentiality aspects of their work, how that's applied and making sure that the policies and procedures are applied correctly through the processes that we implement through training, retraining, ability for information sessions and those types of things. A lot of those are managed by me from a training technical perspective but delivered by other people within the organisation. And the second part, sorry?

CA So privacy information technology and information management and then ethical standards and discipline.

W So some of our systems are Queensland Health controlled. So from my perspective My HR is Queensland Health system so I have a responsibility for ensuring that we use the locally – so we apply locally the procedures and policies that are associated with that, but I don't control the system itself.

CA Do you get any direction from the Department of Health in relation to that?

W Yes, we do. We have regular advice provided on how that system works, how to make sure that we're doing the correct things. And that's the same that applies for Mr Mark WARNER with using the finance and procurement systems, they get regular updates on how that's to be applied. Whether we're going to do updates, whether there's been recognised as a fault or a security issue around that. So that happens on a regular basis. Mark's responsibility with regards to ICT, because we have a number of mobile devices and BYODs, or Bring Your Own Device-type areas, a lot of those things we get a lot of information around how to make sure that we're protecting information that's held on those or transmitted by those or received by those. So that happens on a regular basis, sometimes some would argue a little bit too regular.

CA And what do you think are the greatest risks and challenges to managing privacy at Mackay Hospital and Health Service?

W The greatest risk from my perspective is that staff can do things that they shouldn't be doing. So the ability for in some systems, from a line manager's perspective operationally they can only see from the My HR perspective they can only see the people that work for them. In some systems that we have, a person can look at everything. And I think that's the greatest risk that they can look at everything whether they need to or not.

CA For the purpose of these hearings we are focusing on ieMR-

W -Yes.

CA -as that's the I believe the largest, or the database that holds the largest amount

of confidential information-

W That's correct.

CA -for the public. So that's the focus of our discussion today. Now, are there regular reviews undertaken about the risks and mechanisms put in place to manage the risks of privacy?

W Yes. The QAO report highlighted the fact that the system was designed for there to be unfettered sharing of information for clinical purposes. One of the risks that we've identified in the processes is that that sharing of information is unfettered. There's not a clinical aspect to it. So, for instance, an admin officer in specialist outpatients can access the data of a patient in ICU even though they may have no clinical relationship with that patient. And that's the risk that we've identified is around understanding when people will have access to information and for what purpose. And we've been doing the audits and reviews and everything else to keep a track of when is that inappropriate access occurring.

CA And do you put controls on so that it is relevant to roles?

W Yes, we've put some controls in place, but a lot of those controls are administrative in nature. They don't physically stop the person from accessing that data, but they provide a warning to that person that they shouldn't be accessing that data. So we do that through training. We take people right through the whole process of what data they should be looking at and for what purpose, what data they shouldn't be looking at and the reasons why they shouldn't be looking at it.

CA With the training do you include information in relation to the entire range of repercussions that could have disciplinary and criminal.

W Yes, we do. We've done a number of training sessions that highlight to people the consequences of their actions. Most recently we've highlighted to people through both the Chief Executive and myself to whole of staff around giving some de-identified examples of consequences to their actions, including highlighting to staff up to and including termination of employment.

CA And to what extent, if any, do you see the impact upon your agency's ability to perform its functions from the privacy breaches that occur?

W The biggest issue for us is that in many instances employees feel there is no consequence to their actions because they haven't seen it. So when I terminate an employee, when an employee is terminated it's not public knowledge, the reasons are not made public for privacy purposes. So employees don't necessarily see that. Or they've got such a strong motivation that the consequences are not seen as a barrier to taking inappropriate access to information.

CA And do you conduct any customer surveys?

W We do conduct customer surveys. At this point in time we haven't had a lot of feedback from customers around the privacy and confidentiality issues associated with the information because I'm not sure they're aware in some instances that there has been a breach and where we have a breach that a customer has advised us of we take that directly as an individual complaint rather than a customer survey.

CA Just going back a couple of minutes you talked about the de-identified case studies. How often do you expose your staff to de-identify case studies?

W So each week my HR services team do a detailed analysis of every case that we're managing, whether it is IMR breaches, harassment, bullying, we do that for two hours, we go through every case, every complaint, every case that we have. For the broader group we've only just started doing the de-identified case studies for the broader groups. They understand the consequences of those action.

CA And how often do you intend to expose staff to those? How many, once a month, once every two months?

W We probably go to the quarterly, only because of the time it takes to go through that information and the sensitivities around the fact that when some people are terminated or action has taken there's appeal processes and so on. So monthly would probably be onerous, but also recognising that we, in de-identifying it, we need to make sure there's a time period as well so people aren't aware that so and so was terminated last month and we're talking about this person next month.

CA We had a criminologist expert give evidence yesterday, Professor SMITH, and his evidence was that, in part, that de-identify case studies including showing the penalties imposed have a positive deterrent effect. So if you could go into a little bit more detail about exactly how you impart that knowledge to staff and exactly what that case study includes, then that would be a useful exercise for other agencies to learn from your pro-activeness?

W So the first one that we did was, and that's the only one so far that we've had, the completion of all the termination processes talked around what the accesses were, why they are inappropriate, how the process was investigated, and we notified what the outcome was, there was termination of employment. So we've identified what the inappropriate accesses were so that people understood clearly the things that we were talking about, so looking at their own staff's data, looking at their own data, looking at other patient's data that they didn't need to. So it's very clear they related it back to the policy. We also noted that in addition to the termination of employment that the matter had been referred to the QPS as well. So the people understood that there were criminal aspects

associated with what they'd already done.

CA Very good. And with the culture of our agency around the misuse of information, you're talking here about a strong stance being taken and made, reinforced very clearly within your agency, who is responsible for driving that culture?

W So the chief executive takes it as her personal responsibility to drive that culture, and she expects that the executive team members will also drive that themselves within their organisation. And I take it as part of my role as being responsible for putting the mechanisms in place about deploying – about creating a workforce culture, that I should be driving that particularly hard with my staff around ensuring that people at all levels understand what's appropriate and what's not appropriate in terms of access.

CA And do what extent is it necessary to share data?

W With other agencies?

CA Yes.

W So the only other agencies we share apart from our reporting to here is with the QPS. And that's where we make a determination based on what are the external links to the activities being undertaken. So we could have somebody accessing data but they're only accessing their own or patients internally. Whereas in some instances is very clearly to other activities external to the Hospital and Health Service that need to be reported as part of this activity.

CA Are you aware that there's going to be a Human Rights Act?

W Yes.

CA Well it has taken effect, but for actions as of 1st January next year.

W I'm responsible for implementing that within the Hospital and Health Service.

CA What approach are you taking to that and how do you think it will impact on your work of your staff?

W I think the biggest impact for us will be understanding around people's data and whether it's being shared appropriately or not and whether people view that as being a breach of their human rights and how those two will interact. A lot of the other things we're looking at is around our unwritten practices within the Emergency Department or Mental Health of things that we ordinarily do that may limit people's human rights and adjusting our policies and procedures to correct that. But I think from am IMR privacy and confidentiality perspective it will be around people understanding what are their rights around their personal information and how it should be managed.

CA I'll just go through some more detailed questions for you, and hopefully you can speak to all of the information technology. If you can't, then please let us know who we could speak to. So there's data analytics and proactive auditing which occurs.

W Yes.

CA And the tool that is used for that is P2Sentinel.

W That's correct.

CA I'll just show you a fact sheet from eHealth which no doubt you're familiar with.

I tender that document.

PO Exhibit 42

ADMITTED AND MARKED EXHIBIT 42.

CA So that's a fact sheet that goes through the basics; is that right?

W That's correct.

CA So would you like to just talk to that and explain a bit more about exactly what P2Sentinel does?

W So for us, I'll address the first point there, the scheduled monthly reports. The first part, the first three dot points are fairly standard across all of the Hospital and Health Services, but what it does for us in that fourth dot point it highlights for us what are common behaviours or common indicators of inappropriate access. So the colloquial name for that first subdot point of excessive person searches by hour is referred to patient surfing, and that's not an uncommon practice for some people who quite literally go looking for different patients of notoriety or for instance VIPs or high profile incidents and so on. And we've now got an ability as part of that reporting if we're aware of it within 14 days we can actually watch the keyboard strokes and the mouse movements in part of that search. So I can tell if that person has accidentally typed in that name, or has deliberately typed in that name and then searched for a specific patient name as part of that searching.

CA Is that something that Mackay HHS has-.

W No, it's is from eHealth.

CA That's directly from eHealth. So all Australian health services are able to do that?

W Yes. And from our perspective that's a key element to giving a better understanding whether that is deliberate looking for a name, or whether it is accidental, which is not uncommon when you've got common surnames and you can see the person is actually looking for a particular name because there's a number of common surnames in the database. Failed log ins is not so much of an issue. That's just people who can't remember their passwords or mistype a keystroke or so on.

But the last two are probably the key for us, the same last name as the patient and the same name as patient are key to us around people looking at their own data or their family's data. We have a demographic issue in Mackay, is that there's a number of large family groups with the same name. We have a surgeon called John SMITH. We also have one of our Executive Directors has a surname of FRANETTOVICH, which you think would be uncommon, but there's like four or five different large family groups with the same surname all from the same region. So even if you tried to filter by region you would still be coming up with a large number of people. So it gives us some element of that, then you've got to go into the individual data sets to check them to see whether you think it is inappropriate or appropriate.

CA So those reports are generated monthly from eHealth?

W Yes.

CA And sent to your agency.

W Yes, that's correct.

CA Who receives those reports?

W Our Health Information Unit.

CA What do they do with that?

W They start doing the basic filtering for us and then highlight to the HR services team where they think they've got an inappropriate access or whether they suspect it could be.

CA And what's the timeframes involved from the date that eHealth gives you as an agency to report to a potential breach being given through investigation to-

W Depending on the workload and the size of the file, it could take three to four weeks just on the amount of data that they to crunch through to have an understanding of that and then the ability for them to have an HR adviser who's available to hand that data over to them.

CA Have you got a back log of reports?

W Yes.

CA And how bad is your back log?

W I would say particularly bad.

CA Particularly bad?

W Particularly bad.

CA Okay. What's your definition of particularly bad?

W So we have breaches or suspected breaches that potentially go back to 2018, but that was when the system was implemented and there wasn't strong policies, auditing procedures and those types of things. So that's – I can't remember the exact numbers on the top of my head, but it is around about 1,000 potential breaches.

CA About 1,000 from 2018?

W 2018. The majority of those are I've looked at my own record or I've looked at the record of my family. So we did table a severity matrix.

CA Yes, we have that. Before we go into the severity matrix, could I just discuss with you, which you mentioned earlier, the Queensland Audit Office report?

W Yes.

CA If Mr FRANCISCO can be shown a couple of those pages and the entire report. I'm just going to refer to a couple of them. I tender that part of the report, pages 39 and 140.

PO Exhibit 43

ADMITTED AND MARKED EXHIBIT 43.

CA So I'm referring to 39 and 40. But if you want us to refer to any other parts that's fine. So there they talk about the problems that have been identified with the proactive auditing of ieMR. So they say that the reports are issued by eHealth and then each month given to the HHSs, and they say that there's a problem, I mean this is obviously talking about all of the Hospital and Health Services, that there's a problem that end, at the smaller entity for actioning those reports and relies on staff referring matters to the Human Resources Workforce Solutions. Can you speak to that in a little bit more detail about how your particular agency has tried to overcome that problem and any learnings that other Hospital and Health Services can have? How long have you had ieMR in place?

W I think it is over 18 months, over 2 years now.

CA Over 2 years.

W We were one of the first sites to implement it. I think what we know now and the actions we are taking now, had we understood those risks when it was implemented I think our back log and our workload around doing the auditing investigations would not have been as bad as what it is.

CA Yes.

W One offer the biggest problems that we have is just the sheer volume of the work. And we've got four people that can do those investigations in addition to all of our other workplace investigations that they do.

CA So what learnings over the last two years have you, from this new system, that other Hospital and Health Services could learn from?

W So we've put in places around - and it sounds very basic, but we've got some pretty uncomfortable screen savers. We've got confidentiality alerts on high profile patients, we've got reinforced training on a regular basis and we've been now been more proactive around advising people of the consequences of the outcomes from inappropriate access. So we've been, in some way describe it is it's much more aggressive around that, as opposed to responding and resolving and moving on to the next one, we've become more aggressive at being public about it.

CA If you could just wait one second. And with the Nurses' Union, have you read their submission?

W I have.

CA You have, okay. Did you want to have a copy of it?

W Well we discussed this before, back at the Hospital and Health Services prior to coming here today.

CA Yes.

W My biggest concern around that submission was it seemed to have a focus on training.

CA Yes.

W And a lot of the submissions and a lot of the feedback I've had said we need more training, more training. And my view is that in the heat of the moment or if someone is highly motivated no amount of training is going to stop that person from saying, "I'm doing this because I believe I'm doing it for a good reason."

CA I was particularly interested in the part where they talk about -- did you want to have a copy of it?

W Yes, please.

CA You have one?

W No.

CA Just down the bottom of page 4. And that's Exhibit 33. They talk about the monitoring of breaches and they talk about the Queensland audit report and identified as a gap in the monitoring process. Is there anything that you wanted to respond to the last couple of paragraphs, in particular in relation to Mackay given that it is just a blanket submission?

W From my perspective when it talks about the process not being fully effective because there is a gap in a monitoring process and they talk about user access UI complete their review of potential breaches, from Mackay perspective a lot of that is to do with volume. There is just so many of these breaches to go through that we've prioritised them on a severity basis-

CA So that's the matrix?

W Yes, that's the matrix.

CA I think we'll have a look at that now. If Mr FRANCISCO can be shown a copy of his matrix, entitled ieMR Inappropriate Access Severity and Actions Guide. Would you like to explain about this matrix how it came into being and what's going on in there?

W Yes. So when I arrived an earlier version of this had been developed to give the staff a sense of try to work out literally where to start, what was the most important, what had the highest risk associated with it. So we went through the process and essentially the blue is the Health Information Unit has told us we suspect there may have been inappropriate access, but we haven't had a chance to review it. The green and yellow were viewed as the lowest risk areas, and from our perspective is the lowest risk in terms of potentially somebody using that information for inappropriate purposes. And as you can see there that's people looking at their own records or that of their family members in a once-off occasion or a couple of times with their family, with consent. So even though they're looking at family member's data with their consent that's not appropriate access.

The more concerning for us is the orange, red and purple. And we've prioritised our work around the purple, which is somebody accessing their data and doing something with it. For instance, a doctor admitting themselves to the Emergency Department, ordering their own scans, ordering their own bloods and ordering their own medication. Which they can do by accessing their own

data. For us that's a big risk and that's the single biggest risk around those categories. The orange and red have a high risk associated with them because we're talking about looking at other people's data for non-clinical purpose for which there's no family relationship, for which we may or may not be able to determine the motivations for. Quite often we find when we start the investigation process those motivations are presented clearly to us in responses from the staff that have undertaken those actions.

CA I notice that in red on the right-hand side under the green and yellow, you also prioritise where there's a same name search involving an acrimonious family law matter or domestic violence matter, in particular. So you have classified that as more sensitive information and warranting quicker action?

W Yes. And we've had a couple of cases where it has been quickly aware.

CA How quickly?

W We've either had a complaint or when we've gone to look at the records of the individual we've checked their personnel records to see what the family relationships are and we've identified there's an ex-spouse involved. And they've automatically-

CA How quickly are those type of prioritised matters where there's a risk of harm, how quickly are they dealt with?

W Almost immediately. So then in those instances, it's not a drop everything, but it certainly becomes one of the highest priorities that they're working on to get the data, get the information, and then establish is there a no-risk. So quite often on the person's record we'll have "No contact" warnings for their personal information, those types of things. They're flags for us that that person may have orders in place, court orders, Family Law Court orders of different types, so that becomes a flag for us so that gives us two things; one if there's some sensitivity with how we approach this, but also means that we need to make sure that we've got all that data as quickly as possible to make an assessment.

CA So that's a triaging of the breaches as they come in and then dealing with the back log when you can.

W Yes.

CA Does the Department of Health provide you any assistance with that process?

W Not directly, no.

CA Would it be beneficial if the Department of Health, the controller of IeMR provided you with assistance to get rid of a back log?

W There's two types of assistance I would prefer from a Mackay perspective: one

is addressing the open gate to information, so allowing people who have no clinical need to review information to be somehow secluded from that. That to my mind would slow down the build-up of the back log and as always-

CA Just in relation to the open gate, at the moment you can't put controls on to lock down the-

W -You physically can't lock some information down. So you can lock a specific record down, but generally the people can access any data that they choose to look at.

CA Sorry, I interrupted you.

W That's okay. And we also then, like all organisations, are faced with a back log of work, additional staff would be great to do that. I've spoken with my chief executive about how to do that and we may be funding another person out of that. We've done an estimation based on the severity matrix, of how many average hours and so on, you know, we probably need somebody for another 12 months who would purely work their way through all of these. We believe that would be highly efficient because the person who was doing this would start to see patterns and be able to take very similar approaches to a number of the breaches.

CA And during this back log, the potential misusers, they still are permitted to access the system, or do they have their access restricted or suspended?

W Depending on where we are in the disciplinary process. Some employees may be completely suspended from work, or they may be suspended from duties or they may just have their access to IeMR suspended. So we teach each on the individual case basis.

CA What about the ones that you haven't got to yet that are waiting in that cue?

W They'll still have their access available to them.

CA They still have their access available. So that's a risk.

W Yes.

CA And you try to mitigate that risk with the matrix, but the optimum solution would be provision of more staff to get rid of the back log?

W Yes, that's correct.

CA From the implementation of the new system.

W Yes.

CA From the Department of Health.

W That would be great.

CA Now you talked about taking a proactive approach to trying to improve the culture and take a strong stance. How long has that been going on for? You've been there since May this year.

W That's correct.

CA Has it been before then or did you-

W -There was an element of providing advice and putting the procedure in place, and it was realised about this time last year putting that procedure in place was a start of a process. My role had only been done part-time by consultants, it hasn't been someone consistently in my role, until I arrived 12 months prior. So it was highlighted to me as a significant risk to me when I arrived and we've worked out the last three months we've been working out being incredibly more proactive than we had been previously. Prior to that it had been a bit not hit and miss, but a bit inconsistent, mainly but because there just wasn't somebody sitting in my role fulltime.

CA From the information you've provided to us, I know you've touched on it broadly, you provided orientation, training about the obligations concerning misuse and so that there's a regular let them know, let staff know there's a regular audit?

W Yes, we do.

CA And you do tool box talks.

W Yes.

CA Discussing appropriate and inappropriate access. How often are those?

W They're monthly. Some work groups do it on a weekly. With the nursing units they'll have a varieties of rosters, so they try to do that on a weekly basis and those topics will be brought up.

CA And then the chief executive officer sends on email detailing the audit process and what's inappropriate and - sorry, what's unauthorised and authorised.

W That's correct.

CA How often does that email-

W -The chief executive sends an email every Friday. And each week we add in a different part of from an HR perspective, around appropriate behaviours in the

workplace including ieMR and privacy and confidentiality around that.

CA And do you have screen savers detailing confidentiality?

W Yes. We've got two, what people describe as uncomfortable screensavers, around the whole peeping Tom concept, around people's personal data, designed to get people aware. Yes.

CA Does all of this structure of providing education and deterrence, does it include the range of penalties for sanctions that can be disciplinary and criminal?

W We do not in the orientation packages so we've implemented that so that people are aware it will be up to and including termination, and also the fact that it will be referred through to the Queensland Police Service. We need to be careful when we talk about up to and including termination that we don't indicate that we will abandon procedural fairness under the Industrial Relations Act. So all of our staff have an entitlement to that, so we need to make sure they understand that they'll still be afforded procedural fairness but the end result could still be termination. We have to be cognisant we're not pre-empting disciplinary action on the basis of the severity of a case.

CA And do you have posters in each ward and non-clinical areas?

W Yes. I know the message is getting out there. I go to different training or different workshops and different parts of the hospital. I walk around and meet staff and people talk to me about it. So they ask me about - they're just astounded that it has actually happened and they ask me about the penalties and people ask, "Do people get sacked for this?" And the answer is yes. So I know that it's reaching out there. The issue will be that person feels that their motivation for doing it outweighs the consequences.

CA And you have a confidentiality of patient and organisational information procedure.

W That's correct.

CA Did you want to see a copy of that or you're fine?

W That should be the one that we sent through. I'm reasonably familiar with that one.

CA Yes. And that in there reinforces the staff that their paper access is also monitored.

W That's correct.

CA Could you explain how that takes place?

W The paper access. If you go into ICU there's still a range of data that's recorded on paper files on large patient. It is like a big drafting easel for patients in ICU. So even though we do low data into ieMR we still have a number of different types of data that's secured on paper and the same rules apply to that. So all the staff know that I can't just go and wander around, and I do visits to every ward. I can't just go around and lift up a chart and start reading it. So they understand it is exactly the same process.

CA And Professor SMITH yesterday provided evidence that for training it should all be recorded, participants recorded.

W Yes.

CA Assessed and mandatory. Are those three aspects part of your training?

W Yes.

CA And on a regular basis? He said every one to two years.

W Ours is every 12 months.

CA Yes.

W And some aspects of our training we want to make more regular than that.

CA Is there a warning message before staff log on?

W Yes.

CA Does that include the range of penalty disciplinary and criminal sanctions?

W No, it doesn't, but it does indicate there will be penalties.

CA Would it be a good idea to add that it can be disciplinary and a criminal - Professor SMITH did say that providing the entire range of possible sanctions had a strong deterrent effect.

W I would only do that if I changed the login screen on a regular basis. It is a lot of information. It you put a poster on the wall, people become aware of it. After the second or third time they've seen it they'll just walk past it and become oblivious to it. I could almost guarantee that 90% of the staff know the logon screen, know what it says, but wouldn't be able to tell you what it actually said after logging in. If you changed the fonts, the colours, made it different on a regular basis then people would pay more attention to that and then I'll put that type of information in there because you've got greater awareness.

CA Professor SMITH did say that if there was some assessment from time to time prior to being able to logon that that would assist in keeping staffing engaged.

W Yes.

CA Is that something you could potentially look into?

W It would be from an eHealth perspective but I would support that. If you put on there things like I know that I should only be accessing patients, tick, that I have access to, tick. I know I could suffer disciplinary processes, tick. It's doing those types of things would encourage people to think about their behaviours when they're in the workplace.

CA Thank you. Now, flags for high-profile persons, you mentioned that before. Is the category entitled VIPs?

W It is.

CA Can you explain other persons in that category and how those flags are put on the system and how they work in practice?

W So the VIP category is probably not a great descriptor of it, but it is high profile patients. So for instance we'd all be aware of the two Englishman who had the shark attacks in the Whitsundays in the last couple of weeks. So they would be considered a high profile patient. It's in the news, people are wondering about it. So we put a confidentiality alert on there. We're working through how our protocol works. So who is the authoriser to put it on. But for both of their files that was on within an hour of their file being created.

CA And you also put it on for domestic violence victims?

W That's correct.

CA And is that a flag every time their private information is accessed?

W Yes, so anytime I type in the ieMR that flag will come up with that flag.

CA And the flag notifies who?

W Notifies the user that they're accessing information that it is a confidential added to it and that they must only have an explicit reason for accessing that data.

CA But it doesn't notify anyone else?

W No, no.

CA Okay. Are you aware that there's supervision from the supervisors to assure that staff don't share passwords?

W We are and we've had a recent case where a supervisor and other members of

the team all stated, "Oh somebody must have accessed that while I left my computer opened", and we treated that with the same severity as them doing it themselves. Because if you leave it open for somebody else to use it is just as bad and if you share your password it is just as bad as you doing it yourself.

CA And in relation to controls over access, the system locks out the user after 90 days of not being used?

W I'd have to check that exact time period.

CA Are you aware of any other-

W -All about the systems close out, so you have to re-log in if you're aware from the desk, I think it is 5 to 10 minutes and that's set in various different locations. Like the Emergency Department, I don't think it has got a log out time purely for the fact that in the Emergency Department they don't want people stopping and keep logging back into systems when they're away from the desk. But certainly when I'm away from my desk or people in other roles, it will log you out and you have to log back in straightaway.

CA And your agency, I believe, is working with eHealth Cybersecurity Group on the implementation of an Information Security Management System?

W Yes.

CA Are you familiar with any details?

W I'm not familiar with the detail of their work, but I do know the intent is to be able to provide a better environment in which the information can be distilled more quickly to what we describe as hot spots or problem areas. So that first name, last name, similarities being able to go bang, bang, a couple of filters, yes, we have got a problem, no we don't. So it is about being about to distil that information. We'll quickly be more aware more quickly.

CA So that would cut down on the number of reports that need to be looked through?

W Yes. And I know also their working out what types of reports do we need and what information is in there. So first name, last name, but if we did date of birth, it would very quickly work out that it is exactly the same person, or we have two John SMITHs born on 1st of March.

CA I have a couple of case studies. You were given some notice about that.

W Yes.

CA You've had a chance to familiarise yourself, if you weren't already?

W Yes.

CA So there's the first one, it involves a letter. If Mr FRANCISCO can – just wait one moment. If you could show him the letter. We're just obtaining a hard copy, but it will come up on the screen for you shortly. Is it there? No.

W I'm familiar with both cases, so if you want-

CA Are you?

W If you've got general questions without me having to read a specific part I should be able to respond for you.

CA Thank you. So the first one relates to misuse of ieMR where the employee looked up family, other staff members and family.

W That's correct.

CA It was access only.

W Yes.

CA It was only access. And the employee was in a supervisory role?

W That's correct.

CA And would be a mentor as well?

W Yes.

CA Do you agree that those positions should be dealt with more harshly than the lower positions?

W Only in the instance where the person breached the trust in the relationship. So that person accessed a record of one of their direct reports, and so that employee now has, like, zero trust in her now new supervisor because she trusted the last one and the last one looked at her records. So from that perspective it is more severe than just looking at their own records, but certainly anybody that's in a supervisory role has a responsibility as a leadership function to demonstrate the right behaviours, more so than those at a lower level.

CA And a formal disciplinary process took place to show cause?

W That's correct.

CA And the actions related – she was initially temporarily transferred?

W That's correct.

CA And access removed to ieMR.

W Correct.

CA And while the investigation went on, the employee was then suspended on full pay-

W That's correct.

CA -four months later. And then at the same time, four months later, there was a police referral in relation to a section 408E of the Code?

W That's correct.

CA And then three months after that, the employee was terminated and referred to the Health Ombudsman and APRA?

W That's correct.

CA That's a strong stance taken on access only?

W Yes. So in that instance, the first report was a complaint by the employee who became aware that her supervisor had accessed her details. All the other access was discovered when we went through that process of what other files has this person been accessing that aren't related to her work.

CA So since the referral a few months ago, on 24th May – if Mr FRANCISCO can be shown the letter. That's the letter which relates to the case study that we've been talking about. I tender that document.

PO Exhibit 44.

ADMITTED AND MARKED EXHIBIT 44

CA Since 24 May, when your agency referred this matter to the Queensland Police Service, have you had any response from the Queensland Police?

W Yes, we have.

CA And what has the response been?

W Say at several points in time during that process, the Queensland Police Service has asked for more information on specific aspects of the detail that we provided, and how we've gone about it, and what have been the outcomes associated with that. But it hasn't, like, been to provide a single report, it has been a number of different requests for different information. They followed up a lot of information on background and context to how that access would have occurred. It is like understanding her role. The actual physical location of

the work. How would she actually physically access the information itself.

CA And you haven't received an outcome about whether she's been charged or not?

W No. I checked on that yesterday.

CA Yes.

W So the Queensland Police Service approach is that once they've decided to prosecute, we'll be notified of the charges that are going to be laid, and what Hospital Health Service personnel may be required to appear as a witness in that case.

CA As of yesterday they didn't-

W As of yesterday, we haven't received any of those notifications.

CA Are you aware of any other referrals to the Queensland Police?

W Yes.

CA Can you detail any other examples of referrals and what has happened?

W So we've had one referral where we had a request from the Logan station around some criminal matters that they viewed that the only way that person could have obtained that information was somebody within the Hospital Service had looked up personal information of patients. So we went through that process. And as part of doing that investigation, we discovered that another employee had also accessed that information. So referred that information to the Queensland Police Service as well. We've also had it where we had a-

CA I'll just backtrack. And so that referral, what happened to that employee?

W That's an ongoing Queensland Police Service investigation.

CA When was that referred?

W That would have been in the July period.

CA This year?

W Yes.

CA And sorry, go on.

W And the next one, where we had an employee identify that they believed their records and their family records had been accessed by other staff members. And when we went through that process we realised it was a complex family law

matter. There'd been claims of information being provided to the Family Court that could only have been accessed through ieMR. And we referred that through to the police as well.

CA When did you refer that one?

W If I recall, that was around August.

CA This year?

W Yes.

CA And have you heard back from them?

W We've asked. On both occasions we've had information requested but nothing around any prosecutions.

CA The other case study relates to two high-profile patients where there were multiple accesses.

W Yes.

CA One of them was over a period of three months, and then the other one was a period of a month.

W Yes.

CA Can you detail what actions happened in relation to those two matters with the multiple offenders?

W Yes. So that was my introduction as to how the ieMR breaches occurred. So when I arrived, I was advised that we'd had a number of these breaches. And at this point in time, we haven't taken further action against the individual staff members. We prioritised some of the other work we had to do over this one. But we've identified that in this case we've had a lot of view-only; multiple people looking at certain patient's information. There's a reputational risk associated with that. But there's – we've identified there's no other further risk associated with those, so we moved it lower down the priority list. So what that identified for us was some of those people may, on the face value, have actually had a legitimate reason to look at those files. And some quite clearly didn't. So you could easily identify who didn't. The ones where they may have, you have to go back and look at why, and was this person in that ward, or that unit at that point in time that that person was actually rostered on and working to establish whether they'd had access or not. And in the instance those – those lists are the complete list of people who didn't have appropriate access to those files.

CA Just going through the policies and procedures, as an example of you informing your staff of the full range of possible repercussions for misuse of information,

I'd just like to draw your attention to Access to Patient Integrated Electronic Medical Records ieMR Procedure. And this is from your response material. This is a document that is updated or reviewed every three years?

W Yes. Thank you.

CA Where the changes in technology, have you considered updating it more regularly than three years?

W Yes. And as a result of providing that response, we've got a plan to go back and review all of our procedures and processes relating to ieMR. And our view is that as we start to increase the auditing function, we intend to update the document to reflect, A, the changes in the auditing, but also then updating the different clauses of the procedures that relate back to that so we can be more refined, but very clear to employees around what things we are able to see and what not to see. So, for instance, the ability that we can see keyboard and mouse movements. I think once employees start to realise that, that will have a big impact on inappropriate access.

Sorry, on that, the three years is our standard. So every time we produce a policy or procedure, it automatically get three years. We need to make a conscious decision to make that less, and we're anticipating that we will in this case.

CA I know that you say you've only been there since May and you've implemented a lot of changes to take a strong stance, however, this document hasn't yet come under your purview to amend, and it doesn't mention referral to the Queensland Police Service.

W That's correct.

CA It mentions the Commission, and the Ombudsman for Health. It also refers to the authorising – it calls it "Policies and Standards" on page 4, and mentions the Crime and Corruption Commission Act, Code of Conduct, Information Privacy Act, Right To Information Act, Hospital and Health Boards Act. Do you consider that moving forward, particularly given the Human Rights Act for action taken after January next year for this document to be updated sooner rather than later?

W Yes.

CA To include specific reference to the Criminal Code and the section 408E?

W Yes.

CA And that a referral can be made to the Queensland Police, because this document was done three years ago before you came on board and starting making your proactive steps.

W We had an intention to do that. And to a degree, our focus with Operation Impala coming in was to work on providing the information for that process. And we're taking a lot of the learnings from that and going, okay, we need to adjust this policy, adjust this procedure, update, update a range of documents.

CA I tender that document.

PO Exhibit 45.

ADMITTED AND MARKED EXHIBIT 45

CA Do you receive any assistance at all with the content or template that you should have for policies from the Department of Health?

W Not from the Department of Health directly, but we do share between different Hospital and Health Services. The main problem is that a lot of the – because we're at different stages of implementation that people are putting their policies in different ways. And some other Hospital and Health Services have, like, an Integrity Unit. We don't have anything like that. So our policies are a bit different to theirs.

CA So that the public can have comfort that wherever they go, whichever Hospital and Health Services they attend that their privacy is protected to the same degree, would it be of assistance for the Department of Health to take a more proactive view with respect to overseeing the Hospital and Health Services?

W I think a high-level policy that encompasses anybody that worked in the Queensland Department of Health environment was covered under the same policy and procedures, and as they're applicable within each Health Service because our Health Services do vary by size and function, but certainly something that covered everybody would be very useful, because then I could know as a consumer that if I go do Townsville, Mackay, Cairns that every staff member that works there, whether they're a direct employee, contractor, a locum or agency nurse, are all covered by the same policy.

CA Yes. Now, the Crime and Corruption Commission data that, as part of section 15 of the Crime and Corruption Act, is provided, section 38, in relation to section 15, is provided by your Hospital and Health Services. We've collated some of the data and you're aware of that?

W Yes.

CA Yes. If you can show Mr FRANCISCO. On page 1 there's the allegations. And then page 2 are the actual complaints. If we go to page 2. Your agency is by far the smallest number of complaints.

W It doesn't feel like it from my end.

CA In 2015-2016 there was one. And then 2018-2019 there were nine. But it has been a sharp increase in that last year. All the preceding three years were one, and then it jumped to nine. Is there any reason for that?

W Access. So as we've implemented ieMR throughout the Hospital and Health Services more people have had access. But also more people are inappropriately accessing that and people are becoming aware. So it's – Mackay is not a big town and it is easy enough for – if I've looked at somebody's record inappropriately to say something that somebody else might repeat it and you'd find out, and that's pretty much why we've had more complaints.

CA If you go to page 3, the sub-type of the allegations are broken up and that clearly shows what you've just been saying, that out of the 64 allegations of the 2018-2019 year, that 59 of them were for access, and then five of them for access and disclosure.

W Yes.

CA And then the last page, for completeness, there is an overall proportional breach. The numbers for the population within each agency being taken from the respective annual reports of 2018-2019. And there it is one in 265. I tender that document.

PO Exhibit 46.

ADMITTED AND MARKED EXHIBIT 46

CA For deciding whether or not to discipline, your agency has prescriptive threshold with certain factors that are looked at.

W Yes.

CA Which include the – please expand on that importantly for the purpose of misuse of information – the degree of risk to the health and safety of staff and clients.

W Yes, so in that instance it is around – if somebody disclosing information about a patient that they shouldn't be that might give bias to treatment, or particularly things we've been talking about, people with mental health issues, people will develop preconceived perceptions about those, or that somebody else might decide that, oh no, I won't support them in doing that. It ends up – what it comes around, if you got client-centred healthcare is that people can unduly people's influence by knowing certain things about people to discourage them from taking appropriate actions with their own health.

CA And also another factor: the impact of the substantiated allegations on the public and client confidence in Queensland Health and Mackay Hospital and Health

Services.

W Yes. So if you knew that people were looking at your health information for no other reason than they choose to do so, or because they're doing it maliciously, most likely people will lose trust in the health system. May very well not seek treatment on the basis that they don't trust that their health information will be protected.

With the introduction of the Federal Government My Health Record, a side bar to it is that Mackay was one of those regions that was the pilot area, so everybody got one, so then all the issues that came about with the protection of information there is people in Mackay are weary about the protection of their health information. So if they believe that the Mackay Hospital and Health Services was allowing people to look at their health information without appropriateness, then people would probably say, "I don't want to go to the hospital. I'll go to Townsville. I'll go to Rockhampton" and which will unduly affect the provision of their health care.

CA And with your discipline procedure for your threshold there is emphasis put on whether the records of a domestic violence victim or a high-profile – with a domestic violence order or a high-profile person's records were accessed.

W Yes.

CA And then also a further factor is looked at is whether there was disclosure.

W Yes.

CA Did you want to speak any more in relation to-

W I think we've covered the domestic family violence and the high-profile aspect already, but the disclosure piece is – it's one thing to look at it and know it, it is another thing to do something with it. And we've had people that we've seen who have disclosed that information, and I'm yet to see what somebody can justify in terms of why they've disclosed that information. Morally they might be motivated because they believe it is the right thing to do. We've had one person describe themselves as a social justice warrior in why they disclosed that information, but from our perspective it is completely inappropriate.

CA For the new employees for job vetting, what procedures do you have in place for that?

W So all of our employees have reference checks, they all do a criminal history check prior to being employed. If they are in specific roles, they might do a blue card, yellow card or a national police check.

CA Thank you. You're aware of the NPPs, the National Privacy Principles contained within the Information Privacy Act, in particular no. 4?

W I'd have to be refreshed on no. 4.

CA Okay, we'll give you a copy.

W Thank you.

CA I tender that document.

PO Exhibit 47.

ADMITTED AND MARKED EXHIBIT 47

CA It talks about data security.

W Yes.

CA In (1) "A health agency must take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure."

W That's correct.

CA This is talking about vicarious liability. And there is a matter currently going before the courts in relation to another agency. So it is a focus of ensuring that agencies are taking reasonable steps. Now, you've identified a need, but an inability at the moment to progress the back log-

W Yes.

CA -to quickly move through your back log and identify that Queensland Health could provide you with additional assistance to do that. And you've also talked about the matrix for triaging the most sensitive information where the risks of harm are greater, to action those quickly, and you do action those quickly. And also about putting flags for vulnerable persons on the system-

W Yes.

CA -where there's more sensitive information to ensure, at least, take as many steps as you can to ensure that their data is as safe as possible. So those are all parts of reasonable steps. And you've stated that you're undertaking as part of this process, a review of the policies and procedures, and you've set in place significant educational and awareness campaigns.

W Yes.

CA Is there anything else that you would like to speak to specifically in relation to reasonable steps?

W I just think that in the starting they've referred to it in the QAR report that the system is designed to share the information. I'm not sure that, from my perspective, seeing the outcome, that the depth of the understanding of those risks where it is not a catastrophic outcome, so it is not life or death, in those lower order risk areas how we could improve the ability to ring fence types of roles, or type of work units, so that information couldn't be shared.

So people being able to access information of the mental health in-patient unit so being able to ring fence that, or ring fencing the paediatrics unit. In that sort of manner. A patient could come through ED and go through ED, theatre, ICU and end up in a ward in a space of 24 hours and could quite legitimately have 40 to 50, to 60 people appropriately look at their records. So I understand that you need to be able to share the information for that passage of the patient through the system, but I there's certain areas, I think, that we could work better at to ring fence it or to safeguard that information better from a system perspective so no matter what your motivation is you physically can't do it.

CA You're looking at access controls, but you're already, with the Department of Health, looking at better analysing the data before it hits a person who has to then physically go through it?

W Yes.

CA No further questions.

PO Ms FOTHERINGHAM, just a couple of things. I may have missed it, but did you tend, or did you intend to tender that matrix table? The sanction?

CA I do intend to tender it.

PO Okay, I'll make that Exhibit 48.

CA I tender that document.

ADMITTED AND MARKED EXHIBIT 48

PO Secondly, you showed Mr FRANCISCO what you referred to, I think, as the Queensland Nurses' Union submission.

CA Yes, I tender that as well.

PO Okay, so I'll make that Exhibit 49.

ADMITTED AND MARKED EXHIBIT 49

PO And just a couple of quick things for you, Mr FRANCISCO. You said that you've started using case studies to illustrate the consequences of breach of

policy and procedure and so forth.

W That's correct.

PO Is that a Mackay Hospital and Health Services initiative or is it a QHealth wise initiative?

W It is our initiative. We worked through the process of sat down with a working group of Health Information Unit and the HR team to – what are the issues that we're seeing and how can we better educate that. And then we took it to our Executive Leadership Team and said, "Look, we know we have problem. We think we can better educate this way." They had some views on how that should be done. But it was very clear from the Executive Team, in particular the Chief Executive, is there are very serious repercussions and our staff need to understand them. So we had to wait till the entire termination procedure, including appeal was complete before we could use that. And that's the only case we have at this point in time. Our two other high profile cases, they both resigned before termination. So it is around make sure we have appropriate cases to use.

PO Our experience here at the Commission, I can tell you, in the prevention space is that the use of case studies is the most effective way to educate staff and the public at large, basically. Do you think there's a – there would be benefit in having that system that you've developed of the use of case studies applied across the entire sector, QHealth?

W I think so, yes.

PO Thank you. The second thing is the matrix sanction table. Is that, again, a Mackay initiative?

W Yes, it is. So there was an initial draft done before I started. And they weren't quite sure how to make it work. I've used that type of matrix in other situations and settings. So we've developed that ourselves. And we did liaise with the Commission about the use of that to make sure that we weren't missing anything. We didn't want to go down a path and realise halfway through we had to backtrack. So we developed that. And we intend to put that into that procedure as part of that review.

PO Again, do you think there would be benefit in having that applied across the sector QHealth?

W Yes.

PO Okay. That's all. Mr SCHMIDT, do you have anything?

LR I do, Chair. Firstly, I'm not sure – there was a reference made, and it was showing on the screen, the Severity and Actions Guide. I don't know if that's

been tendered.

PO I think that's the matrix I've been talking about.

LR In relation to that, there are some matters I would like to seek leave on: the first relates to the VIP flags, and whether there's another possibility of how checks on that can be done; the second relates to the Sentinel program and the 14 days that records are kept and how that actually operates; and then finally, the policy position behind the referrals of certain accesses, but not the referral of other accesses.

PO I'm minded to grant leave. Do you have any submissions Ms FOTHERINGHAM?

CA No, thank you, Chair.

PO Thank you. You have leave Mr SCHMIDT.

LR Thank you. I will just touch on the VIP flags. Now, you indicated, if I understand your evidence, that – and you used the example of the swimmers which were attacked up north, that they're flagged. If I access their system it would pop up and say "Be aware", that you'd only be accessing this if you have a legitimate medical leave?

W That's correct. And also it means then that if we went and back and checked your records, we would know that that flag had been activated and that you were aware of it. So, therefore, your access would have had to been very deliberate to do so.

LR Yes. But it is the case that you've actually got to go back and check my records?

W That's correct.

LR Can you actually do a check on the name of whoever one of those persons were?

W I'd have to go and check with the Health Information Unit on that question.

LR Right, okay. In terms of the records, I understand you said that keystrokes and mouse movements are recorded for 14 days.

W That's correct.

LR But the Sentinel program, I think it was Exhibit 42, indicates it is a monthly report.

W It is only newly implemented, so literally in the last six to eight weeks. And it was a bit of a pilot to see that I could actually watch your mouse and keystrokes and it was recorded on a video for 14 days. So if a matter came up we could go

back and check that

LR But if the matters are only coming up every 28 days, as part of the monthly report-

W But we could get complaints and so on as well.

LR Yes, okay. Finally, in terms of the matrix that the Chair has just referred to, you've indicated that you're reporting only certain accesses to the Commission and to the Queensland Police Service and you said something about external access, or there's been an external access.

W So there's an external link to the breach, so if somebody's gone in and looked at a set of data and it relates to something external to the Hospital and Health Service-

LR So, for example, if I was a nurse at your hospital and I looked up myself, then the consequences to that would be that I'd have an informal meeting with my manager?

W That's correct.

LR And you see that – the reasoning behind that. What's the reasoning behind that?

W The reasoning behind that is it is a low risk and it is an ability for the – it is more of an education process that you know you shouldn't look at your own data. You haven't disclosed it to anybody. It relates purely to you. So the reputational risk and other risks associated with that are very low. So we see it from that perspective.

LR So the Hospital and Health Services sees that as really being a management issue as opposed to a discipline issue-

W That's correct.

LR -a criminal issue.

W So in the severity matrix, that's all pre-disciplinary, so that's all around management of the issue. And we'll do an investigation. And that occurs before we go into a disciplinary process.

LR Chair, I wonder if that exhibit could actually be brought back up onto the screen, please.

PO It is 42, is it, the matrix?

LR No, I believe it's one of the last ones we just tendered. 48, I'm informed. I have to be rude and look at the screen over here.

W You're right.

LR On my reading of that, it is the red and purple matters which result in a show cause letter.

W Yes.

LR So that's taking disciplinary action?

W No, that's pre-discipline. So all of these are pre-discipline. So we – a 'please explain' is more of a gentle way of saying 'there's some issues here that you need to address'. It results more often in a performance management discussion. Whereas, the show cause is we think this has got potential and it could well be something more serious and it could be then related to a suspension.

LR Right. So effectively all these colour coded things are dealt with as a management issue initially?

W Yes, that's correct.

LR And the explanation then given in the last two instances isn't sufficient, then you escalate it to either discipline and/or criminal?

W Yes, that's correct.

LR Thank you. Thank you, Chair.

PO Thank you. Anything arising, Ms FOTHERINGHAM?

CA No thank you, Chair.

PO Thank you, Mr FRANCISCO, you're excused. Thanks for coming.

W Thank you.

PO And we'll adjourn now until 10 tomorrow.

CA Yes.

PO Is that right?

CA Yes.

HRO This hearing is now adjourned.

END OF SESSION