essentially, in a very accountable way that I accept these terms and conditions of access. And if I don't, if I don't submit the assessment in time, if I don't do the training, if I don't complete that, I lose access and I then have to make a specific application to a person of authority to get back on. I think this goes to culture in a way and I think we have to ramp up that initial culture by designing our system. So I'm agreeing with you. I actually think it is more than messaging, although messaging is important when you log on. I actually think it's a specific accountable statement that you read and sign at the point of being given access to a system, particularly a system of significant sensitivity.

CA Yes, thank you.

W And that's what I'll be exploring with my Chief Information Officer and it is about good governance I think which is just another layer of maturity and sophistication.

CA Professor SMITH, his evidence was that if there was from time to time a portion of an assessment as part of that logon then that increases the deterrent effects, which is what you were saying-

W -Yes, so I would absolutely agree with.

PO Doctor, we normally have a break about 11.30. So we're going past that, I understand you're going to be a little while yet. Would you like to have a break now, a short break, or would you like to go through till lunch at one?

W I'm very happy to go through, but I'm in your hands.

PO I'm happy to go through. Is the reporter okay to go through? Okay, we might just continue on till lunch and then break then, if that's okay.

CA Yes. One further thing about ieMR. The VIP, I'm not sure, are you aware of the VIP flag that you can insert categories of patients to be VIP and then when their record is accessed a little warning sign flashes up. And that's another play layer of protection. It isn't a flag that then goes to alert anyone, but it is better than nothing. And Mackay have added to their VIP section, domestic violence victims with orders and high-profile persons. And the Gold Coast haven't. So that's, again, when there's some consistency talks, that's another area that some or at least the Gold Coast could improve on.

W Yes. Can I just say in terms of, I mean, and this is two Health Services and obviously we have 14 hospitals in several Health Services, without counting them, where I think these local innovations are really important. And we wouldn't want to cross local innovations, I think. I think that's part of what's great about a devolve system where I think we need to get better at, is in harnessing those and then those that warrant it, you know, after a proof of concept, if you like, bring them into an agreed way of doing business.

We have invested now, and certainly are accelerating action on creating this system governance which goes beyond the technical to more what I would call the business. Now, just by way of example, so the ieMR has largely been run out of the eHealth Queensland, which is essentially a technology provider, and working with individual Health Services to implement. We've shifted now, indeed we've shifted the resources and this is now being established as we speak, a more of a business and clinician-driven focus around how we can optimise the system, learn from each other and move that into a set of priorities that then get the investment flows into the development and the deployment of those changes across the system. Be they technical changes in the software, or be they standard procedural matters. And I think that's a maturity thing, but it's essential.

And that's part of, I think, the Government's decision to slow down and pause the deployment and spend 12 months, which we've started optimising the system and its governance and standards and some of these issues that you've talked about. I think that is where we are now. So I think we haven't been asleep at the wheel of this and we haven't waited for inquiries or audit reports to move into this space, I think we've certainly been proactive in doing so. I think now my job and the job of the CIO, and other key leaders, is to accelerate some of these things and to make sure that we then put them into more system-wide practice. Because what you're describing is variation, good local initiatives that have been put in place. I have a duty to make sure that where they're good and they deliver benefit, but we're all doing it. So I absolutely take that on board as the responsibility of the centre and as Chief Executive of the system.

CA Nearly off ieMR, I just noticed another aspect. As part of that process, it is only the same surname capability, as we talked about. So anyone else, and they're often some, like apart from when there's acrimonious break ups, some of the more serious breaches, that's only able to be done by manual auditing. And as you said, the amount of database use is phenomenal. Unfortunately, the Gold Coast just don't audit at all, ever. And Mackay have an audit plan and do do some manual auditing.

As part of ensuring, in particular, if it's not possible across the board, at least at the very bare minimum, a random audit be implemented throughout the Hospital and Health Services for the high-risk categories such as domestic violence victims. But ideally a regular audit. But if you can't have the Rolls Royce version at least the high-risk category. Is that possible as part of the consistency to look at?

W I don't think it's possible, I think it's necessary. So I think, again, what we're dealing with here I think is we're in the midst of a radical change. Probably the most profound change in our hospital business in decades, which is digitisation of paper that we've had for decades. So I think we are sort of having to adapt as we go. You know, there's no perfect here. I think that what's clear though, is, I mean, once people lift their heads up from the enormity of implementation and the system is in place and, by and large, people have gotten to a level of

business as usual where they can lift their heads up and say, well, you know, we've made this major shift and we've got business continuity now of our working, our workflows and our patient care delivery and so on, we have to put in place a governance which is contemporary around the system.

There are international standards for that. We have a State standard for it in terms of both at a whole of Government level and at Queensland Health level, of an information and safety management system. There's an International Standards Organisation about it. It's not rocket science. It has all the elements that you would expect, that there is a learning cycle where we set protocols and standards of how we want things to happen. We have proactive design of the system to keep -- to minimise that. We have audits, both regular audits with the sort of flags that we're looking at which we follow up. We have targeted audits based on our intelligence. That comes out from the system for a particular issue that we want to raise. Like, we want to go and have a look at a known group of people affected by domestic violence and let's actually proactively target that. And we have the sort of system of governance where all of that is considered and the system is continually improved associated with that. Not just the technical system, but the people sides of the business and our culture.

So I think that's my expectation and I think that is not just my expectation that is our obligation in terms of running a business, which is very high risk. And I think, so again, my job is to take those comments that you've provided, in terms of where we're up to, and make sure that we accelerate some of our – into a more contemporary safety management system, which is not just dependent on an individual health service mobilising that, where the system both supports and expects it. And I think from my position, that, and I know in speaking with my new Chief Information Officer, who started on the same day as I did, that we are locked together in making sure that we move the system forward. Great work's been done and I'm very proud of the work that's been done. But we'll move the system forward to sort of meet and exceed those contemporary standards for information management.

CA Thank you. Just wanted to mention a couple of policies now. Obviously they were around before you commenced. And no doubt you'll be reviewing policies, but I thought I'd bring them up, and just to clarify again some potential confusion and inconsistencies again with the Hospital and Health Services.

So the first one is the Department of Health Human Resources policy in relation to discipline. It was mentioned by Ms BLOCH yesterday, as their, sort of, go-to. Just while you're getting that, again, Mackay have been proactive in this space.

W Thank you.

CA And it's not in the actual document, but they have quite a structured set of factors for determining thresholds with respect to action taken from misuse of information.

W Yes.

CA And, again, they've put in there the vulnerable person category as one of the considerations that would be more serious, and looking at the adverse consequences of the misuse of information, whereas the Gold Coast haven't got any structure. And from a review of a small number, albeit, of their disciplinary outcomes it appears on balance that Mackay take a stronger stance in relation to misuse of information compared with the Gold Coast. So the Gold Coast could probably do with some assistance from the Department of Health with determining the threshold with respect to discipline and also whether there should be criminal action taken.

But just going into this discipline policy that they've sort of flagged as their go-to document. You'll see on page 1, halfway down, it talks about the "Legislative or Other Authority" and the Criminal Code isn't mentioned there, but the Crime and Corruption Act is. So one suggestion would be to put the entire range of potential actions in there.

On page 3 at the top, "Requirement to Consider Management Action", there isn't reference in here to the possibility that there will be a police referral. And has been in evidence to date at the hearing, it is the Commission's view that disciplinary action should be after criminal prosecution is pursued, if that is going to be the case. So just to make it clear, to staff, the entire range of potential sanctions.

And then here, at number 4, "Key Principles", the first dot point, "Compliance with Relevant Legislation and Applicable Policy", so if you leave out the Criminal Code then there may be some confusion there. And the last dot point, there's a distinction between the criminal process and disciplinary process, and it says, "Further criminal process may run", but it doesn't actually state what that is. But then in the definition section on page 3 and 4 and 5, it talks about section 15 of the Crime and Corruption Act being corrupt conduct, but we haven't got anything about there about section 408E of the Code. So just a couple of points there. And there isn't any actual structure threshold. Now other agencies there isn't either, but Mackay have managed to put some rudimentary criterion together that may be of assistance.

W I mean, I'm happy to note that and your comments and suggestions around that. I think, again, with respect to matters of discipline referrals and discipline and relevant policies, I mean, I think the base obligations that are addressed in the Public Service Act and how those processes are managed in a sovereign organisation, that they're responsible for interpreting that and managing that appropriately. I can't speak without having full knowledge and advice of, I can't speak for an individual health service. I mean, I take what you're saying, but I would have to explore that with our own HR and legal people and obviously the relevant health service providers.

I think, for example, going beyond current policies and standards, if you like, and introducing additional algorithms and criteria, and I don't know whether they would be appropriate or not, you know, and withstand scrutiny. I think certainly from our perspective, I certainly acknowledge the fact that the absence of specifics about the Criminal Code and part of a pathway from an allegation leading to referrals to the QPS for consideration, I think, is, I agree, seems to be missing or certainly not overt enough.

CA It certainly formed part of more of the recent memorandum and email.

W Yes. So I'm very happy to take that on and I think that that should lead to changes in here. I think, I guess from my point of view, what I'd like to make sure that,- I mean obviously we have duties to make sure that we pursue matters or allegations with appropriate natural justice and procedural fairness provisions. And I think I just want to make sure that if we're going to make referrals to the police that we've got prima facie evidence of something that ought be referred.

Now, that doesn't mean to say that we have to complete a disciplinary process. But at the same time I think we have to be careful that we don't take the screening report that you mentioned, and on the basis of that, that there's data to suggest someone's accessed their own personal information on the ieMR that we would make a referral to the QPS necessarily. I think we've got to have some kind of decision tree around that. And so I haven't seen the, I think the Gold Coast one that you mentioned or was it Mackay?

CA No, that's your one that the Gold Coast talked about. I'm just about to mention another one of your ones just to go through quickly.

W Okay.

CA A policy for you, while we're on the topic of policy.

W Okay. So in short, though, I accept what you're saying about the fact that the criminal – referral as an alleged criminal act doesn't appear to be strong enough in terms as mentioned.

CA If Dr WAKEFIELD could be shown "Use of ICT Services Standard" from the Department of Health. So this is from 20th January 2017. I take it you'd be updating this soon anyway.

W Yes.

CA Your Department said that there's a three-yearly review of policy. Just using this, in part as a good example for agencies and in part as one where there could be some consolidation and clarification of unauthorised use, and it's a little bit clunky in parts, but if we go to page 8.

W Yes.

CA There's a good strong message there under "Note" that the unauthorised use includes when it occurs out of work hours. And also on page 8 to 9 under as a preventative tool stating that use is monitored. And then again for prevention, talking about the access controls on page 9. So explaining how the system works for staff. And then talking about, on page 7, down the bottom, that a violation can be criminal. But then when you have that section in there, it's a little bit confusing because it doesn't clearly explain what unauthorised use is in accordance with section 408E of the Code, and you'll see that unauthorised use is defined throughout this document in a few areas in different formats. And it would be confusing for staff, it's defined on page 4, and then 5 is another definition, and then 6 there's more definitions. And then unlawful use under 7 and them down the bottom criminal use. So it is all rather confusing.

Professor SMITH said that policy should be as simple as possible, clear as possible, potentially this document could become four or five pages long. So just to raise that as potentially-

W -I agree. And even four to five pages is a lot for the average person to digest.

CA Yes.

W Anyway, I agree with you.

CA Now, trying to move along quickly, because we've been a while.

PO Would you like to tender that?

CA Sorry, I tender that document.

PO That's Exhibit 66. Thank you.

ADMITTED AND MARKED EXHIBIT 66

CA And I tender the previous document as well, the discipline policy.

PO Exhibit 67

ADMITTED AND MARKED EXHIBIT 67

CA In your Department's response, there were two documents, there was a questionnaire that we sent out for a response by September 27th and then there were further questions flowing from that that we asked of you and those were returned on the 28th October, I believe. And as part of those questions, going to the last pages there – we're just finding that document. I'll just show you the second to last page. It wasn't numbered so I haven't got a page number. Yes, and also the Guide to Securing Personal Information. We'll deal with the first

one, first of all. So this is the second to last page from your Department's response to our further questions. Are you familiar with that document at all?

W Yes, I'm familiar with it. Obviously the detail I'll refer to if I may.

CA Yes.

W What was the question?

CA It is only simply for the reference. At the top there you'll see Departmental Response, and the next one, see third paragraph down: "Focusing on the way privacy is approached by adopting a more positive Privacy by Design approach." I tender that document. So my question to you is that quoting Privacy by Design, have you seen the submission from the Office of the Information Commissioner for the purposes of Operation Impala?

W No.

PO I'll just mark that Exhibit 68. Thank you.

ADMITTED AND MARKED EXHIBIT 68

CA I'll show you a copy of that. We're not going to go into it in any detail at all, but they are reference a report. I'll just show you the Office of the Information Commissioner's submissions. They'll be giving evidence next week. I tender that document.

PO Exhibit 69.

ADMITTED AND MARKED EXHIBIT 69

CA It is just for the purpose of showing the trail from the Office of the Information Commissioner to that other report that I've just provided you, the Guide to Securing Personal Information, Reasonable Steps to Protect Personal Information from the Australian Government Office of the Australian Information Commissioner, from June 2018.

It says on page 2 of that, that is referred to and attached to the Office of the Information Commissioners Operation Impala submission at paragraph 20, on - again, they haven't numbered their pages, I'm sorry, at paragraph 20, under Prevention and Detection. They mention Privacy by Design and attach this report.

So on page 2 of the Reasonable Steps report, paragraph 3, it says, "This guide is not legally binding, however, the Office of the Australian Information Commissioner will refer to this guide when undertaking its privacy functions."

And then at page 8, that's where the Privacy by Design is first talked about.

W Sorry, I'll try and triangulate those documents. Yes.

CA So page 8 down the bottom talks about Privacy by Design.

W Yes.

CA And if you go over the page, they cite up the top, footnote 21, Privacy by Design.

W Yes.

CA Is that the Privacy by Design that your Department was referring to? The Privacy by Design down in the footnote says it was first developed in the 1990s by Dr Cavoukian, former Privacy and Information Commissioner of Ontario Canada, and then adopted by private and public sector bodies internationally.

W So in relation to information, security and technology, I can't answer that question. It's not my kind of specific area of expertise. So I'd be speculating. So I think Damian will probably be able to answer that. So Privacy by Design, the design element of that is much more broadly applicable than simply privacy. But in terms of that phrase, Privacy by Design is your question have we captured that based on this report?

CA My question is if, in your response material you say that the way privacy is approached, not just at an IT level but governance and all the ones we're talking about, culture.

W Yes.

CA If approached in a more positive way by Privacy by Design. So Privacy by Design is a concept that is considered by those who support it to be best practice to take reasonable steps and the reasonable steps come out of the National Privacy Principles and the information privacy principles from the Information Privacy Act, the obligation on behalf of the agency to protect the information, take reasonable steps to protect from misuse, loss, impertinent and PP4, unauthorised access modification disclosure. So I was just wanting to walk you through a couple of those aspects as your agency saying that you're taking that approach as a good model for the other agencies to adopt.

W Yes.

CA So at the top of page 9, the three aims are, "To prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information; detect privacy breaches promptly, and to be ready to respond in a timely and appropriate manner." So we've gone through what your agency is doing in those areas.

W Yes.

CA Yes. And then one aspect further down the page is 3, assessing privacy risks. It talks about having a privacy impact assessment. One of the agencies, Department of Transport and Main Roads does that. Does your agency do that, or do you intend to do that in the future for new projects?

W As a matter of specifics, again, I can't answer that question.

CA That's okay.

W I can certainly get information to that effect. But the specifics of do we have a privacy impact assessment I'd have to take advice on. I'm happy to take advice and break if you like.

CA Yes. We'll just finish off. And then where we're talking here at page 12, with assessing reasonable steps, at the top of that part of the assessment should be the possible adverse consequences for individuals in case of a breach, which leads into page 14, half the way down, the adverse consequences for the individual, the material harm. So that's where, as you identified and agreed with, that particularly vulnerable persons should be afforded more protection, in particular domestic violence victims.

W Yes.

CA And then the other aspect is on page 13, which you've talked about, down the bottom, that health in itself, all of it, the information, is more sensitive than other information. And there there's the need for increased steps around sensitive information, such as health and also, in particular, those particularly vulnerable persons in the Health system. I just wanted to have that as something for the other agencies to look towards given that your agency has Privacy by Design as a tool that you are using.

W Yes.

CA Now just quickly going through the other aspect of Health, rather than focusing on the Hospital and Health Services. You have training, which is mandatory, assessed and in particular one of them that talks about information privacy including – does it include the range of penalties being disciplinary and criminal?

W I'd have to again take advice on the exact wording of that in relation to reference to specific penalties, but it is mandatory and there is an assessment component.

CA And then with the Hospital and Health Services, you provide them with some direction in relation to their education and then they devolve that into their own?

W Again, the responsibility for information security, they are accountable for their own information security and the risks controls around that. As we do, as I said

earlier on in my evidence, part of our job as system manager is to create artefacts, tools, training modules and so on, that they can just adopt. But in most cases they're not required to. If they've got something better or they prefer a different approach that they are free to do so. Although their accountability remains.

CA And just for completeness, as with all agencies, I have some Crime and Corruption data that was extrapolated from the complaints made pursuant to section 38 of the Crime and Corruption Act. Do you have that material in front of you?

W I have some material. If I can check that it is the same material that you're looking at that would be good.

CA Yes. And I'll give you a copy.

W It appears so, yes. Four pages, graphs and tables. Yes.

CA I tender the Guide to Securing Personal Information, Reasonable Steps to Protect Personal Information report.

PO Exhibit 70.

ADMITTED AND MARKED EXHIBIT 70

CA And I tender the Crime and Corruption data. All of the figures are taken from what your agency provides to the Commission, apart from on the last page with the proportional breach. The annual report from your agency has been used since 2018-2019 financial year. So if we go to the first page talks about allegations. And then the actual number of complaints is on the second page. And as you'll see the Department of Health is very low, as you said yourself. You believe that they're not a high number. But you'll see that there has been a sharp increase from two in 2015-2016 financial year to 17 in 2018-2019 financial year. Would that be due to the introduction of the new database and proactive audit function that you're working through?

W So I think I can speculate reasonably well on why. I certainly have hypothesis about this which I think is fairly strong from a face validity perspective. And I would argue that the first reason is increased vigilance and a cultural and focus issue. So when an issue receives attention, particularly in the public sector, well, public or private sector, I think the organisation responds and there's very much an increased focus around, and particularly proactive focus around finding and reporting matters. Again, it's not specific to this particular issue if one has a focus on something, it tends to drive more reporting. I think the most significant impact though has been the introduction of essentially our ability to identify issues that previously we were unable to identify. So I go back to what I said about introducing an electronic medical record, for example. In a paper

environment there is no measure, therefore there is no knowledge, therefore there is no report of someone's eyes that cross a page, a physical page of paper.

In doing what we've done over the past three years to essentially digitise 50% of the hospitals, sorry, 50% of patients and 14 hospitals, and I guess consequentially changes in the Department around that with a significant implementation focus, we've moved from a situation where we had no visibility to one where every single stroke of a key is recorded and is auditable. So my hypothesis is that rather than this representing an increase in breaches, that this is representing a visibility of breaches. But, again, every breach is a significant event in my eyes and I think that, you know, whether it's intentional or whether it's an error, these are not just individuals that look at a record that they shouldn't, this also applies to an inadvertent error of somebody sending some information to a patient, for example, or a doctor about a patient and putting the wrong thing in an envelope or putting the wrong information there. I mean, this captures all breaches, intentional, malicious or otherwise. But my argument is, and I speculate that it doesn't represent a worsening of our discipline or performance around breaches, that it's just now much more visible because of the reason that I explained.

And, again, I understand that you've put a denominator under this which is numbers of staff in organisations, and you've sought to compare organisations based on the number of people in there. And I respect that. But, again, I would go back to the sort of numbers that I talked to you about at the beginning, which is really 60,000 unique users across our system, and 436 million transactions in a month. Whilst I'd like that number to be zero.

CA Yes.

W And we'll continue to work to make it zero, I think that gives the sort of context that we're dealing with in the context of our, you know, 90,000 staff that come to work and safeguard, seriously safeguard information of patients and obviously of staff, and that departures from that, particularly intentional or malicious departures are incredibly small. And our job is to identify them, well, prevent them, identify them, and where there's evidence, particularly where there's evidence that there's intent, that we bring down the full force of our discipline and criminal process to it. So I think that's how I would frame it in respect of these numbers.

CA The range comparing with the other agencies, there's on page 4, there's one in 341, whereas you've got the Police and Corrective Services in the 70s, so sort of in the middle of that continuum.

W Again, I think it is not appropriate for me to comment on any other agency. I don't know their circumstances. And, again, whilst I respect the fact that you've chosen to put the number of staff as a denominator, you know, I'm not sure how reflective that is of relativity, actually, in term of either risk or breaches. But I

respect the fact that, you know, I think there's probably a lot of other metrics that could be applied which maybe more robust in terms of comparative.

CA What are your suggestions in that area?

W Well, again, I don't have detailed knowledge of the other agencies' systems or the degree to which the data in those systems is accessible. I guess I'm just saying I don't know how comparative, how helpful it is to compare. I'm just wondering whether we're comparing apples with apples. I can only speak to Health and in my view that's the explanation for why the numbers have jumped from over the last couple of years.

CA From a greater awareness?

W Well, from a greater awareness, but more specifically we now, I think more importantly than that, we now have evidence in a way that previously we would not have evidence. There is no – when we have evidence that someone's logged in and made keystrokes to access something, we have prima facie evidence. We still have to ask them why and seek natural justice for that. But in the past in terms of a complaint it would be much – having prima facie evidence that they accessed an inappropriate record may have been much, much more difficult to establish. It doesn't mean it didn't occur. So I think that's what we're seeing here. But I just wanted to make a point about context. Every one of those is a serious matter. But, again, our job, have a very important job to protect people's information. It's critical and it's both ethical and statutory, but I have a job to do to make sure that information can be provided to people who deliver care and make life about decisions to people. So I think information security is a very critical component of my job, but the purpose of my job is to make sure that information can be provided to people making decisions.

So what I would say is that in a system where I have to provide information to 100,000 people, I carry a lot more risk that a system where one can constrain data to access to 10 people, for example. And I don't think you can compare the two. That's what I'm saying, I guess, it's not simply a matter of how many employees one has, in my view. I hope that makes sense.

PO It does, doctor. Also it brings into sharp focus this point that as you've said quite correctly, there's a delicate balance allowing the sharing of necessary information and the security of it for protection against unlawful use and access.

W That's right.

PO Access and/or misuse. It probably highlights that there's a fundamental part of the equation also that in the prevention space, which is to have a culture-

W -Absolutely.

PO -within the staff that they understand what is proper and what is improper access and/or use. And if you get that right the technical controls are much easier to manage, because you don't want a system where it's almost impossible to access because that defeats the purpose of your clinical care and so forth.

W Absolutely. And I think the QIO make that point very clearly in their report. Again, it is not an absolute. If my objective as Director-General of Health was to keep people's information safe, if that was my objective, then I would lock it up and I wouldn't let anyone have it and I would achieve that. My objective is not, that's not my objective. My objective is to deliver high-quality care to people and particularly in a time critical sense, and make sure that the people making decisions have that information at their disposal. And that's not just 100,000 people in my organisation, that includes through some of our other, like the GP access to the viewer for example, providing our information and data in real-time to general practitioners who are not employees, and others.

So that's how I frame it. I have to balance that objective, which is my core objective, with making sure that I, not only that I comply with my statutory obligations, but that I manage the risk, I manage the trade-off of those risks. As I said it would be very safe to lock it up and have no-one access it. There's a great quote which, in a safety sense, which I think articulates this in a metaphor, that the safest aeroplane is one that sits on the ground and never flies. But aeroplanes are built to fly. And I think it's the same thing here. But the objective for me is not information security, the objective is patient care. Information security is an essential component of my job, but it is not the goal. And I have to trade that off, as do my 100,000 staff, in how we design our systems, in our culture and how we operate, how we design for privacy, but also how we design for access and use usability. So I just wanted to make that point, respect the fact that your focus is about information privacy, but that I think in our system we're trading off security and access all day every day and we take that incredibly seriously.

And, again, I think whilst we are always looking for ways to improve, and I think you've raised some really important things today that I have to act upon, we're actually quite proud our commitment to this. And as I said, its's a fundamental, ethical and professional principle which doesn't exist in other agencies by virtue of their professional regulation and professional ethics which I think is why we probably do better than some other organisations because of that.

CA One last quick question before we all break. Just in the disciplinary specific to Health and you may not be able to answer this question, and we haven't asked someone from the Ethical Standards Unit to attend, so if you aren't able to, then that's fine. But in relation to Queensland Police referrals, do you know if substantiated breaches of privacy where it might amount to an offence as a matter of practice are referred to the Queensland Police Service for consideration of criminal charges?

W I do. And so obviously I can't talk about individual cases.

CA No.

W Nor am I aware of every individual case in a devolve system. I would be aware of departmental ones.

CA We're just talking about departmental.

W Okay. I'm not necessarily aware, although I maybe, because it's part of my role about such matters across the broader system. I am aware that we currently have four matters that have been referred to the police and are currently matters that are under consideration or in a process which involves the Queensland Police Service. So, I guess, in that way, I would submit that that's probably, again, prima facie evidence that there are occasions when we, based on our process of making an allegation and appropriate natural justice and getting some sense of whether there is prima facie evidence of at least a potential criminal act, that we don't hesitate to refer that matter to Queensland Police. And we come down very heavily on people using our disciplinary process as well in parallel with that.

CA Are you aware when those four matters were each referred to the Queensland Police Service?

W I'm not. I wouldn't like to jeopardise that by giving any specific details, but what I can say is these were referred within the 18-19 financial year.

CA Thank you. And I tender the crime and corruption data.

PO It is Exhibit 71.

ADMITTED AND MARKED EXHIBIT 71.

CA Thank you very much for your time. I don't have any further questions.

W Thank you.

PO Ms CLOHESSY, do you have any questions? .

LR No, thank you. If he may be excused.

PO Thank you, Dr WAKEFIELD, thanks for coming and you're excused.

W Thank you.

PO Feel free to go. You're right. Thank you.

W Thank you, Commissioner.

PO 2 o'clock.

CA Yes, thank you.

PO Thank you.

HRO All rise. This hearing is adjourned.

10

END OF SESSION