Crime and Corruption Commission
QUEENSLAND

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 4 - THURSDAY 14 NOVEMBER 2019
(DURATION: 2HRS 45MINS)

Copies of this transcript must not be made or distributed except in accordance with any order made by the presiding officer concerning publication of these proceedings.

LEGEND

PO	Presiding Officer – ALAN MACSPORRAN QC
CA	Counsel Assisting – JULIE FOTHERINGHAM
HRO	Hearing Room Orderly – KELLY ANDERSON
W	Witness – JOHN WAKEFIELD
LR	Legal Representative – PATRINA CLOHESSY for Queensland Health

HRO All stand. This hearing is resumed.

PO Good morning.

CA Good morning. Good morning, Chair. I call Dr John WAKEFIELD.

PO Good morning, Mr WAKEFIELD, how are you. An oath or affirmation?

W An oath, please, Commissioner.

PO Thank you.

HRO Take the Bible in your right hand and repeat after me. The evidence which I shall give.

W The evidence which I shall give.

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.

HRO So help me God.

W So help me God.

HRO Thank you. Take a seat.

LR Yes, may it please the Commission, my name is CLOHESSY, initials P, I'm counsel from Crown Law and I appear for Dr WAKEFIELD.

PO Thank you.

CA Good morning, Dr WAKEFIELD.

W Good morning.

CA Were you given an attendance notice this morning?

W Sorry I'm having trouble hearing.

CA Were you given an attendance notice this morning?

W Yes, I was.

CA Is that the document?

W Yes, it is.

CA I tender that document.

PO Exhibit 61.

ADMITTED AND MARKED EXHIBIT 61.

CA Dr WAKEFIELD, your role at the Department of Health is as Chief Executive Officer as Director-General?

W Correct.

CA And you have 30 years' experience in clinical and management roles in rural regional and tertiary public sector health services in Queensland.

W Yes, that's correct.

CA And you completed a fellowship at the National Centre for Patient Safety in the United States.

W Yes, that's correct.

CA And returned to Queensland 2004 where you established the Queensland Health Patient Safety Centre, which you led until 2012?

W Correct.

CA And you are actively involved in national efforts to improve patients safety in partnership with the Australian Commissioner for Safety and Quality and Health Care.

W Yes, that's correct.

CA You chaired the National Open Disclosure Pilot Project and regularly teach open disclosure and other patients' safety curricular.

W Correct.

CA Your research interests include patient safety culture, safety performance measurement and open disclosure.

W Yes.

CA In 2011 you were awarded the public service medal for services to patients' safety as part of the national Australia Day awards?

W Yes, that's correct.

CA Thank you. Has your agency provided a submission to the Commission?

W Yes, we've provided a submission and a response to subsequent questions, I understand.

CA I believe there was a questionnaire and then some follow-up questions.

W Yes.

CA The submission I'm talking about is the call for public submissions in response to that.

W Oh, I'm sorry. So just by way of correction then, Commissioner, we have responded to the questionnaire and subsequent questions.

CA Yes.

W I'm not aware of a specific submission. I have not made and I don't believe the Queensland Health has made a specific submission.

CA Would you like to make an opening statement?

W Yes, please. Thank you for the opportunity to be involved in the public hearing into misuse of information and to contribute to the improvement opportunities across the public service. Commissioner, at the outset I would like to acknowledge the importance of privacy and confidentiality in health care and certainly recognise as Director-General and as leader of the Queensland Health system that there's a great deal of trust that the community place in us as an organisation to ensure that the confidential information that we have in our possession that is collected for legitimate purposes is used appropriately at all levels of the organisation.

As a doctor myself, I know that immediate access to critical health data can so often be a matter of life and death for patients in our hospitals and clinics. Information is actually our life blood as in the health care system.

The revolution over the past few years, which has seen the shift from patient data, which essentially is locked away in a paper record in the basement of a hospital, to a situation where a clinician in any hospital or clinic across the State can get immediate access to critical information about their patient, no matter where that patient is from across our State, has not only saved thousands of wasted administration hours, it has saved significant amount of patient time and frustration and disruption and distress.

But most importantly it has dramatically improved our ability to deliver the sort of health care outcomes that our community and our patients tell us that they want and indeed expect. And I think it is not hyperbole to suggest that lives depend upon access to this information in a very timely way for the people who need to have it to help those people, particularly where time criticality matters in emergencies.

The fact that we've achieved this, and at the same time retained a very high standard of privacy and security of our clinical data I think a testament to the diligence and the hard work and the integrity of all the people who work in our health care system.

I think for the benefit of some context I think around the complexity and the volume of interactions in our system I'm just going to speak quickly about one of our systems, the Integrated Electronic Medical Record. If I may just give you some facts about that. It is currently deployed in 14 hospitals and represents approximately 50% of the patient transactions across the whole of the Queensland public health care system. Our system has 60,000 unique identified users. In one month, there are 500,000 patients that are treated using this system. 436 million transactions in one month within that system by our clinicians. There are 7.5 million tests ordered. And 14 million individually accessed patient records. Now, one can only imagine the difference between being able to access that on a computer in the system having to retrieve a paper record from a physical location.

Confidentiality of patient data is not only a core ethical and professional obligation of our clinical professions, it is enshrined specifically in the Hospital and Health Boards Act under Part 7. So in addition to our privacy obligations we have very explicit statutory obligations around patient confidentiality.

Our maturity and data protection continues to strengthen, Commissioner, and we are continuously working to find the right balance between ensuring the data is available when and where it’s needed to people who have a right to use it for care. Whilst also protecting what patients have entrusted to us from inappropriate access. So I indeed welcome the opportunity to assist the Commission today in its inquiry.

PO Thank you.

CA Thank you, Dr WAKEFIELD, for that introduction. I'd just like to show you the organisational chart, the management and structure for the Department of Health.

W Thank you.

CA Are you able to speak to that document to provide an overview of the functions and how your organisation is structured with respect to provision of health services?

W Yes, I'll attempt to give a concise overview if that would help.

CA Yes, thank you.

W So Queensland Health is comprised of the Department of Health, as well as 16 independent Hospital and Health Services, which are geographically dispersed across the State. And, indeed, that's represented on this structure tendered in front of me. The Health Services are responsible for delivery of public sector Health Services and are independent statutory bodies governed by their own professional Hospital and Health Service boards and managed by a Health Service Chief Executive. That is a recent development in our system, Commissioner. In 2012 we went from being one single system to having what we now know as a devolved system with independent sovereign Health Services, 16 of them, and a Department of Health.

So the Department of Health is responsible for the overall management of Queensland's public health system at a state-wide level. And my comments today will largely be regarding the Department of Health, again, noting the fact that in some cases it will be difficult for me to comment about the individual governance of an individual Health Service. The functions of the Department include system management and system leadership. And I'll just outline four or five key functions of the Department that are addressed in the Hospital and Health Boards Act: responsible for providing strategic leadership and. Direction for health, through the development and administration of policies and legislation; developing state-wide plans for Health Services workforce and major capital investments across the system; managing major capital works for the public sector health service facilities, purchasing Health Services. So indeed we have a contract between the Department of Health, effectively myself and each Health Service, which covers a range of – it essentially covers what we expect in return for funding.

I'm also responsible for supporting and monitoring the quality, efficiency, effectiveness and timeliness of health service delivery across the system and for each individual health service. Ad also for delivering a specialised range of health services which including prevention, promotion, protection, Queensland Ambulance Service, aeromedical retrieval services, health information and communication, technology and state-wide health support services. Across the system there's approximately 90,000 staff and around 12,000 of these are employed within the Department of Health.

So it is a complex system. And the role of the Department is really one of strategic and system leadership and some key issues, some key components of direction and performance, setting goals and monitoring and managing.

CA Thank you for that overview. I tender that document.

PO Exhibit 62.

ADMITTED AND MARKED EXHIBIT 62.

CA Dr WAKEFIELD, other than the obvious health information, medical information in relation to members of the public, are there any other types of information that is personal for the public that you hold?

W So we, in relation to members of the public. Obviously we have a range of data around our own staff, but I understand your interest is particularly in information that we hold around our patients and the public. We hold significant amounts of information. I guess, perhaps I can summarise that by saying, obviously, names, addresses and contact details are what we would call client registry data items that allow us to identify someone, which includes the date of birth and obviously name and address and so on.

Their medical history that that patient gives to us as part of our assessment of them; any family history; details of diagnosis and treatment; test results; so x-rays and scans. And also a range of other client-based data, such as Medicare and Commonwealth benefit numbers and so on. So I think if we split it into the client metadata and then their clinical data is a way of thinking about it.

CA Thank you. And how would you describe the structure of the Department of Health with respect to responsibilities for privacy information technology and security and management and ethical standards and discipline; those three areas?

W Right. For the Department of Health, so could I just ask you to repeat those three areas for me please?

CA Privacy.

W Yes.

CA Information technology security and information management.

W Yes.

CA And, the third one, ethical standards and disciplinary investigations and sanctions.

W Thank you. So, in respect to privacy, we, in the Department, we have a privacy and Right to Information unit. So we have a specialist unit that has expertise and responsibilities for all matters pertaining to Right to Information, and matters pertaining to the privacy obligations upon us both State and Federal in relation to privacy standards and statutory obligations. That unit has a range of functions, including expert advice, both to the Department and the Minister, but also to Health Services. They have responsibility for managing and independently assessing Right to Information requests. They have policy responsibilities in terms of helping supporting the organisation under my authority; setting policy and standards relating to information privacy. And they also provide significant development of training resources for youth within the Department of Health and across the broader system should Health Services choose to use those. They're not required to. So that's privacy.

In terms of information technology security and information management, there is – and this has been provided in our submissions, responses to questions – we have a Chief Information Security Officer in the information – in the eHealth Queensland division. And I certainly the Chief Information Officer who will be a witness here can explain in more detail how this works. So we have an executive person who has responsibility for matters pertaining to information and security, be that significant actions in respect of cybersecurity, right through to how we design our systems and our risk controls particularly around the IT access. But obviously we still – we're not completely digital across our system, so it’s not just about information technology, we also have information standards and information management across our system which governs I guess the broader perspectives, with policy standards, training and so on around access to information wherever that sits.

We have two committees, we certainly have a committee around IT security and cybersecurity which again Damian GREEN can talk to you in more detail and we have an information management committee that is particularly focused on clinical informatics and standards across our system, which is pretty standard in a health care organisation.

In respect to ethical standards, we have a specific Ethical Standards Unit which resides close to me in terms of the Department of Health in my office. That is a specialist unit with experienced and expert leadership and staff, which deals with matters pertaining to the Public Service Act and other ethical statutory and ethical obligations that we have. And particularly in relation to matters such as whistle-blower status, reports of information access and breaches and advice and determination about the appropriateness of reporting, be that to the CCC, be that to other organisations, and advice in relation to whether a matter constitutes misconduct, official misconduct or, indeed, ought to be considered to be referred to the Queensland Police Service. So that’s a unit, again, which is set up in the Department of Health. After devolution in 2012 Hospital and

Health Services, as part of their sovereign responsibilities have that duty within each Health Service. Certainly the smaller Health Services I think still rely fairly heavily on the advice and support of that unit to manage their accountabilities within the Health Service.

CA Thank you. How do you consider that privacy breaches by your staff impact on your agencies ability to perform its functions?

W Privacy breaches are, where they occur, thankfully they are rare. All of them, regardless of whether they are malicious or accidental, and I think there's a spectrum of how privacy breaches occur, and I'm happy to give examples. Regardless of the cause and the intent behind them, I think, number one, they undermine trust, and they undermine our public trust and our reputation for being custodians of probably the most precious information that citizens hold.

So we take them very seriously. I think that clearly in addition to what I've said I think is the most important aspect, which is trust and confidence, there are clearly matters of compliance and statutory obligations, up to and including criminal liability for certain breaches. And, again, I take that extremely seriously. But I think fundamentally, the public expect us, and they have a very high regard, I think, certainly our information from a range of public and patient experience surveys and interactions is that they have high levels of trust for their Health Service and their health providers. And we value that trust because without that trust we can't do our job. So I think for me, without dismissing our statutory obligations, which are critical, I think for me the biggest challenge with privacy breaches is its impact on trust of our organisation.

CA And how would you describe the Department of Health's culture when it comes to the misuse of information?

W So I think, again, I've been Director-General for two months. I draw much of my experience from this from my various roles throughout my career within Queensland Health both as a clinician and as an executive, both very much in health service delivery, Hospital and Health Services, as well as from the Department of Health. I think I would say two things: first of all I think health is somewhat unique from other agencies in the sense that patient confidentiality is a core ethical and professional foundation of everything we do. It is not simply an issue of our health business and our health employment. It is enshrined in the very training and registration of health care professionals.

So even outside of our employment arrangements, there's a very, very – a core professional obligation to absolute patient confidentiality for registered health professionals. And I think that is also recognised in our Hospital and Health Boards Act, under Part 7, where we have specific statutory obligations in relation to patient confidentiality. So I think I need to point out that that's a critical influencer of our culture in health, which is probably not present in some other agencies.

So all of our clinicians indeed are absolutely aware of their obligation to patient confidentiality. And no-one can argue that they didn't know, or they weren't trained, in my opinion. In my opinion, that is a core artefact of our culture. I think when it comes to the broader issues of accessing information, paper or electronic, to undertake one's duties, I think it would be fair to say that, I think, in terms of our cultural maturity, we've come a long way.

As I outlined in my opening statement, I think even in the last decade we've revolutionised the world of a clinician in terms of their ability to access data when they need it to provide care, which is what clinicians I think tend to focus on. The downside of that I think is that I don't think clinicians – whilst clinicians are absolutely attuned to patient confidentiality, I think there's a maturity of development of working with information systems. Just by way of example, in a busy clinical area, when one opens the electronic medical record to interact with it, if one then goes off and provides care again in a moment, you know, that record potentially is left open. Now, that's not any worse than in a paper record scenario with the same thing. But I think the focus of the clinician is perhaps on the care of the patient, rather than thinking, “Right, I must close this system down.”

So I think our staff are having to learn how to, as patients are, adapt to this digital environment that we're in. But I think the culture in the clinical space is very strong about clinical – about protection of rights of patient confidentiality. I think there are occasions, and particularly with now what I would call this much easier access to data at the point of care, where some individuals, and I stress this, a very small number, potentially allow their curiosity to wander.

So, for example, I think the commonest intentional breach that certainly I have observed is an individual person, clinician, looking at their own clinical record; whereas, previously they'd have to go to the records department and get their own record out. And whilst that may not be malicious, it certainly – and they can access their own personal information, as anyone can through our administrative access process, that is, you know, I think that is something that I think from a cultural perspective we've still got work to do to remind people that that's something that's not appropriate.

But I think coming to your point about our culture, I think our culture is very strong. Could it be better? We're always striving to make it better.

CA Thank you. In relation to your leadership as Director-General, how do you communicate the Department of Health tolerance towards corruption?

W So in many ways. So I think that, as I explained, I've been in this job now as the Director-General for two months, so it is early days for me in terms of my communication and leadership in that regard. I draw upon the role of my predecessor, Michael WALSH, and certainly in August of this year he issued a communication to departmental senior staff, again, in a very explicit way reminding them of their ethical and statutory obligations in relation to confidentiality and privacy of data. And the leadership team; several members of the leadership team subsequently took that messaging and took it through their divisions in a very overt and explicit way. And I think that was provided to you in our responses to questions. But, if not, I can provide artefacts to support that. So that's one very tangible way, very explicit messaging that then, not just from the Director-General, but that it is shared through the leadership team and promulgated through the system. We also have a-

CA Sorry to interrupt you.

W Yes.

CA I'm just have a look at what we do have. We've got a memorandum from 23rd May 2000 and-

W Sorry, I said August, didn't I?

CA Well, there's another document. There’s an email from the 2nd of September 2019. It might be an opportune time for us to tender those documents. I'll show you first.

W I'll try and find them.

CA We have copies.

W You have copies?

CA Yes.

W So there was a memorandum from the previous Director-General, and there were-

CA Yes.

W -communications from the Chief Executive of Health Support Queensland and from the Commissioner of the Queensland Ambulance Service.

W Thank you.

CA Just showing you the email first of all.

W Yes.

CA Is that the email, or maybe-

W -Sorry, the memorandum do you mean?

CA I think about to show you the email first.

W The message from Peter BRISTOW? That one?

CA Yes. Is that the sort of communication you were talking about?

W Correct. I think in reference to the memorandum from the Director-General to the senior leadership team and then subsequently you provided me here with the email message from Dr Peter BRISTOW to all of his team in Health Support Queensland. I'm aware there was another communication I believe from the Commissioner of the Queensland Ambulance Service.

CA Yes.

W Can I check with my counsel about that?

CA Yes. I'll just show your counsel the memorandum that you've been handed.

W Yes.

CA While your counsel is looking for that, we might just have a-

W Yes, of course.

CA Going in chronological order is probably better, starting with the memorandum, which I tender, the memorandum dated the 23rd of May 2019.

PO Exhibit 63.

ADMITTED AND MARKED EXHIBIT 63.

CA I do note down here there's a strong stance taken in the last two paragraphs. Saying that it is not acceptable for employees to use their access to information systems to look up personal or health information about themselves.

W Yes.

CA Family, friends, family members, colleagues or out of curiosity or to further their own interests. And the last paragraph sends a strong prevention message, that there are processes in place to monitor and audit the information systems-

W -Yes.

CA -and that misuse of the information can result in a criminal offence.

W Can I check, so you're referring to the memorandum?

CA The memorandum UI at the moment.

W Yes.

CA It mentions the Crime and Corruption Act there and the Code of Conduct. It may be beneficial – we did have Professor SMITH, an expert from the Australian Institute of Criminology, provide some evidence on Monday. And from a preventive point of view he said that it is best practice to provide, and has a strong deterrent effect, the entire range of possible consequences that can come from misuse, which would include mentioning the Criminal Code there as well. Just for sort of future moving on tightening up.

W Thank you.

CA And on page 2, I notice there that it says the Department takes inappropriate and unauthorised access and disclosure of information seriously; paragraph 1. And has and will come to continue to take appropriate action, including disciplinary action. So it might be useful just to put in and referrals to Queensland Police Service there. But otherwise that's a strong message sent from the top to the senior executives. So just – sorry, did you want-

W -So may I add, so I note your comments and suggestions there. I think so this is obviously a point in time message from a Director-General, which again as the new Director-General, from time to time I would take the opportunity to do the same. I think there are many other components of what I would call a defensive in-depth model to remind people of their obligations, right through from their initial access being granted to a system and the training and support that goes into that. And again I noted the evidence of the criminologist around that, that it's – and certainly from my own experience and expertise in human factors – the strength of the control is much better with face-to-face training than it is in terms of online or some kind of posters or messaging.

So I think very much we take the line that face-to-face training is optimal and certainly that's the line we have taken with the ieMR roll out. That every time a person logs in there is messaging. Again that's useful at the beginning. But I think, as people get used to that, that's easy just for them to click through, but it's important that that’s there.

I think also we have a range of work that happens regularly to remind people not just about the information security, about the broader obligations that they have in relation to behaviour and conduct, ethical conduct as well as lawful conduct. And that includes – we have a week each year where there's specific focus on fraud and data integrity and so on. We have a range of training that is provided in an ongoing basis throughout our system around Code of Conduct, around really going to what you said before about the culture of our system in terms of the integrity and the importance of protecting privacy as well as patient confidentiality.

CA And if we could just turn to the email?

W Yes.

CA And I note, again, a strong stance had come to the staff further down the chain. Down the bottom of the first page, you mention specifically section 408E of the Criminal Code in relation to accessing confidential information on a database.

W Yes.

CA And on page 2, the second paragraph explicitly, the types of misuse at the sort of lower level of the range, just to make sure that everyone knows that that's still criminal it's that it is prohibited to look up yourself, family, friends or a notable person.

W Yes.

CA So that sends a strong message to the Department of Health staff. Now, just a couple of other matters before we sort of move on to some questions in relation to particular aspects of the service. How necessary is it for the Department of Health to share data with other agencies?

W It is critical. So both from a health perspective but also from a statutory obligation perspective we have a duty to share information, which includes at times personal information, patient information, with a range of other agencies. And we provided to you in the response to questions, I think, a fairly – not an exhaustive, but a fairly comprehensive list of key organisations that we have agreements with and the legal basis for those for you to better understand, I suppose, how our interactions, particularly with other health and social care agencies but also other statutory agencies, is critical in terms of discharging our duty under the law, but also discharging our duties to patients in terms of patient care and access to information. And of particular importance to me, again, as a clinician, is the critical role that General Practitioners, for example, play, and others, in the continuity of patient care. And we know that in the absence of being able to access that data that patients suffer adverse consequences.

CA Thank you. I tender the email from the 2nd of September 2019.

PO Exhibit 64.

ADMITTED AND MARKED EXHIBIT 64

CA In anticipation of actions of your staff coming under the scrutiny of the Human Rights Act as of the 1st January of next year in relation to any privacy breaches, what do you anticipate the impact will be on your agency and any changes and approach that your agency will take?

W I think – so we've taken great care to undertake a thorough examination of the legislative obligations and the human rights and mapped that across our various services. Obviously it goes well beyond privacy and data integrity to a whole range of matters. So that work is underway. In many cases it’s complete in terms of mapping our obligations. I think there are some areas of our services where that creates – has forced us to think more carefully about how we organise and deliver services. An example would be in mental health. I think the particular example that I refer to is in Offender Health Services where we provide care to incarcerated prisoners on remand or under sentence. And where we do so, if you like, in the environment which is run by the Custodial Service. And some of the rights, human rights aspects and care of prisoners, I think really challenges not just the health system but the Corrections. For example, their right to the same level of health care as every citizen.

And so I think without getting into any specific detail there I think we’ve taken this very seriously. We've explored where we think we and perhaps in partnership with other agencies have had to strengthen some of our systems. And, indeed, where in some cases we've had to take that issue up with other jurisdictions. So, for example, in the offender health space, Commissioner, prisoners in the Australian contexts are not entitled to access to Medicare benefit schedule. And we think that's at odds with the human rights legislation. So there are things like that where some things are within our control and some things are not.

As it pertains specifically to information privacy, again, I'm largely satisfied at this stage that I don't believe that the Human Rights Act really provides – really increases our current – I think our current obligations are extremely strong in relation to both statutory and ethical in relation to information privacy and patient confidentiality. And I think my focus remains on making sure that we are constantly improving our culture, our systems, our processes, to make that data as robustly secure as possible, whilst not compromising the access to the data, which lives depend upon.

So I see it as a – it is not binary. It is a trade-off between access to data and protecting the data. And I think that's our daily challenge which I would argue that we, to date, I think we’ve – I'm quite proud of the way that the health system has responded to that with the digital revolution which really takes that to a different level of risk.

CA Thank you. And how does your agency provide extra security protections for vulnerable members of the public, such as domestic violence victims concealing their address from the ex-partner.

W So obviously we have many information systems and I can't speak to all of them. I think as a matter of a detail the Chief Information Officer may be – if you have specific questions about specific-

CA Yes.

W -IT applications. But our key clinical repositories of information such as eMR, which is our patient administration system, which it is called Hibiscus which is across all hospitals not just the ieMR hospitals. They all have flags in them that we use that our staff use to denote particular levels of sensitivity, scrutiny, safety for vulnerable populations. So, for example, with domestic violence sufferers or in a sexual health context or wherever there are you know heightened sensitivities, there are flags that are put on records such that when staff go to open them they see such a flag. In Hibiscus, for example, there's three levels. There's the normal level and then there's the first level of flag which essentially is a flag of "take care there's a particular issue here that you have to look out for." And then the third-level flag which essentially closes that data off to access without special permission.

So, again, as time goes by and as our ability to harness such things as artificial intelligence and other smarts in the system those things will doubtless develop to be more sophisticated and more person-centric. But again I'm quite satisfied that from the perspective of standards, from information management standards, from the perspective of international standards, and the responsibility for us to have an information management safety system, that that's reasonably contemporary.

Again, we've got to be very careful that we don't lock away information that is important that needs to be for people that are providing care. But we do put patients in charge of some of those decisions. Many of those decisions, in fact, so that, say in domestic violence situation or in a sexual health clinic situation, patients can actually make a choice to have that information not accessible to anybody. But at the same time we seek their – we make it very clear to them that that's – there are occasions where that could be – that could go against them in terms of getting care that they need if they don't have information available.

So I'm pretty satisfied that with our current approach that we have those flags and those levels of security for vulnerable people of various descriptions. And also, I guess what we might call VIPs, where we may be concerned that they may be particularly attractive for someone to explore or exploit.

CA Thank you.

W The CIO will be able to provide any detail if you wish.

CA Yes, we can ask him more detail. Thank you for that. Now I was just wanting to turn to the Hospital and Health Services, and if you could sort of shed some light on what's happening with their sovereignty and your leadership.

W Yes.

CA So I was just wanting to show you a few sections of the Hospital and Health Boards Act 2011 which you referred to earlier.

W Thank you.

CA I tender that document.

PO Exhibit 65.

ADMITTED AND MARKED EXHIBIT 65.

CA Just go first to section – now this Act predates the establishment of the Hospital and Health Services. You said they were in 2012?

W Well this Act was necessary as a precursor to be able to establish those. So really-

CA It mentions them in UI-

W -Yes. So I think again without getting into detail, this Act established those, got the head of power to establish those agencies and so the timing of that, I guess-

CA -If you could sort of walk us through and let us know what's happening with and who's responsible for what?

W Okay.

CA So you've got section 4 talks about the principles and objectives of the national health system.

W Yes.

CA And at subsection (a) (iii) arrangements are to be in place to ensure equitable access to the services for all eligible persons regardless of their geographical location. So the aim there is for the same experience wherever you are in Queensland; if you go to Mackay Hospital Health Service or the Gold Coast, should be the same experience.

W The aim there, yes, is equity of access to services wherever you live.

CA And then section 4 (b)(iii), the principle is to support - sorry.

W In front of me I only have essentially the first few pages of the legislation.

CA Yes. So it should have section 4 (b)(iii) there.

W I have the index. I'm not sure I have the actual section in front of me. I have got Part 1 of the Act. So if you could point out the specific section you're referring to, thank you. Maybe a page number might help me.

CA Page 18. Halfway down the page.

W Yes.

CA 4(b)(iii).

W Yes.

CA To support an integrated approach to the promotion of healthy lifestyles, prevention of illness and injury and diagnosis and treatment of illness across the continuum of care."

W Yes.

CA So there the idea is again, having a view to the Hospital and Health Services, that similar approach, integrated approach, all on the same page?

W Yes.

CA Yes. And then if we just move to page 19, section 5 (b), subsection (2)(b), that's under Object of the Act, "Providing for state-wide health system management including health system, planning, coordination and standard setting."

W Yes.

CA So again the idea there is everyone does the same thing, or at least to the extent possible given the slight intricacies of different remote locations. Is that the general idea?

W So those comments, so the references to those sections of the Act and those particular points is absolutely the case, that based – there is a national health agreement under the Federation which governs, which all States and the Commonwealth sign up to, which governs how the State and the Commonwealth Governments interact on the health care system, and obviously a major component of that is funding. And the Hospital and Health Boards Act is reflecting some of the principles that underpin the agreements in a Federation sense about how the principles for the health care system that we want, and also some of the ways in which that should be achieved.

So, for example, as a critical component of that, the fact that your post code or where you live doesn't determine the services that are available to you and the standards that are available to you. And in a State like Queensland where we have an extremely distributed population, part of it – we clearly, and I think everybody understands that we can't have brain surgery in Weipa. But our commitments to the principle of equity of access is significantly underpinned by our system leadership and some of the things that we put in place to make sure that if you can't get the level of care that you need in Weipa, that we provide for you through various mechanisms, including transportation, to a place that can provide that sort of equity of access. So it's really underpinning equity in the sense of access to services. What it doesn't mean is that you can get that service necessarily wherever you live in the State.

CA Thank you. Now, just turning to page 20, section 8. It talks about the management of the public sector health system.

W Yes.

CA Subsection (1) explains that the system is comprised of the Hospital and Health Services in the Department, which you mentioned before.

W Yes.

CA Subsection (2) says that the overall management of the public sector health system is the responsibility of the Department through the Chief Executive, the system management role. Could you explain a little bit about that?

W So as the Director-General, I have a system management and leadership role for the whole system, not just the Department of Health. That is exercised – so my role doesn't stop at the door of the Department of Health. My role extends to – I have responsibility for the system, and the Act outlines many of the ways I am to discharge those responsibilities, including, for example, setting standards, providing funding, providing advice and support, monitoring performance etc, etc. There's a range of things and some of which are outlined in an earlier question, a response to an earlier question.

I think there are three – I think it's useful to – this is a large Act. I think it's useful for the purposes of the evidence to consider my role and how I can execute or discharge those accountabilities, system accountabilities, in three-ways: one is the legislation itself, so the legislation defines the roles and responsibilities of the centre and the Department and individual sovereign Health Services. So the Act.

The second mechanism that I have to exercise that I can discharge my accountability through authority, through a head of power, is through what's called health service directives. So I can make health service directives. And there's a process for achieving that. So it requires consultation and collaboration. But essentially I can make a directive which requires all Health Services to do a certain thing. It's certainly been, in a devolved system, I think it's fair to say that the appetite for having hundreds and hundreds health service directives has not been high. That really we wanted to keep that to a minimum and not to bind people in, sort of, endless compliance through those health service directives. But that remains a power that I have. And there are a range of health service directives that are all published including those that pertain to information security.

And the third lever that I have to discharge my accountability is through the contracts between the Department of Health and the Health Services, which in some great detail specify deliverables of the Health Service and the funding that's provided. So those are the mechanisms by which I exercise my authority in relation to the accountabilities for system.

And it's really important – I think the Department of Health has a range of compliance and assurance functions against policies and standards that it sets. And I see that as an important role. But I think just as important as that is this notion of being an intelligent centre and not just seeing ourselves as a compliance, you know, as the policeman for the system, to see ourselves as really a coach of the system and able to draw upon our own specialist and expert advice and support. And particularly where it doesn't make sense to do that 16 different times across the system.

So, for example, in the area of information security, it makes sense for us to set a framework, to establish standards and policies and protocols. The Health Services have their own accountability to establish those and some will choose to do their own. Many will choose to draw upon model standards and protocols that we have and just adopt them.

Similarly, with training, rather than 16 different ways of training, we'll often co-develop a training that can be used efficiently across the whole system. But I think it is important to note that with respect to the sovereignty of Health Services they are accountable for making sure that they are compliant and that's an important facet of our system, local authority and accountability.

CA Thank you. And just go to section 8(3), part of the role as system manager is responsibility and (a) says state-wide planning.

W Yes.

CA And then just over the page, (d), for monitoring the service performance.

W Yes.

CA And then (e) you've already talked about that, the health directives. So we've had evidence from two of the Hospital and Health Services, they are two of the subject seven agencies; Mackay and then the Gold Coast. And it has come to pass that there are some inconsistencies between those Hospital and Health Services. And purportedly some deficiencies with respect to protection of privacy for the public's confidential information held on their databases.

I'd just like to go through some of the identified deficiencies, and with a view to the Act, and what we've just gone through as the objects and the guiding principles and Professor SMITH's evidence on Monday, with respect to the definition of responsibility. I'd just like to flesh out with you any ideas you have on how these deficiencies in the Hospital and Health Services can be ameliorated particularly ahead of the 1st of January next year, with the help if any understanding of the difficulties with their own sovereignty of the Department of Health. If we could just go through a few.

W Sure. Of course.

CA So the first one is with the new ieMR database that's been rolled out over the Hospital and Health Services. The nurses' union, have you read their submission?

W I have.

CA Did you want to be provided with a copy?

W Yes, please.

CA It is Exhibit 49. And also at the same time the 43 as well please, the Digitalising Public Hospitals Report within the Queensland Audit Office. No doubt you're well aware of that.

W Yes.

W Thank you.

CA So in the Queensland Nurses' submission, they're going to be represented here today as well later on after Mr GREEN.

W Okay.

CA On page 4, the last couple of paragraphs, and it's also raised in the Digitalising Public Hospitals Report from the Queensland Audit Office, on page 39, midway down the last two paragraphs of subsection monitoring permission and staff access to patient data. Is the general gist of both of the concerns raised there, and has been vocalised also by each of the two subject Hospital and Health Services throughout this hearing, is that there's some problems with the implementation of ieMR with the proactive auditing ability with the P2Sentinel.

W Yes.

CA And that Mackay has had the new ability, the new service for about two years, and the Gold Coast has had it as of April this year. So Mackay has managed to assist itself somewhat through the length of time it has had it, but also arguably through taking more proactive steps. And the Gold Coast is far behind. I'll go into a bit of detail in a minute.

So the first issue raised is that the reports come through from the Department of Health, as the controller of ieMR, on a monthly basis to the Hospital and Health Services, the Gold Coast said they've asked for it on a weekly basis. And it is a very time-consuming task to sort through what they say – and it is mentioned in the material – raw data. So one aspect is is there a possibility of, from the

Department of Health end, being able to provide that data in an easier, more easily, quicker assessable format to cut down on the time? Is that possible?

W So, thank you, I'm very aware of the situation obviously as the new Director-General. And you'll be hearing from the new Chief Information Officer, Damian, shortly who will give you more detail. I think there's a couple of things I'd say with that. First of all, yes, I'm very aware of it. I think it is important to acknowledge that with respect to ieMR, we are on an implementation journey and so in some respects they're – whilst a lot of work was done in the design phase and, again Damian can take you through that in terms of the governance and the controls as part of deployment, I think it is fair to say that the current approach to the P2Sentinel, which I'll try and illustrate in a moment, is – it's intent is good but I think it's execution is problematic.

So in terms of what we're doing about that, we have, as I said before, one of our two governance committees have set up a special working group now across the Department and the Health Services to refine not just the report that you're speaking of, but to get on the balcony of that issue and say "What are we trying to achieve here? And how can we do that efficiently and effectively?"

So there's a process in place now where we – we are really focusing down on this issue of retrospective auditing of potential – it's like a screening test for potential and appropriate access. So if I can just take to you to illustrate a little bit so that you know what it all means because it is management-speak. In the old world of paper we had absolutely no way of being able to audit inappropriate access. The only way we could manage that is by having records signed in and out of usually the dungeon, the bunker of the hospital, where the records were stored. But once the records are in circulation we have absolutely no way of knowing who's accessed the records. Zero visibility.

In the new system – sorry, in an electronic world, in an ieMR, we have an electronic footprint of every single bit of access of that record. And particularly where obviously we have 60,000 unique users, as I said before, each with a password we know exactly who has opened what, when, where they've gone and what they've looked at. So we now have an opportunity to be proactively reactive if I can – so there's a whole bunch of stuff we're doing from before inappropriate access may occur.

But if we just think about how do we set about creating flags in the system which we can, as I said to you, there are millions and millions of accesses per month, but how do we create some signals out of access and say, well, here's a few cases that may warrant exploration. It doesn't mean they are inappropriate access, but it is a flag. Now, those flags at the moment, because we're only just setting this off, it is very rudimentary. Those flags at the moment include things like someone whose search – whose access has a certain surname, so a WAKEFIELD is accessing a WAKEFIELD in the system will trigger. If I logon and fail to be able to get in with my passwords, I have multiple attempts to logon, it will create a trigger. And there's sort of some very rudimentary flags that then create a report out of the system. Now, I don't know about you, but I've certainly been in a situation where I've failed to be able to login because I just have too many passwords and so there's nothing mischievous or malicious about that.

So I guess the point is that these reports, which are produced after the fact, have what I would call, a whole lot of noise within which may lie a signal. And the report itself has no value until it's analysed and there's context put around it for each case. Now that takes time. That takes human effort. And that's not something you can just do in an office. You often have to then validate that with conversations, with other information. That's a lot of work.

Now in my conversation with the new Chief Information Officer, and as I've said we now – we've established a mechanism to properly unpick this and make sure that what we're doing is effective, is high-value work, and it is not wasting a lot of time. Because if we have – the more people I have in a back office scrutinising noise the less people I have caring for patients. So I take this seriously. But it's not simply a case of hiring a whole lot of people to then retrospectively scrutinise access that's going to take us nowhere. So for me there's two things in there-

CA Sorry, just when you mean "retrospective access", because you've mentioned that a couple of times now.

W Yes.

CA Do you mean where, as it came to pass, over the course of the evidence, Mackay and the Gold Coast have both built up quite substantial backlogs. Is that what you're talking about?

W No, no. I'm referring to retrospective as this access has already occurred. So what I mean – so what we're talking about in the P2Sentinel here is an extract of the millions of accesses that people have every day in the system which have triggered a flag according to our algorithm. So everybody who has tried to logon five times and hasn't made it will be in that mix, yes. That everybody who has – if anybody has gone in there, and it is John WAKEFIELD and I've got a patient called Margaret WAKEFIELD who's no relation to me, I'll be in that mix etc. What I'm saying is that access has already occurred.

CA Yes.

W That's what I mean by retrospective.

CA Potential breach in our terms we've been using.

W I think it could be. Yeah, it's a potential breach. I'm not even sure whether I would call it a potential breach actually. I would call it a trigger, a flag based on our algorithm.

CA Which needs to be assessed before one can determine whether or not it’s a breach?

W Correct. It’s meaningless until it has that validation. So there's a couple of things. And, again, if I may, I'll put my human factors engineering and safety science hat on here. In terms of engineering a system which minimises the need for a whole lot of additional work to explore these flags, I'm exploring two questions now with our information technology experts and our clinical system to be able to help this. I mean it would be very easy to say let's put on two more people in Mackay and every other hospital to work to trawl through these reports. I'm saying that's not necessarily the solution at this stage. What I'm saying is, again, two things: the first thing is what are we doing proactively to obviate the reactive. So, for example, if we have a concern about individuals who access a patient's records with the same surname or the same date of birth, our systems, it’s not difficult for us to flag that with the person at the point at which they're seeking to access it. We don't have to wait for a retrospective report, do a whole lot of work. We can put that flag upfront. That's just one example. That's the smart way of getting in front of that.

PO If I could just interrupt just for a moment. Do you mean that you would, by having a flag at that point, the person seeking to gain access, say it’s WAKEFIELD to WAKEFIELD would that have justified access at the time?

W Exactly.

PO Yes.

W We would specifically – now, you have to be careful to create too many flags.

PO That’s the balance.

W What I'm now asking my team is, if that is a particular issue for us as a flag that has a high yield for potentially inappropriate access, let's get that upfront in the system, that's what contemporary safety systems design does. It doesn't wait and create a retrospective industry which has a whole lot of noise behind it. So say, “Stop. Are you aware this person has the same surname as you? I want to remind of your obligation.” So it’s that kind of approach. So it’s what are we building in proactively so we don't need to have a whole lot of people in the back office doing stuff afterwards. Our objective is to minimise inappropriate access. That's a very important way of doing it, which is what we would call low effort, but high impact.

The second question that will we'll be exploring in respect of the particular issue that you've raised at the level of solving the issue, is at the moment our algorithms or our flags, what we're looking at are pretty rudimentary in terms of inappropriate access. As I said the number of logins with a fail, same person, same surname and so on. There are, and this won't be overnight, but I think from a maturity perspective and this will require investment, there are ways of using artificial intelligence to build in learning patterns which are much more sophisticated than that which will provide a much higher yield. So instead of getting a report every month 20 pages long, which will take five people to sort through and might yield nothing, and we might be able to have one person with a very high yield. Now, that's not going to be done tomorrow, but I think the sort of -- .

CA What sort of timeframe are you looking at, or you don't know yet?

W That's something perhaps Damian can give some more detail on. Again, and you know, artificial intelligence is an evolving science. At this stage we do not have a program which is looking to progress that. But as the new Director-General, my interest is on providing good care to patients and getting our resources into patient care. From a risk management perspective, including inappropriate access, I want to get upfront of that and I want things which are high impact, but low effort. I do not want an army of people, and I don't think our community wants that, sucking resources at the back end, which is very low yield. So if I'm producing a report for people to look after the fact, I want the sort of yield on that which is one in five cases is going to be positive. I don't want one in 1,000 cases that's going to be inappropriate access and 1,000 cases of noise that’s going to sort of come. Does that make sense?

CA It’s a very good idea and we will be having some evidence in relation to that tomorrow afternoon.

W Okay. But I’d stress that right now we have a very assertive piece of work which is addressing that issue that you've raised from essentially Gold Coast and Mackay saying, well, at this early stage of implementation we've got this report which we're struggling to deal with, instead of saying let's more people in there and I'm saying let's think a bit more wisely about how we can solve this problem and doubtless the solutions will be a mix. You know, we might have short-term increased resourcing to make sure that we discharge our accountabilities in the space, but I'm focused on doing things smartly and not just - I can’t justify to the community and to the clinicians the fact that we spend more and more money in the back office when, you know, there are much greater risks in terms of failing to meet patient care needs. So that's the world I live in.

This is incredibly important, but I think it has to be considered in the context of the best, the smartest way to solve some of these problems. So forgive me for sort of putting my technical expert hat on, but I think for me and I know for the new Chief Information Officer these are the sorts of questions that we were progressing now, and we will doubtless be kicking off work that actually seeks to address those in a smarter way rather than just sorting a short-term problem.

CA That sounds like a great way forward, but before that happens there's a couple of things: first of all the backlog.

W Yes.

CA We've got, and I don't know about any of the other Health Services, we've just picked two. With Mackay, - we'll deal with the Gold Coast first of all because that's the worst example. If we could just show you Exhibit 56.

W Thank you.

CA So with the Gold Coast, you'll see the table there of breaches. And there's the section third from the bottom, it says "Allegations awaiting assessment or investigation." And Ms BLOCH yesterday explained that literally they have pulled up stumps and they're not looking at anything going backwards in their backlog, they're leaving it there untouched, and they are dealing with new breaches as they arise. And she gave some evidence that they've managed to keep on top of those.

W Yes.

CA However, the staff who have generated those breaches, and no doubt there are some ones that aren't breaches in there, but they haven't been assessed to see if they are breaches and there's a high number, Ms BLOCH gave some evidence yesterday that they've managed to get about 300 off the 2017-2018, but even so you've got 2,500 breaches dating back almost for three to four years. That's a risk. It's a risk for people's privacy. And moving forward, particularly ahead of 1st January next year when the Human Rights Act takes effect for actions, is there any assistance that can be given to remove that backlog of roughly 2,500 breaches?

W Yes. So can I make a comment and then answer your question? So my first comment would be I think it's really important we don't call them breaches even though they may be, and this maybe our issue in terms of how we're calling these, these are not breaches. These are flags as I referred to previously.

CA They're potential breaches?

W They are potential according to our – yes. But I think it's really important from what is the risk perspective that we're really clear that there's a shared understanding of this is not people that have done a bad thing that are awaiting their assessment and/or discipline. These are process flags that we've put in the system which need further analysis to even get to a stage where they are prima facie, they're something that we need to explore. That's the first point I would make and I think that goes to my point before about signal to noise ratio.

But just to come to your, "John, you've got this risk, or the Health Services are sitting on this risk what are you going to do about it?" I think that's a very fair question. As I've already indicated, we're aware of this. It's not sufficient for us to, and I won't say, "Well, that's a health service responsibility, go fix it." I think this is a system responsibility. Our system leader and manager are their responsibility of this with those Health Service Boards and Chief Executives. And as I said, my Chief Information Officer has established a specific group to work on and address this issue, and in doing so, and he can provide more details of that, and in doing so mitigate the risk both from a short-term perspective, but also the sort of longer term perspective that I'm talking about in terms of how do we frame this risk in going forward. And part of that will include, in assessing, say 100 cases of those 1,600 on this report that are waiting to be analysed, what is the yield. Because I think what's important to me is that, in terms of risk and benefit and what we have to do, if the yield is zero out of 100 or zero out of 1,000, my challenge to both my Chief Information Officer and the Health Services and the governance of the ieMR is we have got this P2Sentinel wrong because we're just creating a whole lot of work which actually isn't eliciting breaches.

So I think for me, there's two actions: one is to, yes, so we cannot sit on that number of reports and say we haven't actioned them. That's not acceptable. That will be addressed.

CA Thank you.

W But I'm not prepared to simply pour in resources into the future to essentially - this doesn't help patients and it doesn't help my - even the legal compliance obligation, in my view.

CA With Mackay, they're a bit more on top of things, they've got about 1,000 breaches and they indicated if they had a dedicated person sitting there in Mackay for a year, trawling the reports that, one, they'd be able to get rid of it and, two, that they'd be able to build up more of a knowledge of how to assess the reports in a more efficient manner. And that makes sense. He said that he had already started to do that. And so that's just moving forward. Some suggestions from the Hospital and Health Services.

The second aspect of Mackay was the matrix for dealing with those potential breaches.

W Sorry, to interrupt. May I just pick up on your first point because I think that is an important one. We have a statewide clinical network for digital as well as the other committee that I spoke about before, which Damian can talk about. Part of what we need to make sure and I need to make sure is happening, is those, and Mackay was one of the earliest implementers, that example of learning, but through scrutiny of these reports we have a duty to share, and make sure we harness that across the system and not just have it in Mackay.

Again I think that's another obligation that I have and I think Damian will be able to speak to that, that we have to -- it may be that some investment in Mackay will help us understand better and more quickly how to get ahead of this problem. So I'm certainly very happy to take that on board as part of the evidence that's been given.

CA Thank you. If Dr WAKEFIELD could be shown Exhibit 48.

W Thank you.

CA That was provided by Mackay. Again, taking the initiative. They seem to be taking quite a few initiatives in Mackay. And that is their triaging of purported breaches. And they go through, it’s pretty self-explanatory, from blue being the ones that sort of are least serious, through to purple, and then they action the serious ones very quickly. And also on the right-hand side, they've identified vulnerable category of person being involved in Family Court matters, so acrimonious separations. Because your system, ieMR is the same name search which can be a serious matter if it’s a couple who have separated and got the same name, but one of them is concealing their location. And domestic violence and then a couple of other things.

So they then prioritise that category, even if it is just a same name search, ahead and deal with that straight away. And that's working for them to, whilst they have got this backlog they’re using that over the whole backlog. So it was identified by the Gold Coast as something that would be of benefit, but in some format, maybe not transferrable across all Hospital and Health Services agencies exactly in that format. But they would seek direction from the Department of Health before initiating that. So if there was able to be some collaboration with the assistance of Department of Health for the Hospital and Health Services to try to manage the backlog and keep on top of the reporting, potentially with some sort of assistance like Mackay are using, then that would be potentially a good way forward before the new marvellous system comes in with a low number of reports.

W Absolutely agree. So I think again, we have a system manager and leader. I have a responsibility to make sure the system is learning from each other. And I think that where a Health Service has particularly progressed a good idea and built a, in this case a decision support sort of tool around the report, we need to be harnessing that. And that's why we have a digital network, a clinical network, so I know that there's a lot of horizontal communication about that. But I think we can do better in that regard. Well clearly we have to do better. And again, I think there are two questions with respect to that: one is harnessing good ideas and sharing them, that individual Health Services may take, adapt, or build their own, which still leaves us with different ways of doing business and that may or may not be a good thing. But secondly, there's also occasions where we might agree as a system, and I think this is a better way to go, that we take a common approach. And so that we agree that we use a single approach rather than have everybody do different things. So I think there's lots of opportunity here in terms of this decision support tool that Mackay have built. And, again, I'm sure that the Chief Information Officer will be able to speak to that in more detail.

CA Thank you. And I'll just show you another couple of exhibits from the last couple of days; 45 and then 55.

W Thank you.

CA This is part of that devolution of responsibilities. Professor SMITH gave evidence, the best practice would be some consistency and some simple clear terms. You can see here the difference between the two Hospital and Health Services policies that they've produced themselves.

W Yes.

CA Both of them are devoid of reference to criminality and section 408E which they've both acknowledged they could make some improvements on. But 45 is from Mackay, it goes for six pages, and then you've got almost a report-size for the Gold Coast, 43 pages.

So in collaborating with the Hospital and Health Services and providing them with some direction to get rid of their various backlogs and maybe start to implement something along the lines of what Mackay are doing by triaging, would it be possible to also give them some direction about at least a prescriptive template they can work from so that we're not getting the differences in policies and procedures as well?

W So in respect of that, I mean, a couple of comments. I think, and I know you've heard some evidence around strength of actions. It’s clearly important that that work goes into considering how we want work to be done and that ranges from, sort of, one page to, you know, massive thesis to PhD thesis in terms of size of said document. Again, if I draw on my experience as a doctor on the frontline, the vast majority of frontline workers certainly lack the time to be able to wade through often the many hundreds and in some cases thousands of procedures that pertain to their work. So it's necessary, but not sufficient. So I think our ability to provide very clear, concise, consumable information at the point of care, and as I said before, particularly in the workflow. And that's one of the opportunities with electronic that you don't have with paper to be able to plug in specific, what they call, forcing functions in the workflow, I think is, in my view, preferential to the creation of large significant documents, no matter how good they are.

I think your question about would it be possible for the system at large to agree on a particular policy or protocol, again, I think that Damian will be able to outline to you where we have those policies and protocols centrally and how we make them accessible to Health Services to adopt and use, and which are binding on Health Services. Again, very much as a major principle of our system, which arose from our previous way of doing business, which is one everybody has to follow the central policy or procedure, is that there is safety, there is benefit, there is reliability in localising procedures to local context.

And so I have to make decisions about binding Health Services to a health service directive to a particular policy versus encouraging them to adopt, or producing a model policy or procedure and saying "Stick your badge on that. Please use that. Modify bits if they pertain to your context." And I think that's where the system, the devolve system has been, and there are good reasons for that. I think we should have very accessible model documents that can be adopted by Health Services. I think, so that's the challenge that I will certainly take on board.

We already have, and I think we've provided many of those to you, we already have model frameworks and policies and procedures and standards, and I think we can make them better and easier to comprehend for the average person. So we've got work to do. And I'm certainly committed to making sure that the system leadership defines that where it should be common and make sure they can be adaptable to local context.

CA Thank you. Nearly moving off the subject of ieMR.

W Okay.

CA If I could show you Exhibit 58. This is from a case study involving the Gold Coast Hospital that we went through with Ms BLOCH yesterday. I don't intend to go through it all with you. It's just pertinent in relation to the Commission's recommendation on page 4. Paragraph 4.

W Sorry, I don't have any page numbers on this document.

CA It should be at the top right-hand side.

W I beg your pardon, I do. Page 4, yes.

CA Paragraph.

W Yes.

CA It was a recommendation that a permanent warning message be displayed upon access to the system. Other agencies have permanent warning signs that you need to read and agree to before logging on. And this is the recommendation for the Gold Coast in response to trying to reduce the amount of breaches coming out of the new software. And Ms BLOCH yesterday gave evidence that, it is paragraphs 4 to 5, sorry, it was the warning message saying it would be disciplinary or criminal and all access is recorded, like you've had in your Department of Health. It was supposed to be, according to Professor SMITH, again, another layer of prevention so that they know that's UI.

So Ms BLOCH, and I know no doubt it probably hasn't come anywhere near your attention, but if you could just possibly speak to it now, that six months ago in May, she sought assistance from the Department of Health before making such a change and they're still waiting for a response back. So given that it is an extra layer of protection, is it possible for, as part of ensuring that there's consistencies with the Hospital and Health Services with all of the matters that we've spoken about with ieMR, that that be added to the mix potentially?

W Is it possible, absolutely. From my perspective, my view is that, there is no silver bullet. As, again, I think you've heard evidence and certainly the contemporary evidence is that any such approach needs to be rooted in culture and it needs to have multiple layers of defence. So there's no one single silver bullet to address this, but I do think we can -I do think we're missing an important accountability step. And, again, I hesitate because I would need to get various inputs to this before I-

CA -Yes, that’s right. And hopefully-

W -as Director-General, issue some kind of directive in this forum. But I will say that a warning every time you login to a system is not a strong control. And I'm sure, I mean, I reflect to my own access to information and I’d ask you to reflect on yours, every time you login to your system, if you can press a button that says "Agreed", do you read the words every time? The answer is not a personal one, the answer is a human factors one which is people don't. It’s not they’re good or bad people, they don't. So if you're going to design for safety and reliability, if you’re going to design for this, my view would be that we need to do both. We need to have that. And I think the message needs to be stronger. But at the point that you first register access to a system, yes, you need training, yes, you need education and yes, you need UI results. But there ought be an upfront training piece, an assessment to show that you've heard and understood. So a simple assessment and then a personal accountable verification. So you read and essentially sign off on a compact.

Now, that's the point where I think we both - that's impactful from a human behavioural perspective, but it’s also good evidence for us when people say after the fact "I didn't know. I wasn't trained. I didn't know I couldn't go in and access this." Which frankly a lot of the time I don't accept. But even so, I think building that in, which is essentially what you're saying, but I think it needs to be stronger at the point of initially being given access to an information system. That's what I'll be progressing with my new CIO and the system. Now, that's a simple change, but it requires a fair bit of work, so I think I would need to understand how long that will take.

I'd like to draw back my experience working in the Veterans Health administration in the US when I did my fellowship there. So I was working for the Federal Agency of Veterans Health in the US. A significant security culture. Very significant. And rather than have a separate process of education, training and all the rest of it and then just being given access, it was engineered into the system. Once I had access, I had a very limited window of time to demonstrate that I've done the training and I've been given the assurance and I sign-off, 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.

END OF SESSION