European Partnership for Supervisory Organisations in Health Services and Social Care

EPSO TAC Working-Group

1st EPSO TAC (Tele-medicine, e-health, e-inspection Artificial Intelligence in healthcare guidelines, Cybersecurity in healthcare and health supervision) working group meeting	**17 November 2021 – 09.30 – 12.00 GMT (10.30 -13.00 CET)**

Tele meeting 17-11-2021 – 9.30 AM UK time/10.30 AM CET

Participants:

Tanya Miller (Australia); Clair Bryce-Smith, Lynda Scammell (England/ EU); Hedi Harzia (Estonia); Evija Andžāne Palčeja, Kaidy Teppe, Kaja Illmarinen, Daina Kromane, Solvita Akule, Anita Fridenberga (Latvia); Jooske Vos (The Netherlands); Helga M. Brøgger, Sjur Kåsin-Hevrøy, Lars Talstad (Norway); Terry A'Hearn (Scottish Environment Protection Agency), Kevin Freeman-Ferguson (Scotland); Chalene Pek, Chrystal Lua, Candy, Chan Weng Chee, Isaac Reuben Gason, Willson Go (Singapore), Sarah Billington; Janet Ortega (England) ; Richard Hayward; Solvita Akule;

Chair: Kevin Freeman-Ferguson (Scotland)

Support and co-ordination: EPSO – Jooske Vos, Sira Consulting – Eline de Koning

Terms of reference

Welcome and introduction

Kevin Freeman-Ferguson: Thank you all for joining the working group of today and, especially, a thank you for the people who are going to speak. The agenda for today as well as the terms of reference have been circulated by Jooske Vos.

My hope for today is that we can move forward together and to get (new) ideas that we can regulate in our own frameworks. The digital healthcare and all other new technologies have real potential to make healthcare more accessible and to give patients more choice. As a regulator myself, I sometimes see things go wrong or that situations are being manipulated. This worries me and therefore we need to get our regulations right.

Without any further ado, we will go to the first item of the agenda. We asked Terry A'Hearn to speak today to give us the benefit of the experience of a cyber-attack and some of the work that has been followed from that. Terry, the floor is yours!

Topic 1. Cyber-security

Scottish Environment Protection Agency

Terry A'Hearn: Thank you for the invitation. I will give you a couple of insights in the cyber-attack that we have experienced. During Christmas Eve last year, I got a call from our governance manager (there are about 5 or 6 office holders in the organisation) – who is looking after resilience and corporate processes – and, therefore, I knew something was wrong. The manager informed me that a cyber-attack happened overnight: it is a massive, catastrophic cyber-attack. Under emergency management protocol, I declared an emergency and I point an emergency management team to run the organisation. That will always include the executive team and then whoever is relevant for that emergency. But how do we have a meeting when the computer system is down? We needed to set up an InterCall but the instructions on how to do this were on the computer system. Immediately there is a situation where you are completely cut off with everything that we do to do our work. On Christmas Eve we had three meetings, in one of them I asked if the people that worked for the company were already paid, and this was the case due to Christmas. So, I thought that we had one month to figure out how to pay people, but the manager informed me that we had one month to find out who works for the company: we did not know who exactly worked for us as we could not enter the computer system.

If you have a major cyber-attack, you are destroyed in a sense. At our company, we work with flood warnings which can be a case of life and death. There was a horrible experience in Germany, Belgium and elsewhere a few months ago that gave a good indication of what can happen during a bad flood. If you do not get the warning-and alerts signs on time and accurately in terms of how terrible a flood is, it can go bad. Somehow our people got accurate warnings and alert signs. So, the situation started like that. Eight months later, we still could not pay people their overtime and expenses. It took us that long to get the payroll system working effectively. We offer to make people a once-off payment which some people took up. However, some of the staff were getting refund tax notices from the tax office in the UK but we have not supplied the final payment roll from January to March. Therefore, this was needed to sort out with the tax officials, and we needed to inform our staff to not use the tax refunds as people should not have received this. However, a couple of months later, the tax offices are sending invoices to staff members, but these were wrong again. These are a few examples of what happened.

A couple of key lessons from that is this is going to be a couple of years in recovering. Particularly in the first few months, we will just have to get by doing what we can do. If we keep in our heads, we judge ourselves by how we are normally do our work. We all had experiences with that during the pandemic: you cannot do what you normally do when there is a pandemic. What we did was using a test everyday when we make decisions by asking ourselves the question: 'how will a reasonable person in Scotland judge us?'. For us that meant that flood warnings and alerts were to be sent out as this was our main priority.

The attack at our company was a ransomware attack and normally they want money for ransom. I have never been asked to pay ransom before. So, what do we do? We had a cyberteam set up in the Scottish government and other Scottish government officials and we had the police Scotland cybercrime team. The police were sensational: what will happen once we confirm it is a ransom attack is that they will publish 10% of the stolen files on the dark web. That happened because that is how they show that they got the files and are willing to publish it. We made the decision – which was cleared by the board chair and the Scottish government amongst others – to go live on BBC radio. On the radio I said that we will not use public funds to pay the ransom. They immediately published the other 90% of the stolen files on the dark web because they want to cause you the maximum pain. So, we set up a team of investigators to go through every line of the files and as we found anything that

was sensitive for a staff member or somebody else outside the organisation, they immediately got a phone call. So, I am just giving you a feel about what is going on.

I commissioned several audits from experts, one of the groups that we have employed looked at how everything happened. We got these different reviews that were published. We redacted information to protect the criminal operation, to protect privacy and our own operation including cyber protection. But you will find very few organisations that will do something like this as most people will stay silent about it. I took the view that we are a public agency using public money, administrating public laws, spending public money to commission the reviews and therefore we should be public about the results to the extent that we can be. Those reports can be useful for other organisations as well.

It is a horrible experience, and we will probably take two years to recover from this. Probably because we decided to build an entirely new IT system we survived. We delivered a high priority service, we have put our workforce together, we work well with our stakeholders, and I therefore think that we will be okay. If I have one piece of advice about a cyber-attack it is 'do not have one'. Next to this, dealing with a pandemic is nothing compared to a cyber-attack!

So, this was a bit of flavour about the different elements: how this it panned out in the first place, what were the sort of things that we needed to deal with and how do you protect yourself. Some of the examples you find in the report.

The only two important issues are:

1. how do you stop yourself having a cyber-attack and?
2. when it does happen, how do you manage?

Kevin: Thank you very much Terry: it is super interesting and sobering. Some of the points were: have we paid people, how do we pay people and even who do we pay. The latter is a mind-blowing fact. I think your approach is recognizable in terms of inspecting high-risk services early on and trying to carry out the most essential work. How you got access to the dark web is intriguing to me because I would not imagine that anyone could just do that. I presume you got specialist support around that.

Terry: Anyone can access the dark web. The dark web is primarily used by criminals. The police Scotland cyber team set up safe systems to look at what is on the dark web, and they would safely transfer the files to us so we could set them up in a more secure area. I was saying to all the staff members to not go to the dark web, but I cannot safely say that nobody did this. Next to this, journalists can go on the dark web and do their investigation. They may be able to write articles about (unrevised) data that have not been published yet.

Kevin: It is sobering, and I think that there is a lot that needs to be done. It is helpful because we can think of it from two points of view: one from an organisational point of view as we got sensitive data to protect, but also as a regulator as we are working with organisations that have sensitive data and what is that they need to do to protect their data. Are there any questions?

Claire Bryce-Smith: Thank you. We had a much lower-level attack. We had an e-mail bomb attack after that we had taken enforcement actions against individuals. We cannot prove any of it, but they were targeting certain individuals that were involved in these enforcement actions. I think that they took e-mail addresses and registered them all over the world. It was not spam, but thousands of e-mails were received every day. It was a very small aspect of everything that you have experienced but it was also very real. In the future there will be varied degrees in it which we need to deal with. Well done.

Terry: I have dealt with organised crime for a long time. They are very sophisticated and are impressive businesspeople. These are professional business organisations. They are publishing their client list every Thursday -we eventually got published as well. They employ people with social expertise and engineering. They are trying to build a trial that will convince you that you are getting something from a legitimate source.

Chan Weng Chee: I am thinking about organisations that we as government partner with other entities such as service providers. As being the entity that was attacked how do you manage the relationship with your other partners? How do you manage that situation?

Terry: We immediately got in touch with the BBC since we could not publish anything on our website since we had no access. Therefore, people knew about the cyber-attack. The emergency management team went calling key partners that had a lot of computer-based interaction and a regular exchange of data. Some of these partners already shut off complete interaction and to others we said to cut access with us. It was hard to reach the key partners as all the contact details were at the computer system. The other thing about is that one of our partners were hit by a cyber-attack. We had to immediately work that out as that affected our system. I do not think that our company would have survived if we had a second cyber-attack. Also, it hit our flooding service and it was flooding that day. We had to work out how to protect that. Basically, we needed to destroy some new stuff. That supply chain is very critical. You can have the best defences in the world for your organisation but if they got into one of the defences in your supply chain, they could affect everything. We took the view to protect everybody the best we could.

Jooske: Thank you very much for hearing your insights for the things that happened in your organisation. Do you have one most important lesson for regulators to share that you have learned from this? How do you protect yourselves in the future?

Terry: For regulators I would say that the most important lesson is to build the most secure cyber defences, and have extra backups, around the most important information. The other important lesson is to work out what is the most critical information or systems in terms of seriousness of information when it is getting out.

Kevin: Jooske has included some of the document that Terry has been referring to such as links from the learning reports. Now, we have colleagues from Norway joining us to give us an overview about digital security in Norway. I hand it now over to our Norwegian colleagues.

Sjur Kåsin-Hevrøy: I will give a quick overview of the Norwegian national security strategy. Norway had a strategy for information security since 2003. It is quite interesting that one of the main points of the information security strategy back then was to 'know your critical assets and protect them accordingly'. Getting the basic rights is hard but it is the main thing you can do. This strategy was updated in 2007, 2012 and 2019. The main reasons as stated in the strategy was an increase focus on the public-private partnership. Earlier strategies did not recognize the need for the private sector to have a responsibility when it comes to securing both society and the public sector. It needs to be acknowledged that some of the best in the business are in the private sector. When you are working to increase cyber security, you need to have public-private partnership.

Another major issue in this strategy is that we must understand that there is a bigger part for the defence sector to play. The reason for that comes from the threat of a hybrid war: critical infrastructure is targeted in a new way. There are international challenges and solutions. A big part in

the strategy is supply chain attacks. Nobody can have a full overview of all the components that are essential to run a secure system. You buy your hardware from someone and your software from someone else, some things are in the cloud and others are in the server. That means that you cannot have a national security that only works on the national level: you need to work on doing something in an international way.

The policy goals from the national strategy are basic. I would say that the one of 'essential societal functions are robust and designed with resilience' is new when you look back at what happened in 2003. It is an acknowledgement that digitalisation has changed society as the infrastructure is now digital. Meaning that societal functions and IT need to be and stay robust so that society does not stop functioning when you have an attach. This has been something of increasing importance.

In Norway, there is a working and steering group and a Directorate for E-health. The main idea is that we should address the sector-specific challenges. Firstly, we have a fragmentated landscape with a lot of general practitioners, hospitals and institutions which are not digitally connected in a meaningful way. They are sort of independent and they buy their own registration systems for medical journals. The digital picture of the sector is that there are a lot of different stakeholders. Secondly, due to this fragmented picture, the accountability – who is responsible for the security of this – needs to be addressed. Thirdly, everybody has a big expectation as to what the digitalisation of the health sector is going to mean That you are going to get more efficient and better quality of treatment. But there is a big gap between the ideal of what medicine can do together with information services and what they are delivering today. You do not have enough research data that is flowing between systems. Basically, it is not as good as what you are hoping it to be.

The background for the health sector is that in 2018 there was a big attack on the biggest health provider in Norway. It is expected that they got access to almost 3 million health journals. In intelligence circles, this was attributed to China, and it is expected as part of China's attempt to build a database of everybody on the planet. We also have some audits showing that information security in Norwegian health institutions is not good. There is a lot of vulnerability, there is weak security governance, and this has not improved the last years. Therefore, our infrastructure is being targeted in the hybrid warfare as well as it being an attractive target for cyber criminals.

The main report is to be presented in March 2022. What we are aiming at is that responsibility and accountability is explicated. As our sector is highly trusted by the public and amongst collaborating practitioners, units, and institutions this should be complied with in future developments and operations. We hope to be able to implement new technology securely. Since Norway is a small country, we need to be much better in having a common infrastructure and coordinated shared services that is used for secure digitalisation. So, if you are a general practitioner or a big hospital you should know how to get access to the most specialist competencies regarding cyber security that exists in the sector.

I took out some activities that are interesting and will become more important in the future. One of the things that is proposed is mandatory pen tests from the health sector. If your hospital has internet facing, somebody is going to try to hack into it and see how far they can get. One of the official governmental organisations is going to do this. They also want to make a new skills and knowledge-program regarding cyber security. The idea is that cyber security is necessary for everybody that works in the health sector. The IT people need to know one thing and the personnel working in the health sector needs to know something else and both groups need more education. There is also a move to strengthen the national health emergency planning regarding the IT crisis. Traditionally, the plan is based on a mass incident or a pandemic. All hospitals systems for journals

are down, that is not coordinated on a national level: this is what they are going to work more on. There are also suggestions for login tools: this can be used to detect if something was stolen or not. The openness of evaluation is going well in Norway. It is common to say if you are hacked and what you have learned from the incident (however without being very specific). Compared to many, there is a strong idea that you should tell everybody about how and why and what could have been done better. There is also going to be a strong initiative about the most critical infrastructure objectives. Going back to the plan of 2003: know your assets and your critical information and protect them. This is something is obvious, and we will keep trying to do this better.

My idea with presenting this was to give a quick overview. But most people have different ideas and views. I am very interested in the questions, and I am looking forward to discussing this.

Kevin: Thank you very much Sjur: that was interesting. There is a theme going through in your presentation and what Terry was saying about what is critical and about applying the best defences to the most critical systems. Could you tell a little bit more about what your expectations are about pen tests? Are you looking to an ongoing plan around that? Is there a coordinated approach to that kind of pen tests?

Sjur: There are different levels of knots, and those people work at the search. They know about the informatics; they read it and understand what is wrong. They have been working in the health search meaning that whenever there is an attack, they will go in and help whatever hospital is attacked. Also, they can and have been asked to do pen tests on demand. Let's say that you are a big hospital, and you are wondering if anything can be done to improve the security. They go in and they do a pen test both from inside and from outside the network. The demand has gone through the roof. It started out with a voluntary service and now they are asked to do these test alle the time. The idea is that they are going to do it often. But should it be a regular part of the quality system, or should it just be once a year per institution?

Kevin: From our point of view, I think there is something about a regular test to check the security of the systems within the organisation. Everyone's hardware is refreshed every now and then, updates and different parts of the organisation procure different bits of digital software. The systems are evolving all the time. From our point of view, we regulate a range of organisations that provide health care. But what kind of expectations do you put on smaller organisations as they also are required to have security. The relative investment needs to be associated with the risks. How much investment and what is reasonable in terms of expectations in terms of the services that we regulate in terms of digital security and how we might understand the risk and expectations in terms of investments around that?

Sjur: Regarding the first thing about what you said about knowing your assets and the critical infrastructure, what I see evolving is that an asset was first an object that was somewhere, and you tried to protect that. Now, you see that people are trying to protect 'a function' such as 'providing healthcare'. What do you need when you need to provide healthcare? The risk analysis framework has gone from protecting the assets of (e.g.) medical journals to protecting reasonable health care. If you lose access to your journals, are you still able to provide health care? These are different sorts of analysis.

Kevin: That is interesting. What are the key things that we need to protect rather than what is the composite range that needs to be protected to deliver our regulative functions and essential services to protect the lives of people?

Sjur: Being able to provide critical societal functions is something that can be a target of sabotage. This is typical for hybrid warfare. Those things are important.

Jooske: Have you also heard that they try to target not only the large organisations but also especially the smaller ones as these are less protected. Have you heard about this as well?

Sjur: Yes, that is something that we have read about in the different kind of threats that are collected by different organisations in Norway. A function of how an attack is done: you have an automatic program running for vulnerabilities and if the program found a vulnerability, you are looking if you can get further in and if you are successful, you see if you have valuable information or not. If you have a very good detection team working for you, you often find an attacker, but they have not started doing anything yet. Mostly this is because they are checking every organisation and maybe you are just not on top of that list. We have seen this in threat evaluations.

Kevin: This entire industry is entirely profit driven and it is about how you can manage the information that are hold by people. On the day that you are subject of an attack, the individual that is causing the disruption has most likely been snooping around for a longer period. It is an important topic.

I think that there are two areas of work here:

1. we can try to consolidate advice for our own organisations and around what people are doing around cyber security to make sure that we got everyone in our network protected as much as it can be.
2. Also, there is probably a guide about expectations in respect to digital security that could be created for the services that we regulate and the organisations that we have supervisory responsibilities for or that we inspect or regulate. It would be helpful as if we could be able to provide additional information to our organisations that we regulate to guide their thinking around this topic.

Are there any other questions and thoughts before we move on?

I was thinking that it would be helpful to propose these ideas at the end of each session and when we are getting to the next steps, we can look for volunteers that might take these ends forward.

Helga Brøgger: A suggestion to get all the people to participate in the discussion of the action points that we are agreeing on. We can use the Mentimeter, for example, to vote for the next topics and then all of us can pull together all the knowledge. The beauty of it is that there is an immediate response from the whole group during the discussion. This might be easy to cope with.

Jooske: Maybe a reaction on the report would also be useful? You may want to add points that you can add to the agenda of next time or put a question at the end of the report so that everyone in the group can have a very short reaction to that.

Besides Mentimeter seems a good idea we will see if we can manage that next time.

Kevin: Good. **We will move to the new topic then**. This is around **intelligence sharing and cross-border intelligence.** Probably we will also get into the experiences of regulating online services. There is a lot of learning and experiences already been going on to take this area forward. I hand it over to you Claire!

Topic 2. Cross-border regulation and sharing intelligence

Claire Bryce Smith: Thank you so much. I am going to run you through the experiences on regulating registered pharmacies. We are a unique regulator in the UK: we regulate both the professionals but also where they are working retail community pharmacy. We are the regulator for pharmacies in England, Scotland, and Wales. Our focus is patient safety and upholding trust and confidence in pharmacy. We do that by setting standards such as education and training for both pharmacists and pharmacy technicians but also standards for registered pharmacies. To operate, they need to be registered with us and they need to meet our standards every day. If they do not, we will take proportionate action.

In terms of how we regulate is under the umbrella of our vision of 2030. Our regulator philosophy is our core focus, and it is to ensure that pharmacists can provide safe and effective pharmacy at the heart of healthier communities. We are outcome focused. We are heading towards and working on how we can practice more of an anticipatory proportional approach to regulate. What that means is that we are trying to be more intelligent informed, more agile and trying to get ahead of problems to minimize the impact of them. This is how we are doing our online work.

The regulatory framework that we use is probably very similar to many of you. We have standards for registered pharmacies. We also have the standards for pharmacy professionals. So, they should both work together to provide that safe and effective pharmacy care. Where our standards are not enough, such as the existence of online pharmacies and online delivery of services, we provide additional guidance which is a guidance that is regularly updated. This sets out additional requirements of how to meet our standards. Online pharmacies are about the people that go online to supply medicines and online prescribing services by themselves or elsewhere.

We have 26 standards in our standards (quality) framework. If pharmacies meet those standards, they should be able to deliver safe and effective care. The point about these is that they should be applied to any setting. Risk assessment and risk management is where it all starts and fails – and is particularly important for online pharmacies. Other things around information governance are more around GDPR (data protection) We are probably not asking the right questions around cyber security – also looking at the stories that have been told this morning. So, the standards framework starts with governance where all the systems are put in place, then the pharmacy team itself that is working there, then the premises, which is the website for online pharmacies, then the quality of the services, the equipment, and facilities.

In terms of the distance, we must opt in our requirements that we are looking for. It is all based on the principle that medicines are not ordinary items of commerce. Because people are going online more, we have strengthened that guidance to ensure that medicines are safe and clinically appropriate. In particularly we put further safeguards in place for medicines that are liable to abuse such as the opioids and laxatives. It covers any third parties who may be working with that pharmacy even in the UK or abroad. That is being a powerful element as how we are regulating because that covers prescribing services as well.

We are looking to make sure that the pharmacies are taking those steps to minimise risks that they identify. This is not only in the way as how they provide these services but as well by medicines. This is context specific. We are looking to make sure that they have done a thorough risk assessment including if they are working with prescribers who are not regulated. We are also looking to make sure that the medicines are clinically appropriate. This comes down to making sure that they got all the information they need from the person receiving the service. Many of these that are inspected are online questionnaire-based models. Identity checks are a major thing online: making sure that they are the person that they say they are and making sure that their system have all the checks that

they need when people, for example, are slightly changing their names or postcodes. This is particularly when people are abusing or misusing medicines. We are looking to make sure their systems can safeguard against those. Identifying requests for medicines that are inappropriate: a combination of medicines that is build into the systems but also making sure that persons cannot choose a medicine and its quantity before a consultation. Obviously, further safeguards are pointed out for medicines that are liable to abuse. We ask that they are contacting the General Practitioner to make sure that the prescription is appropriate.

We have been targeting, because of intelligence, the worst likely models that are the riskiest. These are questionnaire only based models and are often using prescribers that are based in the UK, are independent or they can be medical prescribers from other countries. We have found a lot of failures for these types of models which are well below our benchmark of 85%. As a result, we had to undertake enforcement actions to stop people being able to supply higher risk medicines and a lot of professionals have been referred to our FtP which is sort of our disciplinary angle.

We have learned that those clinical services are being added on to what was a transactional supply model. They were never designed from a clinical mindset and point of view. That has led to a few problems. The people that are working online, there is a lot of technology involved in these models and service delivery. Particularly when they are working with several providers, different systems are not well integrated. The people who are working within them, do not tend to understand all the functions or how to get to the right information in the system which is leading to failures. We also found a lot of weak leadership and governance. Particularly around clinical governance, the setting is underdeveloped. Risk management around safeguarding was not good. A lot of the time, people have not the insurance in place to protect patients. What some of that comes down to is that when we are looking at the way these online services have been put together, there is a little bit of a blindness in the virtual world. We found out that the GP abroad did not really know the patient and what he or she was doing. The number of independent prescribers is increasing rapidly. They are increasingly being used even though they are less experienced in this setting. The standards for registered pharmacies and pharmacy professionals, they are meant to work together: if the system is failing, the professional is meant to kick in and stop problems or issues or patient safety risks. In this occasion, both have failed numerous times (even though a lot of people are doing very well). We cannot forget that people are making money of this. There can be an imbalance in the amount of money people can make and the patient safety concerns.

The fact is that we are fully aware that we are regulating in a very disruptive immature innovation. This is evolving. We are constantly trying to keep up with the different models that are being developed. We do notice that we have a bigger issue around clinical governance structures in community pharmacy which is online where mostly inexperienced prescribers are operating. To be fair, there is also some conscious and unconscious incompetence. Some people are making poor judgements because they do, or they do not know better. There has also been a fast increase of the number of people that are accessing healthcare services online but there has been little public awareness or education to help and inform people of the differences and risks so they can make proper decisions about which providers they are using. Of course, we are also working within a national policy and a legislative framework that was written before such models emerged. There were some loopholes, but they always tried to apply old legislation and policy which is sometimes innovated.

For us in the UK – as a part of Brexit – we continue to recognize the EEA (European) prescriptions which means that some of the business arrangements that we see can now include elements outside

of the UK regulatory control. It is not illegal but there are additional risks and safeguards that come into play.

An example of a patient that goes online to secure the prescription and medicines for a condition: We have a private healthcare provider who operates in the UK. They use pharmacists' independent prescribers, and that person can go to them depending on the condition and get a prescription. They can then go to a UK pharmacy to get that prescription and then it will be sent to the patient. EU Meds is a portal that connects patients with their registered EEA doctor. It means that patients from the UK can get their prescription from a doctor in the EU which is send to a UK registered pharmacy which is delivered to a patient. These business relationships are a lot more complicated than before. We found multiple examples of this. There are real patient safety risks, especially for the ones that are misusing this.

I wonder if there is some mileage for cross border collaboration. In one of these examples, the prescriber was signing of 500 prescription a day for high-risk medicines. Then we must ask ourselves if somebody that is working with a questionnaire-based model, is he really paying attention to whether those medicines are going to be clinically appropriate.

Kevin: Thank you very much Claire for taking the time. Are there immediate reactions on the presentation?

Helga: The key point is that patients are not consumers. We know that and the healthcare providers know that, but the citizens are completely unaware of this. From a regulatory perspective this is important, so somehow educating our citizens is important. This can be applied to the several technologies driven innovations in healthcare.

Claire: I absolutely agree with you. I think that people think it is legitimate as they are getting a prescription.

Kevin: There is a principle in terms of the digital healthcare as medicines are not ordinary items of commerce. In the UK you are not allowed to advertise to the public 'prescription-only' medicines. There is a fundamental point of principle around patients speaking to a clinician about how they feel, what is wrong with them or why they do not feel well, and which way forward is best for them. Informed consent is key: being able to understand the risks and benefits of costs of treatment regardless of what it is, is essential to that relationship between the patient and clinician. This can be picked up by us as well. Are there any other questions?

Jooske: This topic of cross border providing medicines might have different elements that should be inspected. What do you say is this something to look at cross border and how could we work together in your opinion?

Claire: For the UK it would be most helpful if we do not recognize these prescriptions anymore as everything will fall under UK regulatory control. The reason people are doing it is because they are outside CQC regulation or health improvement Scotland/Wales regulation. There is a little loophole there. In terms of cross border, the problem is that we do not always know to whom we need to report. We know that some of these medical prescribers cannot be paying the full attention. We are dealing with the pharmacies and taking the enforcement actions saying that you have not done what you should have done. However, we do not know how to really flag up to the respective regulator. That is something we must look at because you cannot hand high risk medicines to people based on a questionnaire-based model. It is about knowing where other regulators are, how we could be more

efficient in letting people know and forward that information. Secondly, it is about having a forum to look at models. It may be done on a case-by-case basis.

Jooske: Maybe you are also looking for some specific elements of these e-prescriptions? Could it be helpful to find these specific elements that are misused by e-prescription; do you look for a kind of overview on topics that are important for the e-health inspection work?

Claire: I think that it would be the medicines that are most likely to be abused. Because these are the ones that are causing immediate harm as people are dying. Obviously, people themselves need to play a role as well. But the focus can be on these high-risk medicines as this can be helpful.

Kevin: This is about linking and sharing intelligence across countries and there is something around high-risk medicines. Especially when you are a person who is intentionally looking at avoiding safeguards as they are dependent on the medicines combined with a financial motive for high value medicines. It is a drive to supply that demand because it makes money for people. I think it is about tackling that relationship.

Lynda Scammell: We are the regulator of medicines, medical devices, and blood products for human use. We have a lot of concerns about medicines that are sold online. Most cases that we are looking into are medicines that are available on our site that is based somewhere without any regulative controls. We have had increasing complains about this kind of website that involves a legitimate supply mode for the patient. They can go on a website and be directed to a healthcare provider who makes a diagnosis and can describe medicines.

I support everything that the healthcare regulators have said: we are all working hard to explore this. Another couple of things to say about this is about that clear motion to cross border activity. Worth knowing is that in Europe what you can and cannot do various from country to country. Out of the 28 member states in the EU, some like 6 are allowed to sell medicines online including the applied rules. This also means that the rest of them do not allow this. We get a lot of complaints of countries where medicines cannot be sold online but what happens is that patients will pick a county. The patients will go to a website that prescribes e-medicines. What happens is that the medicines go to the patient in another country and that is not legal in the country where they are living. The complaints tell us to take down the website as there are illegal activities taking place. This is difficult because this is where jurisdiction and cross border activity is important since it is not illegal in the UK, but it is illegal in for instance France. This is difficult because one country is allowing one thing and the other one is allowing something else.

Another piece of information that would be helpful to know is that there is an EU resolution on distant supply of medicines. This is what we are trying to update with information about this. We are doing a series of interviews with countries of the EU. That will give you even more variants at what state the countries are at in the case of e-medicines. We have managed to contact everyone to conduct this information. We are setting up a record of all the agencies that might be involved in the patient journey. The pandemic taught us that collaboration is everything. We know that the internet does not have any boundaries and we must expand our thinking about this. We need to contact relevant agencies in other countries. The only way to get a blueprint to get this right is to collaborate.

Kevin: Thank you very much.

Topic 3. Effective regulation of telemedicine and AI driven devices

Kevin: After the next presentations we will go over to the final part of the discussions and conversations in the working group. I hand it over to you Weng Chee!

Weng Chee Chan: Thank you for the invitation. I will approach this very quickly from the perspectives and experiences of Singapore. I have prepared something for the three focus areas: telemedicine, artificial intelligence, and cybersecurity. However, a lot of points regarding cybersecurity were already pointed out by other presenters. Therefore, I will mainly focus on telemedicine and artificial intelligence. From Singapore's perspective, we recognized the growth of digital health trends such as telemedicine and artificial intelligence. We have several regulatory tools to address these risks. This ranges from things such as stakeholder education to sandboxing, innovation and new care models as well as legislation. I will go to each of the areas.

In terms of regulative tools that we use, we started paying attention to telemedicine in 2017 to 2018. We noticed that there were a lot of new standalone telemedicine providers. They did not have a physical premise and it started offering consultations over video or phone. We saw that this was an area where we needed to better understand the risks. Our clinicians were equipped and empowered to use telemedicine in a safe manner. It was a sandboxing kind of approach with a couple of telemedicine providers where the intention was to better understand the risks, co-create effective mitigations and to use the sandboxing structure to test some of the mitigations with the view of supplementing future regulative requirements. Through that experience, we are thinking about how we do then put in place these regulative requirements. This will come in the place of licensing telemedicine providers in 2023. Some of the challenges that Singapore faces in telemedicine is that due to the pandemic, online consultations went through the roof. The issues that we are facing are about the use of telemedicine in different settings when used by different healthcare professionals. This might not be the same as before. So, what does this mean and how do we apply a different regulatory approach when we talk about telemedicine use amongst different providers in different settings?

Another challenge that we face is that we typically regulate and license only 'direct providers of healthcare '(such as hospitals and nursing homes). With the event of telemedicine, we see more and more 'telemedicine platforms 'such as companies that purely come in to provide the platform as a service to the traditional healthcare providers. Many of these platform providers may influence care provision such as the usability of the platform or the clinical standards that are incorporated in the platform. What happens if there is a security breach in such a platform and how are we going to regulate this? Some of these platforms do engage in a form of advertising and how do we then ensure that these providers are also ethnically and morally in line?

I think one of the issues is the risk of cross border regulation and provision. In the provision of telemedicine, we face a situation whereby our patients in Singapore want to consult overseas clinicians and vice versa. We know that there are differences in procedures: some of these will be recognized in our jurisdiction and some will not be recognized. How do we go about ensuring that the patient receives safe care? Therefore, a lot of things that we are trying to do is consumer awareness and educating consumers and patients. Because we know that in overseas consultations, there are risks involved. If something goes on and you want to make a complaint about an overseas clinician, there is little that Singapore can do as we do not have (a lot of) jurisdiction overseas. These are some of the key challenges: raising consumer awareness, updating our guidelines, educating our patients and physicians on how to use telemedicine safely. Those are some of the basic building blocks in terms of what we need to improve.

In the space of artificial intelligence, we have two different authorities who are looking into different aspects. In terms of the medical devices, we have a separate health authority that looks at regulating and licensing of such devices. The other authority looks at regulating healthcare services.

In the context of AI, we are looking at how AI can potentially be used by a healthcare professional. We have not yet looked at AI as essential in providing healthcare services. I think increasingly that we need to recognize that the use of AI is going to be more prevalent in the healthcare space. We can imagine a future where a robot will diagnose you independently of a clinician. This brings an issue of legal liability, medical liability, accountability, and responsibility. But who is responsible if a bot diagnoses you wrongly? And how do we regulate this legally? One of the guidelines that we have in terms of AI needs to be updated frequently to look at the rapid developments in this space.

Essentially, we need to bring together the AI developers and the implementers. The developers of AI are used to working with one of the authorities in Singapore, but they need to work also with the healthcare professionals as they need to effectively use and implement this AI in practice. We need to actively involve the end-users in the development of the algorithm. That is what we are trying to push forward in terms of our guidance. We welcome any feedback on our guidelines or based on your own experiences.

The issue of the rising threat of cyber-attacks in Singapore is the low organisational emphasis on cyber security. During the pandemic, our general practitioners were involved in containing the covid situation. A lot of time we get feedback that cyber security is not on their mind. Their view is that only larger organisations with useful information will be hacked and that no-one is going to hack small providers. How do we then empower and support our private health institutions to improve their cyber security posture? As a regulator, how do we ensure that this is up to certain standards? We are on this journey where we are starting off with guidelines but with the view to move towards enforceable standards. We are trying to make sure that the community is embracing these standards without ensuring them that they are safe when implementing them. Because cyber-attacks can happen to everyone everywhere, I think that the management post-attack is critical.

Kevin: Thank you very much Weng Chee. Because of the time, we will go straight to Norway and then afterwards we can go straight to the next steps. Over to you, Helga!

Jooske: Just a quick point of information. I think the presentation of Singapore is very interesting. We will share the information and ask you to investigate it as it can be a good topic for our next working group meeting in February.

Helga Brøgger: Thank you. I am going to give you a quick overview of the Norwegian Board of Health Supervision. We are the supervising authority of child welfare services, social services and health and care services in Norway. All services are subject to supervision whether they are provided by municipalities, private providers, or publicly owned hospitals. It is important to know that we do not irregulate, but we inspect. The Minister of Health provides the standards and the political adopted act that we use as a framework for our supervision. We work independently of political governance, and we make the decisions about which topics and services should be supervised. These priorities are made mainly on the information about risks and vulnerability.

We work actively to ensure that organisations that provide child welfare, health and social services use supervisory reports in their efforts to develop management systems and to improve the quality of services. We use several methods: area surveillance, incident-related supervision and proactive or preventative supervision of services. Between 200 to 400 system audits are carried out each year and they are available to the public at our website. We also use two or three areas for a country-wide supervision.

In June 2019, the board of health supervision established a taskforce that provides advice and guidance on various ICT issues. The emphasis is based on patient health and care. The taskforce has

made clear that there is an organisational and regulatory gap between IT operations and those who provide healthcare. Those who work with ICT systems in the health service must get a better understanding that their activities and priorities have direct consequences for the healthcare provided. From a patient safety perspective, it is important to ensure that the work with these systems is more patient centred and those who support these systems have the knowledge of what healthcare is and what the risks associated with it are. The people who work with ICT in healthcare services must learn to be an important part of the value chain where all personnel is co-dependent on each other to ensure the main goal that it is a safe and successful procedure without adverse effects for the patients and personnel.

The taskforce group has published a report. This deals with how hospitals are prepared to be able to provide services and proper healthcare in the event of major events. The first report was piloted where they conducted five enterprises. The main finding was that the enterprises have mostly identified the systems that they see as critical. They also have emergency procedures for key functions such as the ordering of tests and investigations. Very few of the enterprises would be able to maintain an overview of admitted and scheduled patients in the event of a loss of critical ICT. Of course, the risk of failure increases with the increasing 'downtime'. There is some unresolved delegation of risk responsibilities between the health trusts and the ICT providers regarding the preparation and approval of risk assessments. There is quite a variability in the quality of contingency plans and practice in case of downtime events. Enterprises think that the emergency procedures are stored as paper folders in the necessary departments, but these contingency plans are tested with real-world evidence in the cases of unplanned downtime events. There is also a practice of evaluating and learning from downtime events.

The next report has examined this further. They have a lot of reports concerning downtime events of one system, but none have done an evaluation of all the ICT systems. These risk assessments often focus on the technical aspect but little focus on the effects on the clinical activity. They have no systematic overview of the ICT cases with technical issues that have the most effect on healthcare and patient safety. There will be a significant risk of failure in health services once the electronic patient record system has been inaccessible for two hours.

We are also in the final stages of a risk assessment of where errors and deficiencies in the use of ICT systems have the greatest consequences for patient safety. We see that the health professionals are dependent on and at the mercy of ICT tools providing healthcare services. The process of digitalisation of health services solves known challenges but it can also lead to unfortunate incidences. We have learned nine different risks that have a corresponding patient history. We have used knowledge gathered from this report to prioritise our own work in the future. We will investigate the technology that is used to administer drugs inside the hospital and primary care. We will look at the systems and applications used for telemedicine. Also, issues related to the use of medical devices. This report was essential as an internal document, but we will publish it nationwide. Therefore, we hope that the healthcare professionals use this as an inspiration for their own work. I have explained to professionals the downside of not having a working system. They do not understand that this is a critical problem.

Kevin: That was interesting Helga! What you are doing around risk assessment and the fact that a lot of patients and healthcare providers entirely rely on systems: it is a real issue and of course a real inability to continue the care if those systems fail. Those are sobering thoughts. I think that system providers think that there is a special requirement when working with ICT systems. But they do not understand that these systems are critical to delivering healthcare. Are there any questions?

Summary notes and next steps

Kevin: It feels to me in terms of the discussions that we had today that we had three key streams of work that we would like to take forward. There is cyber security, there is practical advice and support for regulating healthcare and expectations and what we need to be looking for as we move to a more digital age and how do we get clinical assurance around the use of telemedicine and algorithms. Furthermore, we need to make sure that there are no situations where prescribers are prescribing huge amounts of high-risk medicines daily, and how we link together the different organisations that must work within jurisdictional boundaries regulating services that are provided across the internet. That is not unique to healthcare, but the delivery of healthcare has safety issues that needs to be addressed.

Jooske: That is a good summary Kevin of the three main points. The further steps must be done together, we will make a proposal to the group for that and in the next meeting we will include de Mentimeter too.

Lynda's input was also very interesting in the sense that they are apparently in EU context working on sharing information about providers. Maybe we can include in this also the regulators and inspectors of our EPSO network. It could be very helpful to have contact points and phone numbers to share information.

The reports mentioned by Helga are also very interesting to include in the work of this group as well as well as the other topics and information mentioned in this meeting by Singapore and others.

Helga: Yes of course, we will share this in a couple of weeks.

Jooske: To the group: What do you think about this format of talking to each other for 2.5 hours? Because normally we have only one hour of conversation in our monthly C19 Taskforce meetings.

Kevin: From my point of view, we would not have managed to get through all the discussions of today if we would have done like normally in an hour. Moving forward we can look at whether meetings are taking more or less time and plan accordingly. Today it has been a valuable use of time with all the presentations that we have heard and the key points that came out of it from different regions of the world.

Sjur: I wanted to second your opinion about the time schedule. It was appropriate for today as it was relevant for everybody. For the future we can think about having working groups for one of each topic. Then people who are most interested in each topic can get together.

Kevin: That is a great idea. We can make some subgroup meetings in January to kick off some more detailed thinking in each of those areas and bring this to the February meeting.

Jooske: Maybe we see where you are most interested in and to see if we can find a way in the February meeting to focus on one topic per timeframe, so that we still have all three topics in the meeting but in selected time frames so that people can choose in what timeframe they want to participate. This leaves the opportunity to choose for one or for timeframes depending on preferences and available time.

Kevin: What I will do is to pull together the thoughts and resources of this meeting and send it to Jooske. We can plan and send that around and we can see what the next steps could be. We might get the Mentimeter involved to have an immediate voting next time We can look at these views in the following weeks.

Lynda: I can also share some information, but I must wait until there is a finalised document. This will be from an UK perspective. We do have a great cooperation with Scotland so you can always share that as well. There are ways and means to extend this further. I always recommend that when everybody put their mind to it, we can create a blueprint. As we agreed, different countries have different ways of regulating things: therefore, it might be worth to share best practices. We must have something written before you take it to other organisations and so forth.

Kevin: Agreed. A blueprint can help to pull all the information together. Within the blueprint we can formulate some general principles. It is not necessarily about what needs to be done but about informed consent. However, we still look at the same outcome.

Jooske: to the group: If you know other people who do want to join, please let us know so that we can invite them and share information.

Thank you, Kevin, for chairing this meeting. See you all in February and will keep in touch in the meantime!