HEART
HIGH-QUALITY TECHNICAL ASSISTANCE FOR RESULTS

# Technical Support for the Development of Telemedicine with the Ministry of Health: Data Protection and Cyber Security

## Recommendations Report v.2.0

Prepared by Oliver Hoare, Robert Pritchard, Elliott Atkins of the Cyber Capacity Unit Ltd, with assistance from Anis Fuad on behalf of Oxford Policy Management (HEART) for the Foreign, Commonwealth and Development Office.

10/06/2021 – Draft 2.0

HEART

Clarendon House
52 Cornmarket St
Oxford OX1 3HJ
United Kingdom

Tel. +44 (0) 1865 207300
Email: HEARTforEACDS@opml.co.uk

## Table of contents

# 1 Introduction

This consultancy has been commissioned by the Foreign, Commonwealth and Development Office (FCDO) as part of the UK government's Digital Access Programme (DAP). The work has been undertaken by the Cyber Capacity Unit (CCU), working through Oxford Policy Management (OPM). CCU is a UK company with extensive experience of assisting governments and public bodies, bringing international best practice and experience to bear on regional cyber capacity building projects.

The aim of this project has been to produce technical recommendations for the Indonesian government, '**‘**Ensuring a strategic focus on data protection and cyber security within telemedicine regulation and standards, to ensure the protection of users' is prioritised.'[1]

This report, along with an associated conference (which will take place virtually on June 15 & 16 2021), are the main deliverables of this engagement which began in November 2020. The work has relied on quantitative and qualitative research through extensive stakeholder engagement, and as such, we would like to thank the Indonesian government for their full cooperation. In particular we would like to thank the Ministry of Health (MoH), the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information Technology (KOMINFO) and the National Social Security Administration for Health (BPJS Kesehatan) for their open and prompt responses to our requests for information and meetings, all conducted with congenial goodwill and professionalism, which has been much appreciated by the CCU team.

In addition, we also thank all those stakeholders that have contributed to this study from the private sector, academia and other professional healthcare bodies (a full list of stakeholders can be found at Annex A), again without their assistance this study would simply have lacked integrity and credibility.

Finally, we thank the FCDO DAP team based in Jakarta, who operating under very difficult COVID circumstances (as have all stakeholders), have provided constant and unwavering support to the CCU team, who are based entirely remotely.

[1] Foreign, Commonwealth and Development Office, UK Government Prosperity Fund – Indonesia, Digital Access Programme, Technical Support for the Development of Telemedicine Regulation with the Ministry of Health: Data Protection and Cyber Security, *Terms of Reference* for Consultancy Services, Oct 2020

# 2 Executive Summary

It is universally recognised that the healthcare sector presents an attractive target to cyber attackers. Healthcare professionals handle some of society's most sensitive personal data in the form of medical records, increasingly held and shared in digital format. Furthermore the wide adoption of enterprise and operational digital healthcare technologies, designed to protect and ultimately save lives, present a rich opportunity for digital blackmail, known as ransomware. The situation in Indonesia is further exacerbated by a lack of resources, understanding and expertise in data protection and cyber security across the healthcare sector.

Cyber crime, and specifically ransomware, is on the rise globally across all sectors, with estimated costs running into many billions of dollars (although what is less well reported is that costs double for those who do actually decide to pay any ransom)[2]. Indonesia is no exception, according to Interpol, Indonesia currently has the highest number of ransomware attacks across the entire Association of South East Nations (ASEAN) region.

The impact of the global pandemic cannot be understated, placing unprecedented stress on medical services and associated technology systems and acting as a catalyst for cyber attacks. There has been a profusion of COVID-19 related ransomware, online scams and e-mail phishing campaigns, as well as nation state hackers attempting to steal highly valuable vaccine data and IP.[3]

The threat to healthcare has became so significant that the UK and allied cybersecurity authorities took the unusual step to issue a joint cyber security advisory[4]. Yet, according to a recent study by BSSN, cyber security within the Indonesian healthcare sector is not seen as a priority, identifying a number of specific areas of weakness, including governance and security frameworks, as well as a general lack of awareness, resources and staff training.

> "The Indonesian health industry has not fully realized the importance of the security of the information they manage. Information security governance is not yet a priority among circles of health actors."

*BSSN Whitepaper 'The Indonesian Health Sector', 2019*

In January 2014 Indonesia began the roll-out of one of its most ambitious national policies, Jaminan Kesehatan Nasional (JKN), a universal healthcare programme. As a geographically challenged nation with diverse communities (the world's largest archipelago of over 6,000 inhabited islands), in the midst of the current global flu pandemic, telemedicine services have become an essential lifeline, providing improved access to frontline healthcare. Securing telemedicine services is critical for continued availability of these new and essential services, and robust data protection is also required to boost patient confidence and trust in handling their personal data.

The pandemic has of course driven up the use of telemedicine services, acting as a positive accelerant to existing programmes. Early during the pandemic, along with recommendations to limit visits to health facilities except in emergency situations, the Indonesia government provided the regulatory flexibility, allowing health facilities to provide telemedicine directly to consumers. In addition the Ministry of Health signed MOUs with a number of health and telemedicine start-ups. This has driven up the development and use of telemedicine services, for example the new JKN

[2] *The Real Cost of Ransomware*, Forbes Magazine, June 2020 https://www.forbes.com/sites/adambradley1/2020/06/11/the-real-cost-of-ransomware-and-how-we-stop-paying-it/?sh=ddc954b6e510

[3] *Hackers 'try to steal Covid vaccine secrets in intellectual property war'.* The Guardian, Nov 2020 https://www.theguardian.com/world/2020/nov/22/hackers-try-to-steal-covid-vaccine-secrets-in-intellectual-property-war

[4] *https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development*

app has been downloaded 10 million times, compared to 3 Million at the end of 2019. Yet more is clearly required to provide wider coverage and increase uptake across a population of 270m, and as such the DAP is working closely with the MoH to assist with digital inclusion.

This study, and the 12 recommendations outlined within it, are designed to address some of the telemedicine data and network security vulnerabilities outlined above. However, in so-doing our recommendations, if implemented correctly, can also provide the foundations for longer-term digital security across telemedicine and indeed to wider healthcare digital services. The following recommendations have been arranged as practical achievable steps, mainly at the national level, on which future cyber security across the health sector could be built upon.

It should be noted that Indonesia is in the process of ratifying a Personal Data Protection Bill (PDPB) and a National Cyber Security Strategy. Our recommendations are designed to align with, and support, both of these important landmark policies.

Data protection and cyber security are clearly closely linked, and whilst this report deals equally with each discipline, we have grouped our findings under the following headings:

- Security framework
- Cyber security awareness and culture of data protection
- Collaboration and cooperation
- Skills and professional training
- Governance and risk

Within each of these headings we have identified specific, practical, recommendations (see below). Our main finding being the need to establish a clear, consistent and lightweight, security outcomes based framework to be considered throughout the telemedicine supply-chain. Other measures include data privacy assessments, particularly for e-medical records, and a wider set of provisions for cyber security set around the creation of a MoH Computer Emergency Response Team (CERT) and a programme of testing, exercising and training. Perhaps most significantly, is the need to establish cross-agency governance arrangements, in the form of a new Coordination Group. This will strengthen cooperation between healthcare agencies, act as a focal point for data protection and cyber security issues across the sector, and coordinate the delivery of the recommendations, but above all, to manage strategic risk.

The below recommendations will provide the necessary groundwork to improve security and data protection, enabling the MoH, and other telemedicine stakeholders, to offer increased public and patient confidence in handling their data. It is hoped that this will encourage further uptake and foster a culture of security in telemedicine services more broadly.

Indonesia faces significant challenges to increase digital literacy in order to successfully deliver telemedicine healthcare provisions. It is felt necessary to ‘bed-in’ good cyber security practices and data handling processes from the outset. To this extent we strongly suggest that any digital literacy outreach programmes include basic cyber hygiene and data protection principles.

Whilst there are no specific recommendations here to encourage private sector entrepreneurialism, it should be recognised that if implemented correctly, these recommendations will clearly signal the Indonesian government’s commitment to security within the telemedicine sector. With additional investments and continued support to both the public and private sector telemedicine providers, Indonesia may consider these recommendations as the first step toward creating a digital ecosystem for the commercialisation of healthcare digital security.

The below recommendations should not be considered mutually exclusive (with perhaps the exception of 8 and 9); each one could form a discrete stand-alone project. However, we strongly propose that all recommendations are implemented along with consideration of the sequencing and prioritisation:

1. Security outcome based framework (understood by non-experts) for telemedicine based on international best practices
2. Privacy Impact Assessment (PIA) process model with specific case study on electronic medical records based on GDPR principles
3. MoH to develop of a cyber security awareness programme
4. Multi agency incident response exercise programme
5. Information and cyber intelligence sharing protocols (across public and private telemedicine supply chain)
6. MoH to establish a central Computer Emergency Response Team (CERT)
7. Multi-agency workshop programme for data scenarios to test security outcomes for the different stakeholders across the entire telemedicine supply chain
8. Undertake a Training Needs Analysis (TNA)
9. Implement a training programme (following a TNA) for MoH technical staff and Data Protection Officers (DPOs) to develop and deliver a tailored training programme
10. Provide basic cyber security and data protection training alongside digital access and literacy initiatives (particularly at Puskesmas level)
11. Create a cross-agency Health Sector Coordination Group for Data Protection and Cyber Security issues.
12. Development of a Data Protection and Cyber Security Strategic Risk Assessment (SRA) for the healthcare sector.

Finally, fundamental cultural change will only come about with strong leadership and cooperation. To this extent the Indonesian Minister of Health, in recent discussions with the UK Foreign Secretary, was very supportive of these recommendations. The MOU signed in June 2020 by the UK FCDO and the Indonesian Ministry of Health, provides a good foundation for this continued and important cooperation. During the development of and as a consequence of the research presented in this report, the UK FCDO through its DAP initiative, has made the decision to fund and provide oversight for the implementation of a number of the key recommendations outlined in this report.

Those recommendations taken forward will form a 14-month ‘intervention’ programme (see Section 7 below) which will be overseen by the UK Embassy in Jakarta, and delivered by commercial partners CCU and KPMG, alongside the Ministry of Health and key stakeholders. In a broader context of national cyber capacity building, it should be noted that these interventions are also designed to strengthen Indonesia's cybersecurity maturity as described in the Capability Maturity Model (CMM), developed by Oxford University’s Global Cyber Security, and widely acknowledged as the standard metric for measuring cyber security maturity for nations.[5]

[5] Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition, https://gcscc.ox.ac.uk/the-cmm#/

# 3 Background & Context

## 3.1 The Cyber threat to healthcare services

Personal data protection and cyber security are interrelated disciplines considered essential in building trust and confidence in delivering digital services to the public. Digital healthcare services, delivered either directly to members of the public, or amongst healthcare professionals to share data (collectively referred to as Telemedicine), require protection from a variety of malicious and benign cyber threats.

Cyber threats continue to proliferate; in recent years attacks such as Wannacry and Not Peyta have affected healthcare services across the globe. Moreover, 'internal' threats, including a lack of security awareness, basic mishandling of data, or simply bad system processes have led to significant data breaches. Data supply chains continue to become longer and increasingly sophisticated, offering a weak-link that is targeted by cyber threat actors. The recent SolarWinds cyber incident, saw a nation state actor compromise an entire enterprise management software solution, affecting large numbers of governments, critical national infrastructure providers and private companies.

Hospitals in the US have been targeted by malicious hacker groups looking to steal data and disrupt systems. In September 2020 250 facilities, part of the hospital chain Universal Health Services, were affected leaving doctors without the use of computers. In a very few cases fatalities have even been attributed to cyber attacks, due to critical health services not being available, and patients being required to move hospitals etc.[6]

The healthcare sector is also vulnerable due to a general lack of maturity in cyber security which has been exacerbated by a significant increase in targeting due to the COVID 19 pandemic. The risk to the Healthcare sector is considered so significant by UK and US authorities, that the UK National Cyber Security Centre (NCSC) and US Cybersecurity and Infrastructure Security Agency (CISA) took the exceptional step and issued a joint advisory, warning:

> "APT (Advanced Persistent Threat) actors are actively targeting organisations involved in both national and international COVID-19 responses. These organisations include healthcare bodies, pharmaceutical companies, academia, medical research organisations, and local government. APT actors frequently target organisations in order to collect bulk personal information, intellectual property and intelligence that aligns with national priorities. The pandemic has likely raised additional requirements for APT actors to gather information related to COVID-19. For example, actors may seek to obtain intelligence on national and international healthcare policy or acquire sensitive data on COVID-19 related research".[7]

[6] '*US hospital systems facing 'imminent' threat of cyber-attacks, FBI warns',* The Guardian, 29 Oct 2020. https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi

[7] 2 *Advisory: APT groups target healthcare and essential services,* 5 May 2020, United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). https://www.ncsc.gov.uk/files/Joint%20NCSC%20and%20CISA%20Advisory%20APT%20groups%20target%20healthcare%20and%20essential%20services.pdf

## 3.2 Cyber security - Indonesian healthcare

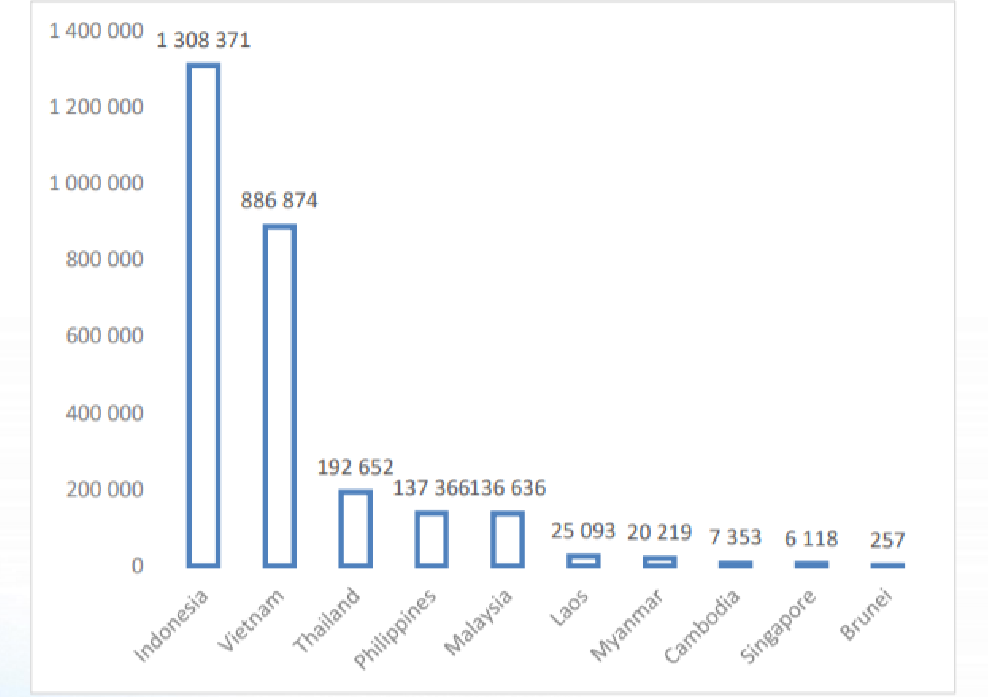
In Indonesia, the threat to healthcare has been similarly singled out for attention; the Directorate of National Critical Information Infrastructure Protection within BSSN has produced an extensive Whitepaper on the state of cyber and information security in the Healthcare sector, stating that almost 69% of health institutions (based on their sampling) have weak cyber security levels. The whitepaper identified a number specific areas of weaknesses, including governance and security frameworks, as well as a general lack of awareness, resourcing, security technology and staff training, stating:

> "cybersecurity managers are generally employees who have concurrent positions or other duties, even honorary staff. Most of them lack competence in cybersecurity. This is getting worse due to the lack of attention from the top leadership in providing budget support or opportunities to increase competence in the cybersecurity sector".[8]

The global 'WannaCry' malware incident in 2017 also affected a number of hospitals in Indonesia. Dharmais Cancer Hospital, which is the national referral hospital, reported that out of 600 computers at least 60 were infected with WannaCry. There has been a general increase in cyber attacks against healthcare in the region, with hospitals targeted in Thailand and Singapore.

It is not just the healthcare sector being affected, a recent Interpol report stated that there were 2.7 million ransomware detections in ASEAN region during the first 3 months of 2020, with Indonesia suffering most, with 1.3 million counts, accounting for almost half of all detections in the entire region. [9]

**Figure 1: Ransomware in ASEAN**

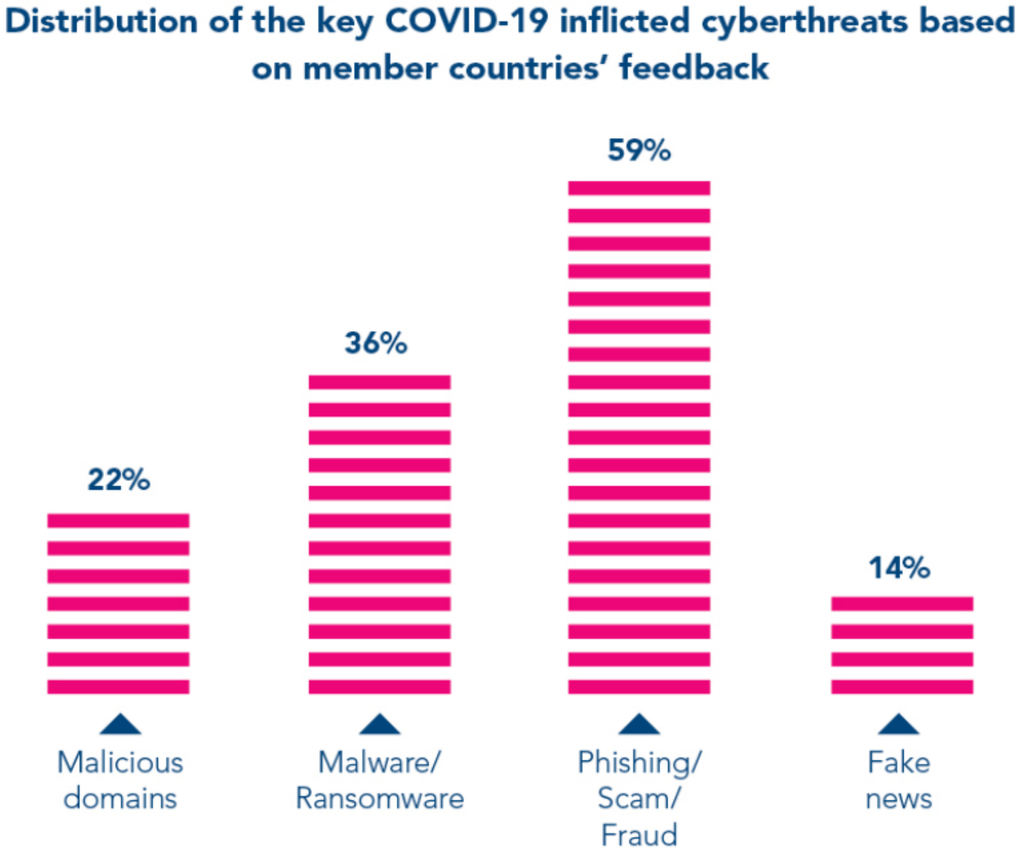


Source: ASEAN Cyber Threat Assessment 2021, Interpol file:///home/chronos/u-b82711bc3fcf9da1f956c4f86768b114a6713fda/MyFiles/Downloads/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf]

[8] The Indonesian Health Sector in Indonesia, BSSN Whitepaper, 2020

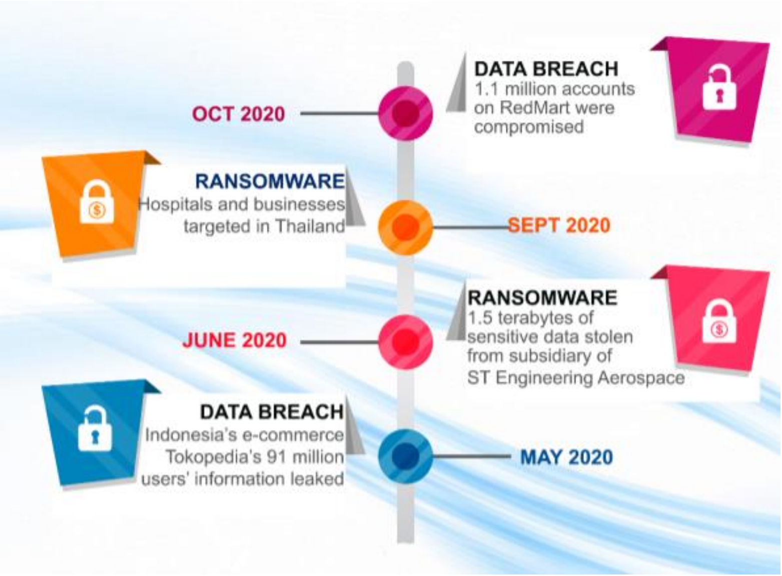
[9] Interpol, ASEAN Cyberthreat Assessment, 2021 https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

## Figure 2: Based on ASEAN countries



Source: ASEAN Cyber Threat Assessment 2021, Interpol https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

## Figure 3: Significant data breaches in ASEAN region


OCT 2020
DATA BREACH
1.1 million accounts on RedMart were compromised
RANSOMWARE
Hospitals and businesses targeted in Thailand
SEPT 2020
RANSOMWARE
1.5 terabytes of sensitive data stolen from subsidiary of ST Engineering Aerospace
JUNE 2020
DATA BREACH
Indonesia's e-commerce Tokopedia's 91 million users' information leaked
MAY 2020

Source: ASEAN Cyber Threat Assessment 2021, Interpol https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

## 3.3 Data Protection Bill Draft and Cyber Security Strategy

Indonesia is in the process of developing two significant legislative and policy initiatives around handling and securing data; the Personal Data Protection Bill (PDPB) and a National Cyber Security Strategy. Developed by KOMINFO and BSSN respectively, these two developments provide an important contextual backdrop to this study.

Whilst at the time of writing both the PDPB and National Cyber Security are yet to be ratified, our recommendations have been designed to align with, and support, both of these important landmark policies. In particular, we note that the PDPB is based largely on the European Union's General Data Protection Regulation (GDPR), and to that extent we are recommending the implementation of Privacy Impact Assessments (PIA). Regardless of what the final PDPB stipulates, PIAs provide a standard way to assess the sensitivity and commensurate protections around personal data. Similarly, we note and support, BSSN's intention to promote the international information security standard ISO27001 (this is reflected in recommendation 1 - see section 5.1 below), as well as their intention to establish CERTs across the CNI (section 5.3.3 below).

## 3.4 Telemedicine Services in Indonesia

Presently, the use of telemedicine in Indonesia, as outlined in the Circular Letter of the Ministry of Health No HK.02.01/MENKES/303/2020, is carried out by various parties. The Ministry of Health has the Sehatpedia app which relies on doctors in vertical hospitals owned by the Ministry of Health to provide direct teleconsultation to patients and prepare for the referral process. The Ministry of Health also manages the Temenin, a web-based application for teleconsultation between health care facilities. BPJS Kesehatan has also developed a new feature in the Mobile JKN app that allows participants to consult to the primary health center. Since the pandemic, mobile JKN has been downloaded 10 million times, compared to 3 million at the end of 2019.

The COVID-19 pandemic has prompted BPJS Kesehatan to develop new features to ensure access to health services. Allowing users to perform self-screening through the Mobile JKN application and also consult remotely with doctors using the new feature called teleconsultation. For doctors, among the advantages of using this application is that they do not need to reveal their personal cell phone number to the patients. However, the application is still not connected to electronic medical records, so doctors still have to enter data into the general medical record application.

It was noted that both telemedicine apps, Sehaptpedia and Tenmin, contained very little by way of technical security specifications, and or security user acceptance testing.

# 4 Methodology

This report has been based largely on qualitative and quantitative research methods conducted remotely by CCU through extensive stakeholder engagements via a series of meetings, workshops and questionnaire based discussions. A full list of stakeholders can be found at (Annex A).

The project has five incremental phases:

1. Project initiation, inception & project management
2. Stakeholder engagement
3. Research, review and analysis
4. Stakeholder conference
5. Reporting and project closure

Key deliverables being:

1. Inception report
2. Recommendations report (this document)
3. Stakeholder conference

## 4.1 Terms of Reference

The FCDO Terms of Reference (ToR) identified the main aim of the consultancy as:

**'Ensuring a strategic focus on data protection and cyber security within telemedicine regulation and standards, to ensure the protection of users' is prioritised.'**

**'The project will work primarily with the Indonesian Ministry of Health (MOH) and other key players in the public, private and non-profit sectors across the country to provide technical advice, support and best practice sharing in the context of the development of telemedicine regulation in Indonesia.'**

The scope has thus been broken down into three overall and essential areas of work:

- Research & analysis – using both quantitative and qualitative methods to produce in depth needs analysis and research products co-produced with the MoH. This will be on topics of data protection and cyber security standards in telemedicine regulatory and platform development. This will include assessment of the current situation, needs and gap analysis along with key recommendations.
- International best practices - reviewing and recommending international best practices on data protection / cyber security to support the development of telemedicine in Indonesia.
- Stakeholder engagement - through facilitation of events, meetings, conferences and workshops for the development of research products and to drive buy-in on the recommendations that will emerge from the research and analysis work.

# 5 Key Findings & Recommendations

Through our research we have identified and grouped our findings around five critical areas to be addressed:

- Security Frameworks
- Cyber security awareness and fostering a culture of personal data protection
- Collaboration and cooperation
- Skills and professional training
- Governance and strategic risk management

Within each of the above heading we have provided a number of recommendations. These recommendations are designed as foundational building blocks on which to build cyber security capacity, not only within the telemedicine sector although this is the prime focus, but to the healthcare sector more generally. Furthermore, in some cases the recommendations support wider capacity building across the Indonesian CNI.

It is also important to note that there are no specific recommendations encouraging private sector entrepreneurialism, however it should be recognised that if implemented correctly, these recommendations will clearly signal the Indonesian government's commitment to cyber security and data protection within the telemedicine sector as a whole. With additional investments and continued support to both the public and private sector telemedicine providers, Indonesia may consider these recommendations as the first steps toward creating a digital ecosystem for the commercialisation of healthcare digital security.

The following recommendations have been arranged as practical achievable steps, mainly at the national level, on which future cyber security across the health sector could be built upon.

## 5.1 Security Frameworks

That hospitals must be supported by an information system has been stated in Law No. 44/2009 on Hospitals. Further regulations regarding the hospital information system have been stipulated in the Minister of Health Regulation no 82/2013. In this regulation, the Hospital Information System (HIS) is defined as a system of information and communication that processes and integrates the flow of services in the entire hospital through a network of coordination, reporting and administrative procedures to obtain accurate information. Hospital information systems are also an integral part of the Health Information System. It is estimated that 85% of hospitals in Indonesia have information systems in place. However, until recently, the penetration of Electronic Medical Records and Telemedicine implementation in Indonesian hospitals was unknown.

In terms of governance, the Ministry of Health regulation states that hospitals must have an organizational structure, human resources, and a standard information technology governance framework. In the security aspect, the regulation states the need for security assurance physically, networks and applications. However, more importantly the cyber security governance framework is not defined.

Given the limits of the regulation regarding hospital information system governance, efforts to develop information systems are highly dependent on the initiative, motivation and capacity of each hospital. A number of hospitals with strong leadership allocated resources for the development of hospital information systems, including implementing a number of innovations in the form of electronic medical records, telemedicine and a number of other digital services.

A clear need has been identified that the MoH needs to provide security requirements to telemedicine providers, ensuring a consistent approach to security across the supply chain, and to help all the service providers ensure they are compliant with the upcoming data privacy legislation. One example of a similar set of requirements related to security is the regulation of the Financial Services Authority to ensure security in the banking sector. Through Regulation 38/2016 on the Implementation of Risk Management in the Use of Information Technology by Commercial Banks, OJK has prepared a more detailed guide regarding the principles and general framework of information technology system security.

This regulation specifies banks should have at least 4 aspects of risk management, including:

a. active supervision by the Board of Directors;
b. adequacy of policies, standards and procedures for the use of Information Technology;
c. adequacy of the process of identification, measurement, monitoring and risk control of Information Technology usage; and
d. internal control system over the use of Information Technology

During our workshops we provided an overview of the approach the UK's Information Commissioner's Office (ICO) has taken. Working with the UK's National Cyber Security Centre (NCSC) they produced a set of security outcomes that every organisation in the UK processing personal data must achieve. The NCSC/ICO approach has four high-level security outcomes, with subcategories under each of them.[10]

These high level categories are:

a. Manage security risk
b. Protect personal data against cyber attack
c. Detect security events
d. Minimise the impact

Organisations must consider technical and procedural methods for ensuring they can achieve these outcomes, taking into account the sensitivity of the personal data held. Health data would be considered very sensitive.

This presentation led to discussions of developing a framework specifically for the MoH to use for telemedicine purposes, although which may also be more widely applicable. Further discussions elicited the following set requirements:

- The outcomes-based framework must not be overly complex, but provide a sound foundation for future data protection and cybersecurity provisions
- It should meet the requirement of the PDP legislation (which is based on GDPR) regarding the protection of personal data
- It should not replace, or otherwise contradict, but support and provide foundation for more comprehensive frameworks such as ISO 27001

To that end, the CCU recommends the development of a lightweight set of security outcomes, based on the work done in the UK to ensure compliance across data processors with GDPR. This set of security outcomes will be tailored specifically towards healthcare and telemedicine, with corresponding emphasis on ensuring data confidentiality and availability of services. The goal will be to provide the MoH staff with a framework they can use to ensure that appropriate baseline security measures are in place in a consistent manner across a range of service providers.

[10] https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

This outcomes framework will not be a replacement for an accreditation standard such as ISO 27001, which is more complex and requires greater cyber security maturity and expertise to achieve, but will, and is designed to, offer a sound foundation from which to build on and adopt standards such as ISO 27001.

Subsequent to the development of this framework we would recommend training sessions/workshops with relevant stakeholders to walk through how the security outcomes framework can be used by different organisations. The training sessions/workshops should also cover how the various outcomes can be achieved in different ways depending on the nature of the organisation, the types of data processed and their risk levels, and choice of technologies amongst other considerations (see section 5.4 - Skills and Professional Training).

**Recommendation 1**

To develop a security outcomes based framework (taking into account any key legislative arrangements following PDP and Cyber Security Strategy) with a particular focus on telemedicine service providers. This framework is intended to ensure a minimum level of security across service providers, and to be understood and managed by non-experts.

## 5.2 Cyber Security Awareness & Protecting Personal Data

Cyber security and data protection are interrelated disciplines. Understanding what to protect and how to protect it are crucial to developing the foundations of good cyber security practice. Identifying what information assets need to be protected, whether it is personal, classified, or in any other way sensitive data, is the first step in developing a security conscious culture.

Below we discuss two important elements - firstly, the formal process of identifying and classifying sensitive personal data, specifically related to medical records accessed by telemedicine. Secondly, is the need to raise the general levels of cyber security awareness through a programme of briefings, learning sessions and training with clearly defined objectives.

### 5.2.1 Privacy Impact Assessment

Privacy Impact Assessments (PIA) are the formal way of classifying sensitive personal data in accordance with data protection principles as defined by the General Data Protection Regulation (GDPR). GDPR being the EU law widely accepted as best practices for data protection. Conducting a PIA is the first step in understanding what needs to be protected and once classified, how that data should be handled and protected.

Through our research it has been highlighted that electronic-medical records (EMR) present a challenge. The data is currently not classified, and is widely handled across numerous different healthcare facilities (FASYANKES). EMRs tend to include a wealth of sensitive data relating to patients, including name, address, payment details etc., as well as medical conditions, treatments, doctors, and other highly sensitive personal data. Such information clearly represents one of the most valuable and sensitive assets held by healthcare organisations, both public and private. Under GDPR regulations such data must be subjected to a PIA assessment.

It is highly recommended that a PIA assessment is undertaken for e-medical records accessed by telemedicine services, in order to correctly identify, classify and protect this data. It is suggested that conducting a PIA for e-medical records will also serve as a good model for understanding and applying processes to other types of telemedicine data, as well of course as other types of data held across the healthcare sector more generally.

Under GDPR guidelines a PIA should be undertaken before the data is actually processed, moreover, PIA's must be carried out if there is any indication that processing represents a high risk to the individual, or contains data of a highly personal nature (such as medical information). It should also be noted that a PIA process, for such data, should be conducted again every three years.

It is noted that Indonesia's draft Personal Data Protection Law (PDPL) is largely based on GDPR principles and therefore is highly likely to include provisions for a PIA. However, whilst this draft legislation is not yet enshrined in Indonesian law, carrying out a 'PIA-type' assessment for e-medical records should be done now, in order to determine necessary protections, as arguably this data is currently at high risk.

Under the UK's Information Commissioner's Office (ICO) guidelines on GDPR, there is a useful and clear 'PIA Awareness' check-list of implementing PIA processes this cover the following:

- Provide training so that staff understand the need to consider a PIA at the early stages of any plan involving personal data
- Existing policies, processes and procedures include references to PIA requirements.
- Develop understanding of the types of processing that require a PIA, and use the screening checklist to identify the need for a DPIA, where necessary.
- Create and document a PIA process.
- Provide training for relevant staff on how to carry out a PIA

**Recommendation 2**

Conduct a Privacy Impact Assessment (PIA) for electronic medical records. This assessment would be an important first step in determining classification of data and identifying generic types of security measures required for EMR.

### 5.2.2 Cyber Security Awareness Programme

As has been noted elsewhere in this document the level of maturity in cyber security knowledge across the medical community in Indonesia is relatively low. We recommend the MoH consider the development of a cyber security awareness programme aimed at improving the security culture across the organisation and other service providers. Obviously this is a broader focus than just telemedicine, and indeed the healthcare sector as a whole, to this extent we would recommend that BSSN might want to consider coordinating a wider awareness programme across all CNI sectors. Having said that, any telemedicine focussed improvements, will require some form of awareness training and general upskilling.

Before embarking on a cyber security awareness programme it is advisable to define some objectives. A set of suggested high-level objectives, developed by CCU over a number of years, is defined below. These can be tailored of course to suit MoH specific requirements as the development work proceeds, but it is recommended that at least this set of requirements is used at the beginning:

- All personnel should know not to automatically trust emails and other forms of messaging, and understand how and when they should verify the sender
- All personnel should understand how to work appropriately securely and how to handle personal, and other, data
- Personnel should recognise and know how to report cyber security incidents
- Personnel should have the confidence to give feedback when a policy is not appropriate (for instance, data is not adequately protected or a particular security requirement is overly

onerous). This is important as working practises change over time and hence security controls will need to adapt

- All personnel should understand why the MoH has certain security requirements, and why it is important that these are followed
- Personnel should know who is responsible for cyber security, how to contact them, and be willing to engage. Security teams have historically often been considered unapproachable, or unwilling to engage with end users in a productive manner. This should be considered poor practise - the security team are there to support the rest of the organisation, helping them achieve their goals in an appropriately safe and secure manner. Staff should know who the security team are and how to engage with them, and be willing to do so.

These are some of the suggested objectives of the cyber security awareness programme. Reaching these objectives will require a variety of ongoing approaches including in person (or recorded) briefings, online learning sessions, phishing training and more.

**Recommendation 3**

MoH to develop a cyber security awareness programme based on principles and objectives of international best practice.

(NB - BSSN to consider co-ordinating a wider CNI-wide cyber security awareness programme)

## 5.3 Collaboration and cooperation

Working with, sharing and learning from others is critical to develop cyber security maturity, however, developing relationships and then providing structure and formal arrangements are key. Below we discuss the benefits of testing and exercise programmes and the many benefits this creates.

In the Indonesian health system, the private sector plays an important role. The growth of private hospitals in the last 10 years has exceeded the growth of public hospitals. Although since 2014, the government has implemented the National Health Insurance program, private insurance is still an option, especially for the middle and upper class groups.With the spread of digitalization, the government is also placing the health sector as an important aspect of the digital economy. To date, no less than 100 health tech startups have provided services, and some of them have joined the Indonesian Healthtech Association. At the start of the pandemic, a number of health providers signed an MOU with the Ministry of Health to respond to the pandemic, especially in terms of teleconsultation. With the high use of telemedicine, especially during a pandemic, the action items identified below could be used to strengthen this cooperation.

### 5.3.1 Testing and Exercising

In the face of ever-growing and increasingly adaptive threats, we must accept that healthcare systems will be compromised, necessitating a shift from a purely protective security model to one designed to limit harm when an incident occurs. Cyber exercising can realistically simulate incident scenarios, providing a safe, secure way to define and rehearse the roles and responsibilities of internal and external stakeholders. A programme of cyber exercises, designed to bring stakeholders together in a non-crisis environment, is an effective way of helping organisations establish how resilient they are to cyber attack. Exercises are designed to deliver a variety of tangible benefits:

- validate plans and processes
- test assumptions and priorities

- clarify roles and responsibilities
- develop new ideas to complex problems

Participants also find that cyber exercises often provide intangible benefits, including:

- building working relationships with peers
- promoting cooperation between teams and organisations
- identifying strengths and weaknesses in others
- improving preparedness and personal confidence

It is recommended that focused desktop exercises are initially run with individual key stakeholders in the Indonesian healthcare sector, including the Ministry of Health, before multi-agency/ministry incident simulations are introduced. Any scenario will need to be specific to Indonesian telemedicine, and carefully designed to test the interaction and communication between multiple agencies and organisations in response to a simulated incident.

Cyber attacks and the vulnerabilities they exploit do not respect international boundaries, and benefits can be gained by working collaboratively with others in the global cybersecurity community. As organisational resilience and confidence increases, the option of international and multinational exercise participation should be explored. However, the complexities involved in planning, designing and executing a multi-national exercise should not be underestimated, and dedicated resources may be required to ensure that operational capability is not affected.

A well-defined testing and exercise programme should be run in parallel with other recommendations, combining increasingly complex and adaptive scenarios with qualitative assessment to track improvements in resilience and operational effectiveness over time.

**Recommendation 4**

To develop multi-agency/ministry incident response exercise programme to raise awareness across agencies and to help shape and develop governance and procedures for cyber incident response regarding telemedicine

### 5.3.2 Information Sharing

An important, and useful, component of maturing the overall cyber security posture of a sector is to foster the sharing of cyber security related information. Information sharing can encompass threat intelligence and reporting of incidents, but does not need to be limited to this. It can also be very useful for organisations to share details of specific cyber security challenges they have faced and how they have overcome them.

Defining information sharing in this broadest sense has two advantages; it enables organisations to learn from the experiences of others on implementing cyber security measures which can save time and money, and allows trust between organisations and a community to develop through the sharing of less sensitive information. It can be difficult to encourage sharing the details of incidents between organisations that do not have established trust-relationships, and sharing on less sensitive topics to begin with can help get over this initial hurdle.

The UK has run what are called ‘Information Exchanges’ since the establishment of its original critical infrastructure protection unit in 1999, on a sectoral basis. The information exchanges began as in person meetings, hosted by the government and jointly chaired by a government and industry sector representative. These information exchanges allowed for the UK government to brief industry sectors on threat, and for the industry members to share their own cyber security experiences and threat information.

This model still continues, but also now includes an online component - the Cyber Security Information Sharing Partnership[11] (CiSP). This is open to any UK organisation that wishes to join (with some validation) and allows for sharing of information and discussion on cyber security related issues. It also enables closed groups, which allows for the IE model to exist online, as well as anonymous sharing, which means organisations can share details of cyber security related incidents without having to reveal their identity.

Whilst recommending widespread adoption in Indonesia of the Information Exchange and CiSP model is beyond the scope of this report, it is recommended that the MoH consider improving information sharing in the health sector, and specifically between telemedicine service providers. This does not necessarily require the development of a CiSP style online portal, but also does not necessarily need to be done physically in person. Indonesian health service providers are distributed across a large area, and Covid has forced all organisations to adapt to remote working, The MoH could use this shift in working practises to develop an online information exchange model, where information sharing meetings happen using secure confidential videoconferencing platforms.

**Recommendation 5**

The MoH to consider improvements in cyber security related information sharing throughout the telemedicine supply chain (public and private sector). This should not be limited to threat and incident related sharing - the community can usefully learn from each other about implementing cyber security defensive measures.

### 5.3.3 Establishment of Computer Emergency Response Teams (CERTs)

Given the need to respond quickly to incidents, we recommend the establishment of a Computer Emergency Response Team (CERT) within the Ministry of Health (MoH). The MoH-CERT will have responsibility for coordinating the response to cyber security incidents impacting the Indonesian healthcare sector, as well as acting as a central trusted source of advice, guidance and education on the wider cyber threat, building on the information sharing recommendation above.

CERTs typically provide a combination of reactive services (e.g. alerts, warnings, incident response coordination, vulnerability disclosure) and proactive services (e.g. announcements, security assessments, development of tools). Selecting the right services for the MoH-CERT constituency will be an important step in the definition and implementation of the CERT.

Fortunately, a number of international organisations have published recommended approaches to take when creating a CERT, including the UK NCSC[12], International Telecommunication Union (ITU)[13] and the European Union Agency for Cybersecurity (ENISA)[14]. Whilst none provide an exact blueprint for the MoH-CERT, they act as a useful tool for helping to define the services and activities required.

More broadly, the Indonesian government should consider CERT establishment for other sectors of the Critical National Infrastructure (CNI). We are aware that BSSN are already working on the development of a CERT community across the CNI, and is considered that the development of MoH CERT, with UK assistance, will not only support BSSN's work, but could serve as a useful model for this important initiative.

[11] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
[12] Build: A cyber security incident response team (CSIRT): https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team
[13] Creating a CSIRT: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Creating%20a%20CIRT.pdf
[14] A step-by-step approach on how to set up a CSIRT: https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport

**Recommendation 6**

Establish a Ministry of Health Computer Emergency Response Team (CERT) based on international best practices and standards.

(NB - CERT establishment should be considered for other sectors of the Critical National Infrastructure (CNI))

## 5.4 Skills and professional training

Developing the necessary skills in human resources is vital to cyber capacity building. The success of all the recommendations contained within this paper will rely to a greater or lesser degree on individuals ability to comprehend, implement and maintain them. As already noted above (3.2) there is a cyber skills shortage across the Indonesia Healthcare sector, both centrally and regionally. To this extent we recommend some specific areas of training to support the recommendations.

### 5.4.1 Training on security outcomes framework

Following on from the development of a lightweight security outcomes framework (recommendation 1), it is recommended that the MoH run a series of workshops to train staff on using the security outcomes framework developed specifically for health and telemedicine providers. The goal of these would be to introduce staff to the framework, and demonstrate how to use it both for implementing a security strategy and assessing the security controls in place at an organisation or service provider.

The training goals should include:

- Overview of the framework
- Practical examples of how to use the framework to ensure baseline security controls are implemented at an organisational level
    - This should include walkthroughs of how outcomes would be met for different kinds of telemedicine providers, and different kinds of health data. This would demonstrate how the framework delivers outcomes appropriate to the risk and threat facing the organisation using it
- Worked examples of how to use the framework as an assessment tool when reviewing the security controls a vendor or service provider has in place

**Recommendation 7**

To workshop different data scenarios based on security outcomes for the different stakeholders across the telemedicine supply chain. To enable a better understanding of data flows, processing and risk levels, and thus allow for the development of commensurate security and privacy controls across different organisations along the supply chain (this can include medical records, but not exclusively, and may include only partial access to EMR).

### 5.4.2 Training Needs Analysis (TNA)

In the Indonesian health system there are approximately 170,000 physicians working in more than 2800 hospitals, 10,000 Puskesmas and 8,000 private clinics. Although specific standards and regulations regarding electronic medical records are not yet available, the practice of processing electronic medical records is already underway. In fact, at the primary service level, BPJS Kesehatan has provided an electronic application for cloud-based primary services, called PCare, which has been used routinely every day by 23,000 primary services.

In line with the increasing threat of cyber security, the public's awareness of the protection of personal data and the imminent law on the protection of personal data, it is important to strengthen the capacity and literacy of health workers and health facilities.

Although the health sector highly values the confidentiality and security of patient data, the standard and management guidelines are still more for non-electronic systems, particularly paper-based medical record management. Therefore it requires the involvement of various parties to develop more specific standards and practice guidelines, especially in the management of electronic systems and data, both within and between institutions. Although the Personal Data Protection Bill is currently under discussion, the health sector needs to raise awareness regarding these developments and eventual adoption. Collaboration with other sectors will be essential. KOMINFO has the Siberkreasi program for digital literacy awareness and training, but such a program is not available for healthcare professionals.

Before undertaking a widespread training programme it is vital to fully understand what are the training needs and requirements, including such aspects as professional career path progression and 'training the trainer'. To this extent we recommend that the MoH undertake a Training Needs Analysis (TNA), a defined process for identifying the gaps between employee level of skill and training needs.

**Recommendation 8**

MoH to undertake a Training Needs Analysis (TNA) to better understand the cyber security and data protection training needs across the telemedicine sector

**Recommendation 9**

To develop and implement a training programme following the TNA process.

This is likely to include specific medical/healthcare data protection training for Data Protection Officers (DPO) based on GDPR, and cyber security standards (ISO 27001) in preparation for Indonesian Personal Data Protection Bill and cyber security strategy.

(NB - similar training should be considered for all other ministries, CNI agencies and private sector providers handling personal and official government data.)

It has already been recognised that in order for the telemedicine programme to be successful there is a requirement to increase digital access and literacy skills, particularly at regional levels. It is therefore recommended that any digital literacy training should include the fundamentals of data protection and cyber security at a user level.

**Recommendation 10**

Alongside, or in conjunction with Digital Access and Digital Literacy programmes (such as Siberkreasi), user-level training in personal data protection and basic cyber security hygiene should be implemented, particularly at the Puskesmas and mobile level of healthcare provision.

## 5.5 Governance and Risk Assessment

Managing the process of implementation, of these recommendations, and any other data protection and cyber security measures identified, will require coordination and clear governance arrangements. This will be critical to the success of any such programme. Moreover, there will be a need to provide ongoing oversight, provide a focal point for data protection and cyber security issues, as well as managing strategic risk across the healthcare sector.

Whilst the following two recommendations are considered to relate to a wider remit than just telemedicine, it was felt necessary that strategic coordination and overall risk management of wider healthcare data and systems (not just telemedicine) was entirely appropriate.

### 5.5.1 Governance

Coordination across the relevant healthcare agencies and associated ministries will be key to strengthening relationships and ultimately successfully protecting telemedicine services, as well as other data and systems across the healthcare supply chain. Taking responsibility and ownership for the delivery of the recommendations outlined in this paper and acting as an ongoing focal point for data protection and cyber security issues is key. To this extent it is recommended that a cross departmental Coordination body is set up to manage data protection and cyber security, including being responsible for strategic risk management across the sector.

This Coordination Group should be chaired by the MoH, but include the following members at a minimum: BSSN (National Cyber and Crypto Agency), Kominfo (Ministry of ICT), BPJS Kesehantan (Social Security Administrator for Health), BAPPENAS (Ministry of National Development Planning), BKKBN (National Family Planning Coordination Board), FDA (National Agency of Drug and Food Control) and SJSN (National Social Security System).

| **Recommendation 11** |
|---|
| MoH to establish a multi-agency Data Protection and Cyber Security Coordination Group, to act as a focal point for strategic risk management relating to healthcare data and systems |

### 5.5.2 Strategic Risk Assessment

Key risk management principles of understanding threat, vulnerability and impact, are critical to assessing where you are, what assets (data and systems) you have and what you need to protect and prioritize. Whilst having risk management tools and analysis is fundamental, how that process is managed and documented is equally important. Conducting a strategic risk assessment will help organise thinking around threats and vulnerabilities, as well as helping to design and coordinate mitigations strategies. It is recommended that the MoH establish, under the auspices of the Healthcare Data Protection and Cyber Security Coordination Group, a strategic risk assessment.

| **Recommendation 12** |
|---|
| MoH to develop a Data Protection and Cyber Security Strategic Risk Assessment (SRA) for the data and systems across the Healthcare sector. |

# 6 Digital Access Programme (DAP) - Pillar 2 interventions

This study was commissioned by the UK FCDO as part of the DAP programme. The DAP programme is designed to facilitate wider, safer and more secure access to digital services in five partner countries, Nigeria, Kenya, South Africa, Brazil and Indonesia. The DAP strategic aims, or pillars, are to: enhance digital access policy through ‘models & enablers’ (Pillar 1); to build national cyber capacity through ‘trust & resilience’ (Pillar 2); and, to support local digital entrepreneurship and innovation by creating ‘Sustainable Digital Ecosystems’ (Pillar 3).

As a follow on to this study it has been agreed, as part of the ongoing DAP (Pillar 2) programme, that a number of recommendations outlined in this report have been selected to be taken forward as ‘DAP interventions’ programme funded by the UK government and supported by UK cyber security and data protection expertise.

CCU and KPMG (the prime contractor appointed by FCDO for the DAP) have been commissioned to help implement a number of recommendations, although currently under discussion, it has been informally agreed that there are initial resources to cover recommendations 1, 2 and 4 in this report; namely security outcomes framework, privacy impact assessment (PIA) for e-medical records, and development of a testing and exercising programme.

The MoH and the key stakeholders, as well as other interested groups have all been consulted on these ‘interventions’, agreeing that it would provide a sound basis from which to build future cyber capacity and data protection culture in telemedicine, as well as supporting digital resilience for the wider healthcare sector in Indonesia. It is, however, strongly advised that all the recommendations in this report are taken forward.

# 7 Summary of recommendations

It should be noted that the following recommendations are not mutually exclusive (with perhaps the exception of 8 and 9), they do not necessarily have any specific sequencing and could be implemented as stand alone projects. Having said that, we strongly advised that all the recommendations are implemented, along with a consideration of the sequencing and priority of implementing the recommendations.

### Recommendation 1

To develop a security outcomes based framework (taking into account any key legislative arrangements following PDP and Cyber Security Strategy) with a particular focus on telemedicine service providers. This framework is intended to ensure a minimum level of security across service providers, and to be understood and managed by non-experts.

### Recommendation 2

Conduct a Privacy Impact Assessment (PIA) for electronic medical records. This assessment would be an important first step in determining classification of data and identifying generic types of security measures required for EMR.

### Recommendation 3

MoH to develop a cyber security awareness programme based on principles and objectives of international best practice.

(NB - BSSN to consider co-ordinating a wider CNI-wide cyber security awareness programme)

### Recommendation 4

To develop multi-agency/ministry incident response exercise programme to raise awareness across agencies and to help shape and develop governance and procedures for cyber incident response regarding telemedicine

### Recommendation 5

The MoH to consider improvements in cyber security related information sharing throughout the telemedicine supply chain (public and private sector). This should not be limited to threat and incident related sharing - the community can usefully learn from each other about implementing cyber security defensive measures.

### Recommendation 6

Establish a Ministry of Health Computer Emergency Response Team (CERT) based on international best practices and standards.

NB - CERT establishment should be considered for other sectors of the Critical National Infrastructure (CNI)

### Recommendation 7

To Workshop different data scenarios based on security outcomes for the different stakeholders across the telemedicine supply chain. To enable a better understanding of data flows, processing and risk levels, and thus allow for the development of commensurate security and privacy controls across different organisations along the supply chain (this can include medical records, but not exclusively, and may include only partial access to EMR).

### Recommendation 8

MoH to undertake a Training Needs Analysis (TNA) to better understand the cyber security and data protection training needs across the telemedicine sector

**Recommendation 9**

To develop and implement a training programme following the TNA process.

This is likely to include specific medical/healthcare data protection training for Data Protection Officers (DPO) based on GDPR, and cyber security standards (ISO 27001) in preparation for Indonesian Personal Data Protection Bill and cyber security strategy.

(NB - similar training should be considered for all other ministries, CNI agencies and private sector providers handling personal and official government data.)

**Recommendation 10**

Alongside, or in conjunction with Digital Access and Digital Literacy programmes (such as Siberkreasi), user-level training in personal data protection and basic cyber security hygiene should be implemented, particularly at the Puskesmas and mobile level of healthcare provision.

**Recommendation 11**

MoH to establish a multi-agency Data Protection and Cyber Security Coordination Group, to act as a focal point for strategic risk management relating to healthcare data and systems

**Recommendation 12**

MoH to develop a Data Protection and Cyber Security Strategic Risk Assessment (SRA) for the data and systems across the Healthcare sector.

# Annex A Stakeholders

| |
|---|
| Ministry of Health |
| Ministry of Communications and Information Technology (KOMINFO) |
| National Cyber and crypto Agency - BSSN |
| Hospital Accreditation Committee (KARS) |
| Health Social Security Agency (BPJS Kesehatan) |
| National Standardization Agency (BSN) |
| Indonesian Hospital Association (PERSI) |
| Indonesian Medical Doctor Association (IDI) |
| Council of Indonesian Medical Doctor (KKI) |
| Indonesian Healthtech Association |
| Halodok |
| Alodokter |
| Good Doctor Indonesia |
| mySiloam |
| Indonesian Association of Cloud Computing (ACCI) |
| Gakeslab (Indonesian Association of Medical Devices and Laboratory Equipment Company) |
| ID CERT |
| SAFENET |
| Indonesia Cyber Security Forum (ICSF) |
| National Agency of Technology Assessment and Application (BPPT) |
| Universitas Indonesia (UI) |
| Universitas Gadjah Mada (UGM) |
| Institute Teknologi Bandung (ITB) |

# Annex B Sources and bibliography

[TBC]