CfDS
CENTER FOR DIGITAL SOCIETY

university of groningen
campus fryslân

Data Research Centre

Nuffic
meet the world

Information Security Policy in Health Data Governance in Indonesia

Authors

Surahyo Sumarsono
Ratna Lestari Budiani Buana

Editor

Annisa P. Wiharani

The health ecosystem is a complex, complicated system consisting of various aspects. In addition to being complex, the health ecosystem also consists of a wide variety of interrelated stakeholders. These stakeholders play a synergistic role in maintaining public health throughout its life cycle, from the fetus to death, whether promotive, preventive, curative, or rehabilitative. Several issues and challenges in health services are still being faced by Indonesia today to achieve this goal. As expected, In Indonesia, these issues and challenges will not be easy to overcome, especially considering the complexity of the health services and the nature of the society. In addition, ethical and legal aspects also play a significant role in health services, such as privacy, confidentiality, data and information security, doctor's and patient's identity, fraud, abuse, and compliance issues.

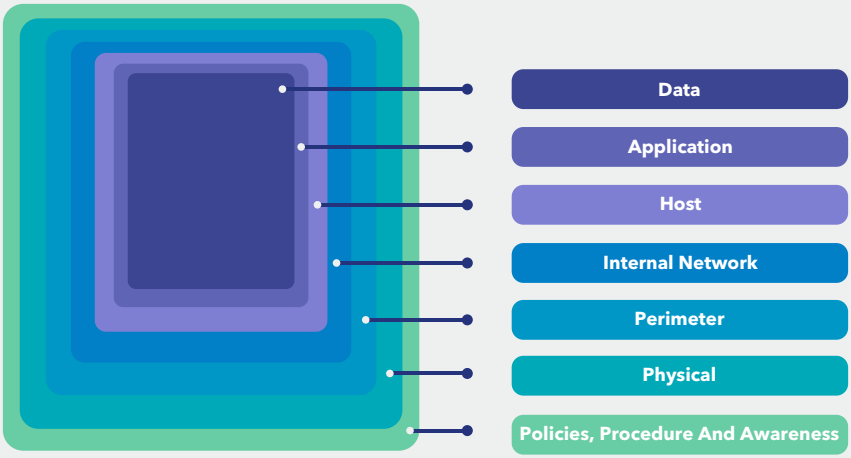
On the other side, the digital transformation proliferates and affects a revolution in the medical service system, enlightening some complexities. The information technology could be used to clear up the high demand for health services and the human resource limitation issues and reduce the visitor density of a health facility, which has a high-risk infection, especially in the pandemic plight. However, what cannot be forgotten is the adequacy of information and communication technology (ICT) infrastructure.

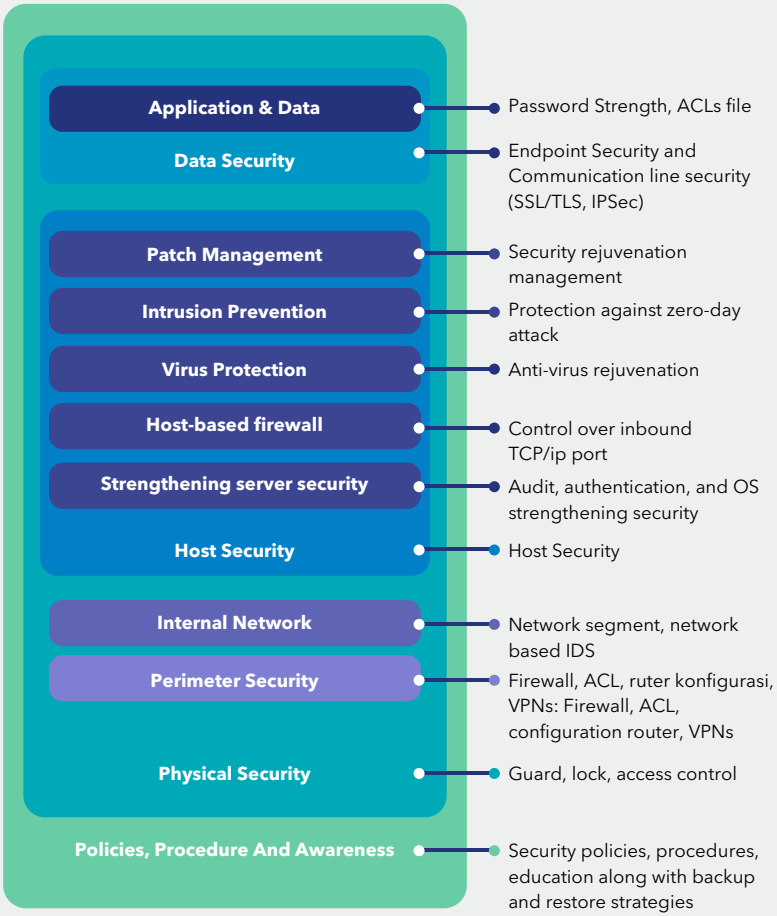
Digital data security is a meeting between ethical and legal aspects with information and communication technology infrastructure facilities. Digital data security protects information from unauthorized access, misuse, leakage or interception, interruption, modification, and fabrication based on these aspects. Computer networks connected to the internet can face information security threats, such as cybercriminals' intrusion of hospital assets. Therefore, it is necessary to pay attention to the information security aspects, consisting of confidentiality, integrity, and availability.

There are tons of hospital assets that cybercriminals can infiltrate. Nowadays, every device is inevitably connected to the internet, including the medical appliances used for remote service systems, identification systems, network equipment, interconnection systems, clinical information, mobile client devices, medical device networks, or even the health facility building controllers. This phenomenon poses an additional risk due to the emergence of non-formal health institutions that are not clear on the accuracy of their health information and content providers and system administrators. Thus, the public must accept the risks due to system errors and data security risks. The graph below shows the relationship between data use and data disclosure risk.

The graph below shows general data security based on the application ecosystem. The health information system is also required to refer and comply with the following procedures.

The graph below shows data security based on the application ecosystem.




Application & Data
Password Strength, ACLs file
Data Security
Endpoint Security and Communication line security (SSL/TLS, IPSec)
Patch Management
Security rejuvenation management
Intrusion Prevention
Protection against zero-day attack
Virus Protection
Anti-virus rejuvenation
Host-based firewall
Control over inbound TCP/ip port
Strengthening server security
Audit, authentication, and OS strengthening security
Host Security
Host Security
Internal Network
Network segment, network based IDS
Perimeter Security
Firewall, ACL, ruter konfigurasi, VPNs: Firewall, ACL, configuration router, VPNs
Physical Security
Guard, lock, access control
Policies, Procedure And Awareness
Security policies, procedures, education along with backup and restore strategies

Cases of data breaches have occurred several times, thus threatening cybersecurity in Indonesia. According to cybersecurity experts, one of the things that cause these violations to occur is the absence of the Personal Data Protection Law (UU PDP) in Indonesia. Data breaches in the health sector have also occurred, such as hacking and selling personal data of COVID-19 patients from the Indonesian COVID-19 patient database, the WannaCry global computer virus attack on the Dharmais Jakarta Hospital system[1], and the discovery of an Insecure Direct Object Reference (IDOR). Vulnerability on the site http://inahac.kemkes.go.id. IDOR Vulnerability often arises due to the absence of checking user access rights to a data to change the critical reference (key reference) to an object (e.g., ID in the database) and gain access to the data. An unauthorized external IP has also carried out an upload activity on the https://covid19.kemkes.go.id/uploads/ page caused by a vulnerability in the File Manager feature of the Ministry of Health, which the public can access without logging in, so it is misused by attackers to do web defacement. Bill gates Malware activity has also been found on the Ministry of Health server's http://presence.kemkes.go.id originating from an external IP via a connection after the attacker implanted a crypto-miner script. Healthcare and Social Security Agency of Indonesia (Badan Penyelenggara Jaminan Sosial Kesehatan - BPJS) has also been hit by data breaches[2][5], where there are allegations of leaks of health data containing national identity number mobile phone numbers, email addresses, home addresses, and salaries.

The case of data breaches in the health sector that should be studied is the SingHealth case[3], where the response occurred within 16 days of detection. On 27 June – 4 July 2018, there was a breach of 1.5 million Singaporean population data, with NRIC data type, name, address, gender, race, date of birth, and prescription drugs medicine for 160,000 patients. After that, Singapore's Ministry of Health, CSA, and IHIS issued safety recommendations and formed an independent investigation team. In the United States, the US Department of Health & Human Services and the Office for Civil Rights reported leaks of electronic medical record data (EMR), approximately 113 patients in 2015. In 2017, Identity Theft Resources United States reported that 25% of HTAG occurred in computer network systems in the health care sector, causing losses of up to 5.6 billion USD annually[4]. According to IBM's Cyber Security Intelligence Index in 2015, more than 100 million health records are vulnerable or at risk across more than 8000 devices and more than 100 countries.

This cyber threat is getting more complicated by the absence of specific regulations regarding information security in the health sector. Some references to standards and regulations regarding information security are as follows:

SNI
Standar Nasional Indonesia (from Indonesia's standardization body)[16]

ISO 27799:2017 Health Informatics[7]

HIPPA
Health Insurance Portabillity and Accountability Act[14]

GDPR
General Data Protection Regulation[15]

PermenKominfo (regulation of the minister of communication and information technology)[13]

Rancangan Undang-Undang Perlindungan Data Pribasi (personal data protection bill)[12]

Law on Adminduk (Law on administration and population)[11]

Law no. 29 of 2004 concerning Medical Practice which regulates medical secrets and medical ethnics[10]

PP No. 46 of 2014 concerning the Health Information System, which regulates security (confidentality, integrity, and availabillity) and privacy in general and domestic data processing and storage[8]

PMK No. 269 of 2008 Regulation Of The Minister Of Health concerning Medical Records, which regulates security (confidentiality, integrity, and availabillity) and privacy in the scope of medical record data[9]

These scattered regulations make it more difficult for any institution to manage, let alone find a solution if undesirable things happened.

Taken together, the high complexity and lack of integrated regulations make the health sector one of the main targets of cybercrime threats. In fact, health data is the most sensitive and critical information that can threaten the security and welfare of the community. The medical record data have now become a "gold mine" that has a very economical value that can be traded. On top of that, health data is 60 times more valuable than credit card or ID card data. This is because of the extensive information in it, including name, date of birth, national identity number, address, etc. Those extensive data make it more vulnerable to insurance and credit card fraud, foreign intelligence, prescription drugs, extortion material, and many more. Therefore, we need a holistic approach to design, develop, implement and manage health information systems that work to avoid cyber threats.

References

[1] Puspita, S., 2017. *Kronologi 60 Komputer RS Dharmais Terserang Ransomware WannaCry*. [online] KOMPAS.com. Available at: <https://megapolitan.kompas.com/read/2017/05/15/14024721/kronologi.60.komputer.rs.dharmais.terserang.ransomware.wannacry> [Accessed 13 July 2021].

[2] Ramalan, S., 2021. *Data Peserta Dibobol Hacker, BPJS Kesehatan Alami 2 Kerugian*. [online] SINDOnews.com. Available at: <https://ekbis.sindonews.com/read/436832/34/data-peserta-dibobol-hacker-bpjs-kesehatan-alami-2-kerugian-1621915533> [Accessed 13 July 2021].

[3] Hooi, E. 2019. *Cyber Security: Beware the Human Factor.* © S. Rajaratnam School of International Studies. http://hdl.handle.net/11540/10859.

[4] Koczkodaj, W. W., Masiak, J., Mazurek, M., Strzałka, D., & Zabrodskii, P. F. (2019). Massive Health Record Breaches Evidenced by the Office for Civil Rights Data. *Iranian journal of public health*, 48(2), 278–288. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6556182/

[5] Shalihah, N., 2021. 279 *Juta Data Penduduk Diduga Bocor, Ini Kata BPJS Kesehatan, Kominfo, dan Kemendagri Halaman all* - Kompas.com. [online] KOMPAS.com. Available at: <https://www.kompas.com/tren/read/2021/05/21/125000465/279-juta-data-penduduk-diduga-bocor-ini-kata-bpjs-kesehatan-kominfo-dan?page=all> [Accessed 13 July 2021].

[6] Schlesinger, J. and Day, A., 2016. *Dark Web is fertile ground for stolen medical records.* [online] CNBC.com. Available at: <https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html> [Accessed 13 July 2021].

[7] ISO.org. *ISO 27799: 2016*. Available at: <https://www.iso.org/standard/62777.html> [Accessed 13 July 2021].

[8] 2021. *Peraturan Pemerintah (PP) No. 46 Tahun 2014 tentang Sistem Informasi Kesehatan*. [online] Available at: <https://peraturan.bpk.go.id/Home/Details/5485> [Accessed 13 July 2021].

[9] Menteri Kesehatan Republik Indonesia, 2008. *Peraturan Menteri Kesehatan Republik Indonesia No. 269 Tahun 2008.* pp.1-7.

[10] WHO MiNDbank, 2021. L*aw of the Republic of Indonesia N. 29 of 2004 regarding the Medical Practice.*

[11] DPR.go.id. 2006. *Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. [*online] Available at: <https://www.dpr.go.id/dokjdih/document/uu/UU_2006_23.pdf> [Accessed 13 July 2021].

[12] Kominfo.go.id. *Rancangan Undang-Undang Republik Indonesia tentang Perlindungan Data Pribadi.* [online] Available at: <https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf> [Accessed 13 July 2021].

[13] Kominfo.go.id. 2020. *Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020.* [online] Available at:<https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020> [Accessed 13 July 2021].

[14] Cdc.gov. 2021. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* | CDC. [online] Available at: <https://www.cdc.gov/phlp/publications/topic/hipaa.html> [Accessed 13 July 2021].

[15] 2021. *General Data Protection Regulation (GDPR).* [online] Available at: <https://gdpr-info.eu/> [Accessed 13 July 2021].

[16] Bsn.go.id. 2021. *Tentang SNI.* [online] Available at: <https://www.bsn.go.id/main/sni/isi_sni/5> [Accessed 13 July 2021].

Information Security Policy in Health Data Governance in Indonesia