Seri Internet dan HAM

Policy Paper

Memastikan Pelindungan Privasi dalam Tata Kelola Data Kesehatan



ELSAM

PI

Policy Paper

Memastikan Pelindungan Privasi dalam Tata Kelola Data Kesehatan

Lembaga Studi dan Advokasi Masyarakat (ELSAM)

Memastikan Pelindungan Privasi dalam Tata Kelola Data Kesehatan

Penulis:

Blandina Lintang Setianti

Shevierra Danmadiyah

Editor:

Adzkar Ahsinin

Sampul & Layout:

Dodi Sanjaya

Pertama kali dipublikasikan dalam bahasa Indonesia oleh:

Lembaga Studi dan Advokasi Masyarakat (ELSAM) 2021



Except where otherwise noted, content on this report is licensed under a Creative Commons Attribution 3.0 License. Some rights reserved.

DAFTAR ISI

DAFTAR ISI.....I

I. PENDAHULUAN.....1

II. PRIVASI DALAM TATA KELOLA DATA KESEHATAN.....9

III. INSTRUMEN PELINDUNGAN DATA DARI WORLD HEALTH ORGANIZATION (WHO).....33

IV. INSTRUMEN PELINDUNGAN DATA MENURUT *GENERAL DATA PROECTION REGULATION (GDPR)*.....46

V. PRAKTIK PELINDUNGAN DATA KESEHATAN DI BERBAGAI NEGARA.....50

VI. PEMETAAN KEBIJAKAN DAN AKTOR PELINDUNGAN DATA PRIBADI DALAM SEKTOR KESEHATAN.....69

VII. PERMASALAHAN PELINDUNGAN DATA PRIBADI DALAM SEKTOR KESEHATAN DI INDONESIA.....106

KESIMPULAN DAN REKOMENDASI.....114

PROFIL ELSAM.....116

Memastikan Pelindungan Privasi dalam Tata Kelola Data Kesehatan

I. PENDAHULUAN

Dari beragam konsep dan persilangan isu, data atau informasi terkait kesehatan memiliki karakteristik penting dalam privasi. Dalam dunia medis, data, dan informasi kesehatan seorang pasien merupakan rahasia yang harus dijaga oleh layanan kesehatan dan petugas medis. Berbagai negara bahkan menetapkan data kesehatan sebagai data sensitif dalam regulasi pelindungan data pribadinya. Klasifikasi data sensitif tersebut tidak terlepas dari realita bagaimana kesehatan memiliki kaitan erat dengan kehidupan langsung seorang individu. Selain itu, data kesehatan juga terdapat kaitannya dengan kebutuhan lainnya, seperti pekerjaan, asuransi, perbankan, hingga akses papan, dan layanan lainnya dalam siklus kehidupan. Cukup berbeda dengan data lainnya, data kesehatan tidak ditentukan oleh individu yang bersangkutan sebab dimasukan dan dikelola oleh penyedia layanan kesehatan atau rumah sakit dengan bantuan tenaga medis. Pengembangan teknologi dan tata kelola rekam medis menjadi penting dalam dunia kesehatan, terutama dalam hal penekanan penyebaran penyakit menular dan pencegahan dini penyakit dengan melakukan pemantauan gaya hidup. Tata kelola data dan rekam medis juga menjadi esensial mengingat sistemnya berpengaruh pada pengambilan kebijakan yang berimplikasi pada kesehatan publik. Dalam hal inilah, isu privasi di sektor kesehatan perlu mendapatkan sorotan lebih lagi.

Mengacu pada Organisasi Kesehatan Dunia (WHO), definisi *'health'* atau kesehatan adalah keadaan kesejahteraan secara fisik, mental dan sosial yang utuh dan bukan sebatas tidak adanya penyakit atau suatu kelemahan.[1] Definisi ini kemudian mendapat sejumlah kritik mengenai pelabelan orang dengan disabilitas atau kondisi kronis tertentu sebagai 'tidak sehat' atau *'unhealthy'*. Kemudian dimunculkan definisi alternatif lainnya meski dinilai masih terlalu luas, yakni kemampuan organ manusia untuk beradaptasi dan mengelola diri sendiri.[2] Definisi ini berkaitan dengan pemaknaan data kesehatan, khususnya layanan kesehatan yang bersangkutan dengan kehidupan seorang individu, baik secara fisik dan mental. Sebab, kesehatan bukan sebatas konsep normatif berkaitan dengan keadaan 'sehat' maupun 'sakit', dan tidak terbatas pada rekam medis individu sebagai pasien. Melainkan juga sejumlah pemanfaatan teknologi yang berimplikasi pada pengumpulan data

[1] WHO, http://www.who.int/about/definition/en/print.html
[2] Leslie P. Francis Privacy what everyone needs to

pribadi, termasuk aplikasi-aplikasi dalam ponsel pintar atau jam tangan pintar yang dengan mudah diakses oleh masyarakat.

Peningkatan penggunaan teknologi informasi sektor kesehatan diharapkan meningkatkan penanganan kesehatan bagi pasien serta mampu memfasilitasi peningkatan layanan perawatan berbasis bukti dan mengurangi kesalahan medis. Bahkan beberapa pihak berpandangan, peningkatan pembagian informasi atau pemanfaatan data kesehatan di antara penyedia layanan akan mengoordinasikan peningkatan perawatan sebagai bagian dari layanan kesehatan.[3] Sebagaimana telah disebutkan sebelumnya, selain itu akses data kesehatan erat kaitannya dalam hal penanggulangan penyakit termasuk surveilans dan penegakan karantina. Misalnya, dalam penanganan penyakit menular, seperti pasien HIV/AIDS yang membutuhkan penelusuran pengakses ARV dengan tujuan mengurangi angka putus layanan (LFTU). Dalam penanggulangan pandemik COVID-19, penelusuran setiap kasus terbaru menjadi sangat penting untuk menurunkan angka penyebaran lebih tinggi, termasuk perangkat dan aplikasi kesehatan yang sering digunakan publik dengan pemanfaatan jaringan internet.

Organisasi Kesehatan Dunia (WHO) berpendapat bahwa teknologi digital dapat mendukung pelaporan cepat, pelacakan kontak, dan manajemen data. Dengan mempertimbangkan penyebaran global COVID-19, WHO menyatakan bahwa tujuan utama surveilens selama pandemi ini adalah:[4]

> untuk memungkinkan deteksi cepat, isolasi, pengujian, dan pengelolaan kasus, untuk memantau kecenderungan kematian COVID-19, untuk mengidentifikasi, menindaklanjuti dan mengkarantina kontak, untuk mendeteksi dan menahan klaster dan wabah, ... memantau kecenderungan dan evolusi epidemiologi jangka panjang dari virus SARS-CoV-2.

Perangkat surveilens digital jauh lebih mudah memungkinkan pemerintah untuk mengidentifikasi wabah penyakit dan terlibat dalam identifikasi kasus. Perangkat seperti Go.Data yang dikembangkan oleh WHO menggunakan data berdasarkan *real time* untuk mendaftarkan kasus dan kontak mereka, memfasilitasi analisis data pelacakan kontak, dan rantai penularan untuk lebih memahami epidemi. Pada saat yang sama perangkat teknologi sering dijalankan oleh pihak ketiga, seperti perusahaan teknologi dan lembaga penelitian, yang kemudian memiliki kapasitas untuk menambang data melalui *machine learning* dan *crowdsourcing.* Selama krisis COVID-19, perangkat

---

[3] Deven McGraw. *Privacy and Health Information Technology. Legal Solutions in Health Reform.* 2019. Journal of Law, Medicine & Ethics. Halaman 123

[4] Pemanfaatan perangkat digital dalam surveilens kesehatan masyarakat tidak hanya terjadi pada krisis COVID-19. Selama wabah sindrom pernafasan akut yang parah pada tahun 2003, Hong Kong mengidentifikasi kelompok penyakit menggunakan sistem data elektronik. Demikian pula selama wabah Ebola di Afrika Barat pada tahun 2014–2016, data ponsel juga digunakan untuk memodelkan pola perjalanan dan pelacakan kontak. Lihat, Sharifah Sekalala, et.al., *Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis*, Health and Human Rights Journal, Volume 22 Number, 2 December 2020, hlm. 8-9

digital untuk identifikasi kasus telah digunakan melalui aplikasi pelaporan gejala *online* di berbagai negara, seperti Singapura, Malaysia, Inggris, dan Afrika Selatan. Perangkat-perangkat tersebut dapat dengan mudah diintegrasikan dalam database nasional.[5]

Dalam konteks pandemic COVID-19 kemudian menurut Nani Jansen Reventlow memunculkan fenomena terjadinya ketegangan antara upaya melindungi kesehatan masyarakat dan menegakkan hak dan kebebasan dasar masyarakat. Meskipun perlu menerapkan upaya perlindungan untuk memperlambat penyebaran virus, pada sisi yang lain juga sangat penting bahwa langkah-langkah ini seimbang dan proporsional. Namun demikian, Nani Jansen Reventlow mengidentifikasi kangkah-langkah baru yang terburu-buru untuk mengekang penyebaran virus berpotensi mengubah dunia seperti penyakit itu sendiri. Perubahan ini juga tidak selalu bersifat sementara begitu diterapkan, banyak di antaranya tidak dapat dibatalkan. Langkah-langkah baru yang berpotensi memunculkan krisis hak digital:[6]

1. Peningkatan biosurveilens.
   Biosurveilens dilakukan melalui pelacakan pergerakan orang, komunikasi, dan data kesehatan yang digunakan dan dilakukan untuk menahan laju persebaran virus. Negara yang sering dibantu oleh perusahaan swasta, memantau warganya melalui beragam cata, seperti data telepon, rekaman CCTV, pos pemeriksaan suhu, pemesanan maskapai dan kereta api, informasi kartu kredit, catatan belanja *online,* data media sosial, pengenalan wajah, dan kadang-kadang bahkan menggunakan *drone*. Perusahaan swasta mengeksploitasi situasi dan menawarkan produk yang berpotensi menyalahgunakan hak dengan dalih mengelola dampak pandemi. Satu perusahaan *spyware* Israel telah mengembangkan produk yang diklaim dapat melacak penyebaran virus corona dengan menganalisis data selama dua minggu dari telepon pribadi orang, dan kemudian mencocokkannya dengan data tentang pergerakan warga yang diperoleh dari perusahaan telepon nasional;

2. Penyensoran dan Misinformasi.
   Penyensoran menjadi marak dilakukan rezim yang opresif melalui adopsi undang-undang "berita palsu". Adopsi undang-undang tersebut seolah-olah untuk mengekang penyebaran informasi yang salah tentang virus, tetapi dalam praktiknya, undang-undang ini sering digunakan untuk menindak suara-suara yang berbeda pendapat atau menekan kebebasan berbicara.

[5] ibid
[6] Nani Jansen Reventlow, *Why COVID-19 is a Crisis for Digital Rights*. Lihat: https://digitalfreedomfund.org/why-covid-19-is-a-crisis-for-digital-rights/, diakses pada 8 Juni 2021.

3. Kecerdasan Artifisial, Ketimpangan, dan Kontrol.
   Penyebaran teknologi kecerdasan artifisial memiliki konsekuensi bagi pemajuan HAM, tetapi adopsi teknologi ini dilakukan tanpa pengawasan dan diregulasi dengan minimal. Teknologi dikembangkan sebagau alat surveilens dan kontrol sosial. Implikasi teknologi terhadap HAM, termasuk efek bias dan diskriminatifnya harus terus dilawan dan ditentang karena potensinya untuk memperburuk ketidaksetaraan yang sudah dialami oleh mereka yang paling terpukul oleh pandemi.

4. Mengikis Hak Asasi Manusia.
   Banyak dari tindakan pelanggaran HAM yang telah diadopsi sampai saat ini diambil di luar kerangka pembatasan HAM yang tepat berdasarkan pada instrumen HAM yang berlaku. Instrumen HAM perlu menjadi rujukan untuk memastikan bahwa tindakan darurat tersebut bersifat sementara, terbatas dan diawasi.

Pernyataan serupa juga dinyatakan oleh Sharifah Sekalala, dan kawan-kawan bahwa teknologi surveilens baru ini memperkuat ketegangan lama dalam kesehatan masyarakat antara hak individu dan kepentingan kolektif. Teknologi ini berisisan dengan beberapa kecenderungan kontemporer, seperti ancaman privasi *online*, monetisasi data pribadi *online,* penggunaan big data dalam pembuatan kebijakan, dan penyalahgunaan surveilens *online* oleh pemerintah. Kecenderungan ini dipandang sebagai menciptakan *surveillance states* dan bentuk baru *surveillance capitalism* dengan kapasitas yang berpotensi mengikis HAM dan merusak demokrasi. Diskriminasi terhadap populasi yang rentan dan terpinggirkan telah mengakar dengan upaya surveilens dini.[7]

Sharifah Sekalala, dan kawan-kawan mengidentifikai 4 (empat) perhatian utama terhadap HAM, dan masalah HAM yang merupakan konsekuensi dari peningkatan skala dan kompleksitas surveilens kesehatan digital:[8]

1. Kedayagunaan perangkat digital untuk surveilens kesehatan global dipertanyakan karena banyak dari perangkat ini masih dalam tahap percobaan. Misalnya, setidaknya 40 negara menggunakan aplikasi pelacakan kontak, tetapi belum ada cukup bukti tentang kemampuan perangkat ini untuk mengurangi penyebaran penyakit;
2. Fakta terdapat aktor pihak ketiga membuat, menggunakan, dan menyimpan data menimbulkan pertanyaan tentang akuntabilitas mereka. Sementara surveilens kesehatan klasik masyarakat terutama melibatkan negara. Seiring kemunculan perangkat surveilens digital keterlibatan sejumlah besar aktor swasta pihak ketiga yang memiliki akses ke data kesehatan pribadi. Data pribadi dapat dieksploitasi dengan cara yang merusak kepercayaan terhadap surveilens kesehatan masyarakat;

[7] Sharifah Sekalala, *et.al*., *Op,Cit*., 9-10
[8] Ibid, hlm. 11-12

3. Selain ancaman terhadap masyarakat umum, peningkatan surveilens kesehatan digital dapat memperburuk kerugian secara khusus bagi kelompok minoritas seperti orang LGBTQ dan migran. Ini mungkin dalam bentuk peningkatan pelanggaran hak privasi mereka, peningkatan diskriminasi, dan penguatan ketidaksetaraan;[9]
4. Langkah-langkah surveilens kesehatan digital dapat menyebabkan penyalahgunaan oleh negara dan aktor pihak non-negara jika langkah-langkah tersebut menjadi tertanam dalam proses lain yang berbeda dari tujuan awal. Sifat jangka panjang dari krisis COVID-19 telah menimbulkan kekhawatiran bahwa rezim surveilens kesehatan yang diperpanjang memerlukan surveilens permanen yang berpotensi merugikan karena telah melampaui tindakan "sementara" yang dibenarkan oleh konteks "darurat".

Pada titik yang lain, upaya menyeimbangkan kebutuhan untuk mengumpulkan data untuk mendukung pengambilan keputusan yang baik *versus* kebutuhan untuk melindungi anak-anak dari bahaya yang ditimbulkan melalui pengumpulan data tidak pernah lebih menantang daripada dalam konteks pandemi COVID-19 global. Respons terhadap pandemi telah melihat peningkatan pesat teknologi yang belum pernah terjadi sebelumnya untuk mendukung pelacakan dan surveilens kontak digital. Sementara banyak masalah dan kekhawatiran yang sama dapat mempengaruhi anak-anak, dampak dari risiko ini pada anak-anak mungkin sangat berbeda dengan dampaknya terhadap orang dewasa dalam kehidupan anak-anak. Paling tidak terdapat beberapa pertimbangan dan refleksi tambahan dan eksplisit mengenai dampak pada anak-anak ini berasal dari risiko-risiko berikut:[10]

1. Teknologi sering kali tidak dirancang untuk mempertimbangkan anak-anak dan mungkin, pada kenyataannya, berkinerja buruk bila diterapkan pada anak-anak, misalnya, teknologi pengenalan wajah;
2. Anak-anak cenderung kurang memiliki hak atas data mereka sendiri dan orang tua serta pengasuh mereka mungkin tidak memahami dampaknya terhadap privasi anak-anak. Selain itu, anak-anak mungkin juga kurang mampu mengidentifikasi cara untuk dan mencari ganti rugi atas kesalahan atau pelanggaran data, mereka mungkin terpengaruh secara tidak proporsional oleh insiden tersebut;

---

[9] Sementara data lokasi yang dikumpulkan dapat memantau arus populasi secara real time, mengidentifikasi hotspot transmisi potensial, dan efektivitas intervensi kesehatan masyarakat, seperti pembatasan perjalanan, dapat membahayakan pengguna yang rentan dengan mengidentifikasi lokasi fisik mereka. Hasil analisis baru-baru ini terhadap 50 aplikasi terkait COVID-19 di Google Store menunjukkan bahwa hanya 16 aplikasi yang secara eksplisit dalam kebijakan menyatakan untuk menganonimkan data pengguna. Kelompok minoritas sangat berisiko terhadap penyalahgunaan privasi; misalnya, pelacakan kontak untuk wabah COVID-19 di Korea Selatan menyebabkan pelecehan homofobia yang ditargetkan pada komunitas LGBTQ Korea Selatan. Terdapat laporan bahwa beberapa kelompok minoritas telah terpengaruh secara tidak proporsional oleh COVID-19 dan mengalami hambata ketika mencari perawatan kesehatan karena riwayat diskriminasi. Lihat, ibid.,

[10] Gabrielle Berman, et.al., Digital contact tracing and surveillance during COVID-19: General and Child-specific Ethical Issues, Office of Research – Innocenti Working Paper WP 2020-01 | June 2020, hlm. 15-16

3. Penggunaan teknik dorongan dalam desain teknologi ini dapat mendorong anak-anak untuk memberikan lebih banyak data pribadi daripada yang seharusnya mereka lakukan secara sukarela;
4. Orang tua atau pengasuh dapat mengunggah atau menginstal aplikasi atau sistem pada ponsel anak sesuai dengan atau bertentangan dengan keinginan anak;
5. Anak-anak mungkin lebih rentan terhadap risiko stigma dan diskriminasi jika diidentifikasi terinfeksi. Anak-anak juga menghadapi implikasi jangka panjang untuk pengembangan identitas pribadi mereka dan berkaitan dengan peluang potensial di masa depan ketika anak-anak telah dipermalukan di depan umum.
6. Anak-anak mungkin menghadapi risiko keamanan tertentu jika lokasi mereka diketahui atau kontak atau detail mereka dipublikasikan atau dapat diakses oleh kelompok pengguna yang lebih luas;
7. Anak-anak lebih rentan terhadap penyimpanan data jangka panjang, yang menghasilkan kemungkinan yang lebih besar untuk keterkaitan dan identifikasi data di masa mendatang. Lebih lanjut, anak-anak kemungkinan akan menderita paling lama jika pengumpulan data dan pembatasan hak privasi tertentu menjadi permanen;
8. Data yang dikumpulkan dari anak-anak dapat berdampak negatif terhadap peluang pendidikan, pekerjaan, keuangan, atau sosial mereka di kemudian hari.

Pada titik yang lain, gender selalu tertanam dalam berbagai hubungan yang kompleks merefleksikan kekuasaan dan represi yang dikaitkan dengan pelaksanaan surveilens. Jauh sebelum perkembangan teknologi surveilens kontemporer, gender dan seksualitas sangat dikendalikan oleh norma-norma sosial dan moral. Saat ini, surveilens membantu memperkuat norma seksual dengan menciptakan tekanan untuk pengaturan diri *(self-regulation).* Operasi surveilens juga sarat dengan asumsi laki-laki dan berbagai dinamika gender.[11]

Dalam konteks data dan perempuan, upaya untuk memahami populasi mana yang paling dirugikan oleh pandemi ini, dan bagaimana efek tersebut bermanifestasi dalam konteks yang berbeda merupakan bagian integral dari menciptakan respons kebijakan berbasis bukti, berorientasi pada tindakan, ditargetkan, dan sensitif gender. Data gender berkualitas tinggi menjadi landasan dalam pembuatan kebijakan yang efektif untuk memastikan kesetaraan hak dan peluang bagi semua, dan menjadi semakin penting dalam konteks COVID-19. Kegagalan dalam memenuhi tantangan ini dapat mengakibatkan pemulihan yang buta gender *(gender-blind recovery).* Pemulihan yang buta gender akan menghambat daripada mempercepat pekerjaan untuk meningkatkan status, hak, dan

[11] Hille Koskela, *The problematic of surveillance and gender,* dalam Kirstie Ball, Kevin D. Haggerty and David Lyon, (eds.), Routledge Handbook of Surveillance Studies, (Oxon: Routledge, 2021), hlm. 49

peluang bagi semua. Lotus McDougal, dan kawan-kawan, merekomendasikan tindakan pada 5 (lima) bidang utama berikut:[12]

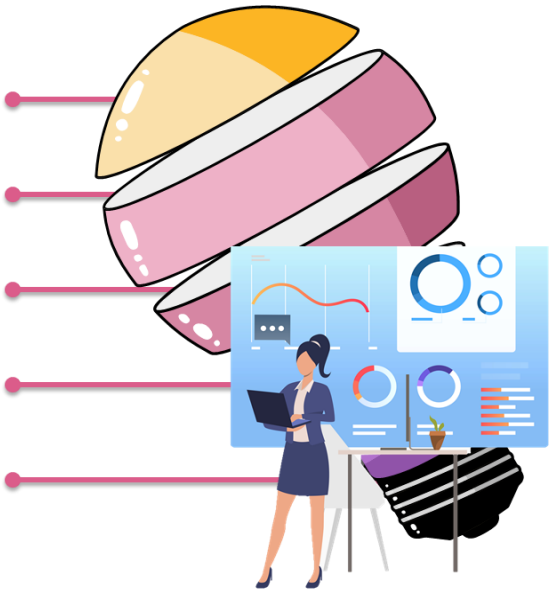
Pemilahan secara konsisten data terkait COVID-19 berdasarkan jenis kelamin dan karakteristik utama lainnya yang relevan dalam konteks nasional untuk menganalisis dampak pandemi terhadap kesehatan dan sosial ekonomi.

Pengumpulan data gender yang terstandarisasi dan dapat membandingkan pada wilayah mana kehidupan perempuan dan anak perempuan mungkin terpengaruh secara tidak proporsional oleh COVID-19.

Peningkatan penggunaan data gender non-tradisional untuk memahami dampak kesehatan dan sosial ekonomi dari COVID-19, seperti aktivitas media sosial, media berita, geospasial yang dihasilkan perangkat seluler dan data lainnya, penggunaan internet, dan data sektor swasta.

Perluasan ketersediaan, akses, dan penggunaan data gender terkait COVID-19 dengan cepat.

Penyediaan sumber daya yang memadai dan mendukung infrastruktur data yang terkoordinasi untuk menghasilkan data gender selama dan setelah pandemi COVID-19.



Pada saat bersamaan di tengah masifnya pemanfaatan data kesehatan ini, persoalan kebocoran data pribadi kesehatan merupakan tantangan yang nyata di berbagai negara. Amerika, kebocoran data kesehatan meningkat 25% pascapandemic melanda di tahun 2020. Setidaknya lebih 29 juta rekam medis bocor di tahun 2020.[13] Di Singapora, 14.000 data orang dengan HIV (ODHA) dilaporkan bocor ke publik.[14] Di Pakistan, sejumlah data dalam format Excel yang berisikan data lengkap terkait pasien Corona di Kota Quetta dan Taftan beredar di grup Whatsapp.[15] Hal ini juga terjadi di Indonesia, pada bulan Juni 2020 lalu, salah satu akun dalam forum Hacker mengklaim memiliki lebih dari 200.000 data pribadi pasien COVID-19 Indonesia. Elemen data yang dimiliki adalah nama, nomor telepon, alamat, hasil tes PCR, dan lokasi tempat pasien dirawat.[16]

Selain data pasien COVID-19, data jaminan kesehatan juga memiliki risiko tinggi jika terjadi kebocoran. Terutama pascapemanfaatan data BPJS Kesehatan melibatkan sejumlah pemrosesan data lanjutan, seperti pengembangan *data analytics* dan fasilitas *payment gateway* untuk

---

[12] Lotus McDougal, *et.al.*, Strengthening Gender Measures and Data In The Covid-19 Era: An Urgent Need For Change, (Washington DC: Data2X, 2021), hlm. 9-17

[13] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

[14] https://www.bbc.com/news/world-asia-47288219

[15] https://balochistanvoices.com/2020/03/private-data-of-coronavirus-patients-leaked-in-balochistan

[16] https://www.kompas.com/tren/read/2020/06/20/180500065/data-pasien-covid-19-diduga-bocor-mengapa-hal-ini-bisa-terjadi?page=all

pembayaran iuran,[17] dan penerbitan data sampel basis data kepesertaan dan jaminan pelayanan kesehatan yang digunakan untuk penelitian dan pengambilan kebijakan berbasis bukti. Data jaminan kesehatan ini menjadi urgen dan memiliki risiko tinggi, mengingat data kepesertaan juga terasosiasi dengan rekam medis peserta BPJS, termasuk status kesehatan seperti HIV dan penyakit lainnya.[18] Kebocoran data kesehatan memiliki potensi dan risiko yang lebih besar, mengingat data pribadi pasien dan rekam medisnya berdampak langsung pada kehidupan langsung sehingga berpotensi mengalami diskriminasi bila terungkap ke publik.

Data kesehatan sebagai data sensitif merupakan bentuk kategori khusus, sebab dalam pemrosesannya memerlukan tingkat pelindungan tambahan yang lebih tinggi. Langkah-langkah khusus terbatas dalam pemrosesan data pribadi spesifik, yakni:

1. Dilakukan atas persetujuan yang jelas, spesifik dengan kalimat afirmatif terkait jenis data pribadi yang akan diproses, misalnya dituangkan dalam Form Persetujuan;
2. Pemrosesan ditujukan untuk melindungi kepentingan vital dari subjek data;
3. Pemrosesan merupakan aktivitas yang sah dari yayasan, asosiasi, atau lembaga non-profit;
4. Data yang tersedia secara terbuka dari subjek data;
5. Dilakukan untuk proses penegakan hukum secara terbatas, misalnya di Korea Selatan, preskripsi obat dan pasien dilarang untuk dibuka ke pihak ketiga.

Selain itu, risiko juga bertambah karena data kesehatan juga menyangkut data pribadi lainnya seperti nama atau alamat, atau data diri lainnya. Seperti di Indonesia, setiap akses layanan kesehatan termasuk jaminan kesehatan (BPJS Kesehatan) mengharuskan Nomor Identitas Kependudukan (NIK) yang memuat data pribadi cukup lengkap. Hal ini diperparah dengan keadaan bahwa kebocoran data kesehatan tidak bisa dipulihkan atau diperbaiki, sebab karakteristik rekam medis yang tidak memungkinkan adanya diubah atau penghapusan.

Berangkat dari risiko yang besar dan tingginya potensi penyalahgunaan seiring dengan masifnya pemanfaatan data kesehatan dan perkembangan teknologinya, privasi harus ditempatkan sebagai konteks khusus dalam tata kelola data sektor kesehatan. Terutama memastikan kembali bahwa subjek data memiliki kendali terhadap alur datanya, termasuk pengambilan keputusan dan pemanfaatan dari data tersebut. Dalam rangka itulah kerta kebijakan ini disusun, dengan harapan menjadi rujukan akademis dalam pembentukan perangkat teknis implementasi tata kelola data kesehatan di Indonesia.

---

[17] https://swa.co.id/TelecommunicationUpdate/telecommunicationupdate/telkom-update/telkomgroup-dan-bpjs-kesehatan-sepakati-kemitraan-strategis-optimalisasi-penyelenggaraan-program-jkn-kis

[18] https://www.cnbcindonesia.com/tech/20190225142730-37-57456/sri-mulyani-wanti-wanti-agar-data-bpjs-tak-bocor-ada-apa

II. PRIVASI DALAM TATA KELOLA DATA KESEHATAN

Privasi dan kesehatan merupakan bagian dari hak fundamental HAM yang diakui pelindungannya, baik secara konstitusional maupun perjanjian internasional. Dalam Undang-Undang Dasar 1945, hak atas privasi diakui dalam Pasal 28G ayat (1). Sedangkan hak atas kesehatan dicantumkan dalam Pasal 28H yang berkaitan erat dengan kesejahteraan dan akses pelayanan kesehatan. Penegasan serupa juga tertuang dalam Pasal 29 UU Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Selain itu, Indonesia juga telah meratifikasi kovenan internasional hak-hak sipil dan politik atau *International Covenant on Civil dan Political Rights* (ICCPR) melalui UU Nomor 12 Tahun 2005 yang juga secara eksplisit memberikan pelindungan hak atas privasi.

Sebelum membahas pelindungan privasi dan tata kelola data kesehatan di Indonesia lebih jauh, pemaparan mengenai konsep kesehatan menjadi jembatan penting untuk memperkuat diskursus privasi dalam tata kelolanya. Selain itu, perlu juga memahami mengenai sistem kesehatan informasi beserta realita pemanfaatannya. Konsep kesehatan menurut WHO cenderung sangat luas, yakni kondisi paripurna, baik secara fisik, mental, dan sosial tanpa penyakit atau kelemahan tertentu. Karena menimbulkan sejumlah kritik, definisi alternatif dilahirkan yakni kemampuan organ manusia untuk beradaptasi dan mengelola diri sendiri.[19] Sedangkan hak atas kesehatan pada dasarnya berkaitan dengan sejumlah elemen, mencakup kewajiban negara dalam memastikan ketersediaan, aksesibilitas, penerimaan dan kualitas hak sosial dan ekonomi lainnya termasuk kesehatan. Layanan tersebut harus sesuai dengan prinsip kesetaraan dan realisasi progresif.

Privasi merupakan gagasan yang sulit untuk didefinisikan sebagian karena dilekatkan pada relativisme budaya. Misalnya, membuka pintu tanpa mengetuk mungkin dianggap sebagai pelanggaran privasi yang serius dalam satu budaya, namun diizinkan di budaya lain. Definisi privasi dimaknai secara deskriptif atau normatif apabila melihat privasi sebagai kondisi atau sebagai klaim moral pada orang lain untuk menahan diri dari aktivitas tertentu. Lebih jauh, beberapa orang memandang privasi sebagai gagasan turunan yang bertumpu pada hak-hak yang lebih mendasar, seperti kebebasan atau hak milik.[20]

Apabila ditilik dari dimensi historis pemaknaan privasi perlu menelisik pada konteks yang lebih luas, yang mencerminkan perubahan sosial yang lebih besar. Periodisasi historis yang paling umum dalam historiografi Barat-Eropa. Sejarah privasi dapat ditelusuri sebelum Abad Pertengahan sampai periode lebih modern dan kontemporer pramodern (500-1789) yang mencakup Renaisans,

[19] Leslie P. Francis Privacy what everyone needs to know

[20] Privasi telah didefinisikan dalam banyak cara selama beberapa ratus tahun terakhir. Mengikuti Hakim Thomas Cooley, Samuel Warren dan Louis D. Brandeis menyebut privasi sebagai hak untuk dibiarkan sendiri. Roscoe Pound dan Paul Freund mendefinisikannya dalam istilah dari perpanjangan kepribadian atau diri pribadi. Lihat, Adam D. Moore, *Privacy Rights: Moral and Legal Foundations*, (Pennsylvania: Pennsylvania State University Press, 2010), hlm. 13

Reformasi, dan Pencerahan. Periode berikutnya Periode selanjutnya abad kedua puluh (1914-1991), yang mencakup Perang Dunia Kedua dan Perang Dingin, dan sesudahnya. Periodisasi ini oleh Sjoerd Keulen dan Ronald Kroeze membagi abad kedua puluh dalam era sebelum dan sesudah komputer, dimulai pada tahun 1970-an. Perubahan privasi terbaru sangat dipengaruhi oleh dampak teknologi informasi baru. Dengan kata lain, pada 1970-an privasi didefinisikan ulang untuk menekankan otonomi individu daripada keluarga dan berkonsentrasi pada privasi informasi.[21] Bahkan adanya indikasi bahwa interpretasi privasi progresif telah menjadi aspirasi global. Ide-ide Barat dan non-Barat tentang privasi mungkin berbeda tetapi juga telah menyatu karena privasi karena privasi telah menjadi HAM yang dicita-citakan secara global. Pembentukan Deklarasi HAM dan Konvensi Eropa tentang HAM telah mendukung perubahan ini, serta fakta bahwa Pengadilan Hak Asasi Manusia Eropa memiliki hak untuk memutuskan dugaan klaim campur tangan negara.[22] Pada periode ini, serangan teroris 9/11 pada tahun 2001 dan undang-undang antiterorisme yang dikeluarkan sebagai reaksi terhadapnya, telah membuat privasi menjadi masalah yang lebih kompleks dan terus diperdebatkan. Pada 2007, Wikileaks Julian Assange mengungkapkan dokumen tentang dampak tindakan antiterorisme, yang membangkitkan emosi publik pada masalah privasi. Pada 2013, Edward Snowden menerbitkan dokumen rahasia tentang apa yang telah dikumpulkan oleh pemerintah di bawah payung kontraterorisme, termasuk informasi pribadi. Sementara media sosial mengaburkan garis batas privasi. Mark Zuckerberg pendiri Facebook mengklaim bahwa privasi bukan lagi norma sosial, komunikasi tatap muka masih sangat penting dan banyak pesan media sosial hanya memiliki relevansi untuk sebagian kecil kelompok pengguna. Oleh karena itu, privasi perlu diletakkan sebagai nilai kontekstual daripada hanya prinsip individu dan absolut. Helen Nissenbaum menekankan pentingnya integritas kontekstual privasi mengenai

---

[21] Pada 1969, Jerry Rosenberg menulis The Death of Privacy untuk menyampaikan pandangannya bahwa komputer dapat digunakan sebagai akses data pribadi. Arthur R. Miller menulis pada 1971 bahwa komputer akan menciptakan 'sistem surveilens yang akan mengubah masyarakat menjadi dunia yang transparan sehingga rumah, keuangan, dan asosiasi yang diikuti seseorang akan terekspos. Kekhawatiran yang berkembang tentang campur tangan negara juga dapat berasal dari perhatian baru terhadap konsep panopticon, misalnya dalam Discipline and Punish oleh Michel Foucault. Pemaknaan hukum terhadap privasi ditandai adanya kerusuhan sipil yang mendesak politisi untuk mengambil tindakan. Di Belanda dan Swedia pada 1970-an, warga sipil memprotes sensus dan penyimpanan data sensus di komputer mainframe baru. Hal ini menyebabkan pengenalan Undang-Undang Privasi di Swedia pada tahun 1973. Adopsi Konvensi untuk Perlindungan Individu sehubungan dengan Pemrosesan Otomatis Data Pribadi oleh Dewan Eropa pada tahun 1981, dan undang-undang perlindungan data nasional Belanda pada 1989. Di Inggris pada 1972, pemerintah mengeluarkan komite yang dipimpin oleh Kenneth Younger untuk mempertimbangkan undang-undang tentang privasi dan Amerika Serikat mengadopsi Undang-Undang Privasi pada 1974. Upaya untuk menambahkan fluorida ke air minum sebagai tindakan kesehatan masyarakat dibatalkan oleh Pengadilan Tinggi Belanda pada tahun 1973 karena Mahkamah Agung berpendapat bahwa tindakan yang luas seperti itu memerlukan dasar hukum. Dengan demikian, campur tangan dalam kehidupan pribadi oleh pemerintah yang dapat diterima dalam negara kesejahteraan pada 1950-an tetapi tidak lagi pada tahun 1970-an ketika bentuk-bentuk ini campur tangan dalam kehidupan pribadi membutuhkan dasar yuridis yang jelas. Lihat, Sjoerd Keulen and Ronald Kroeze, Privacy from a Historical Perspective, dalam Bart van der Sloot & Aviva de Groot, (eds.), The Handbook of Privacy Studies *An Interdisciplinary Introduction, (*Amsterdam: Amsterdam University Press, 2018), hlm. 4-36

[22] *Ibid.*, hlm. 37

aturan dan harapan seorang individu dan lingkungan. Pada periode kontemporer saat ini aturan dan harapan ini sedang dirumuskan kembali tentang privasi dalam masyarakat, politik, dan sains.[23]

Seringkali konsep privasi gagal untuk mengenali perbedaan antara konsepsi deskriptif atau netral dan yang normatif. Konsepsi netral berarti menyatakan privasi tanpa memasukkan maknanya bahwa privasi adalah hal yang baik, berharga, dan layak mendapat perlindungan moral dan hukum. Sementara konsepsi normatif privasi, sebaliknya, menggabungkan anggapan bahwa privasi adalah sesuatu yang berharga dan layak dilindungi. Ruth Gavison mendukung perlunya konsepsi netral sebagai landasan kokoh untuk membangun konsepsi moral dan hukum. Ruth Gavison mendefinisikan privasi sebagai ukuran akses yang dimiliki orang lain kepada seseorang melalui informasi, perhatian, dan kedekatan fisik. Skala untuk menetapkan seseorang memiliki privasi lebih atau kurang berdasarkan ukuran sejauh mana informasi tentang mereka adalah rahasia atau diketahui orang lain, sejauh mana mereka anonim dan tidak diketahui atau di bawah pengawasan orang lain, dan sejauh mana mereka beroperasi dalam kesendirian atau dalam kedekatan fisik yang dekat dengan orang lain. Salah satu manfaat memulai dengan konsepsi netral tentang privasi adalah memungkinkan seseorang untuk berbicara tentang keadaan privasi yang meningkat dan menurun tanpa mengajukan pertanyaan normatif apakah keadaan ini baik atau buruk. Ini membuka kemungkinan bahwa dalam keadaan tertentu lebih sedikit privasi mungkin lebih baik daripada lebih dan pengurangan privasi tidak perlu merupakan pelanggaran atau intrusi atau serangan. Semua istilah ini menandakan bahwa sesuatu telah terjadi yang seharusnya tidak terjadi. Robert Post menyatakan bahwa pelanggaran privasi dikaitkan dengan tindakan, praktik, atau sistem yang mengurangi atau melanggar privasi.[24] Pembagian senada juga diusung oleh Adam D. Moore yang membagi 2 (dua) perbedaan terkait dengan definisi privasi. Pertama adalah perbedaan antara konsepsi privasi deskriptif dan normatif. Pertimbangan deskriptif atau non-normatif menggambarkan keadaan atau kondisi di mana privasi diperoleh. Di sisi lain, pertimbangan normatif berkaitan dengan referensi kewajiban moral atau klaim.[25]

Kebutuhan untuk mengartikulasikan dan memberikan legitimasi pada hak atas privasi harus mencakup definisi hak, penjelasan tentang sifatnya, misalnya, moral, politik, hukum, dan lain sebagainya serta prinsip-prinsip untuk menggambarkan ruang lingkup hak atas privasi. Pada titik ini normativitas privasi berdasarkan preferensi atau kepentingan sebagai basis klaim bahwa orang memiliki hak untuk mengontrol informasi tentang diri mereka sendiri, atau memiliki hak untuk

---

[23] *Ibid.*, hlm. 38-37

[24] Helen Nissenbaum, *Privacy In Context: Technology, Policy, and the Integrity of Social Life, (*Stanford: Stanford University Press, 2010), hlm. 68-69

[25] Adam D. Moore, *Op.Cit.*, hlm. 14.

membatasi akses ke informasi tentang diri mereka sendiri, karena ini paling sesuai dengan kepentingan mereka atau karena ini sesuai dengan preferensi kepentingan sebagian besar orang. [26]

Berkaitan dengan legitimasi terdapat 2 (dua) kategori pendekatan dalam memperhitungkan tingkat dan batas klaim privasi yang sah secara moral. *Pertama,* klaim privasi yang sah secara moral mencakup semua informasi, menggambarkan tingkat dan batasan klaim tersebut dalam kapasitasnya untuk mempromosikan nilai-nilai moral dan politik penting lainnya. *Kedua,* legitimasi moral privasi dengan kapasitas privasi untuk melindungi zona pribadi. Oleh karena itu, hak atas privasi berkisar pada informasi pribadi. Helen Nissenbaum merujuk secara bergantian pada klaim privasi yang sah secara moral dan hak privasi untuk menentukan status hukum suatu klaim atau hak. Dengan demikian, maka paling tidak terdapat 3 (tiga) bentuk hubungan yang ditarik privasi dan nilai-nilai, yaitu privasi dan kehidupan individu; privasi dengan nilai-nilai dalam hubungan manusia; dan hubungan penting antara privasi dan nilai-nilai sosial.[27]

Ruth Gavison menempatkan nilai privasi dalam hubungan fungsionalnya dengan tujuan yang dihargai, termasuk kesejahteraan dan perkembangan manusia, kreativitas, otonomi, kesehatan mental, dan kebebasan. Jeffrey Reiman kembali memperkuat nilai privasi karena privasi sangat penting dan baik bagi manusia. Privasi sebagai sarana untuk melindungi kebebasan, kepribadian moral, dan kehidupan batin yang kaya dan kritis. Di samping itu, privasi ketika ditegaskan sebagai kapasitas untuk menarik diri dari pengawasan, sama dengan ekspresi kedaulatan individu atau kepemilikan diri.[28]

Pada titik yang lain, terdapat 2 (dua) pendekatanyang mencirikan privasi sebagai kendala akses dan sebagai bentuk kontrol. Ruth Gavison memberikan aksentuasi pada privasi dimensi akses yang ditandai dengan adanya kondisi yang diukur dalam kaitannya dengan tingkat akses yang dimiliki orang lain kepada seseorang melalui informasi, perhatian, dan kedekatan. Jeffrey Reiman mendefinisikan privasi sebagai kondisi di mana orang lain kehilangan akses ke beberapa informasi tentang dirinya atau beberapa pengalaman tentang dirinya. Pada sisi yang lain, meskipun tingkat deprivasi akses adalah kondisi kunci yang menentukan privasi, masalah siapa yang memiliki kebijaksanaan atau kendali untuk menentukan tingkat akses ini merupakan bidang negosiasi yang penting antara dan di antara individu dan masyarakat. Jeffrey Reiman menolak kondisi yang menunjukkan tingkat perampasan akses yang sepenuhnya di bawah kendali orang lain, tetapi juga tidak mendukung definisi privasi yang menurut individu diberikan kontrol secara penuh. Namun, sebagian besar, konsepsi privasi mendefinisikan privasi sebagai klaim individu, kelompok, atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain. Charles Fried menyatakan privasi bukan hanya ketiadaan

[26] Helen Nissenbaum, *Op.Cit.,* hlm. 72.
[27] *Ibid.*, hlm. 73.
[28] *Ibid.*, hlm. 73-75.

informasi tentang kita di benak orang lain, melainkan kontrol yang kita miliki atas informasi tentang diri kita sendiri. Sejalan dengan itu, Michael Froomkin mencirikan privasi sebagai kemampuan untuk mengontrol perolehan atau pelepasan informasi tentang diri sendiri. Jerry Kang juga memberikan aksentuasi yang sama yakni kontrol individu atas pemrosesas, meliputi perolehan, pengungkapan, dan penggunaan informasi pribadi.[29] Demikian pula halnya dengan Adam D. Moore memaknai privasi. definisi privasi berbasis kontrol *(control-based).* Hak privasi adalah hak kontrol akses atas diri sendiri dan informasi tentang diri sendiri. Hak privasi juga mencakup karakteristik penggunaan atau kontrol, yaitu, hak privasi memungkinkan seseorang menggunakan dan mengontrol secara eksklusif informasi pribadi dan badan atau lokasi tertentu.[30]

Sementara itu, Charles Fried menegaskan dimensi privasi yang dikontekskan pada hubungan manusia yang berharga yang tidak hanya instrumental dan kontingen. Hal ini berarti privasi bukan hanya satu cara yang mungkin dan memastikan bekerjanya beberapa nilai lain, tetapi terkait dengan tujuan dan hubungan yang paling mendasar, yaitu rasa hormat, cinta, persahabatan dan kepercayaan. Dalam konteks ini, ide privasi sebagai konteks tidak terlepas dari nilainya yang tidak hanya terletak pada pengaturan kedekatan, tetapi juga dalam mengatur kekhasan atau keragaman hubungan. James Rachels kemudian menegaskan bahwa nilai privasi didasarkan pada gagasan adanya hubungan erat antara kemampuan seseorang untuk mengontrol siapa yang memiliki akses dan informasi, serta kemampuan untuk menciptakan dan memelihara berbagai jenis hubungan sosial dengan orang yang berbeda.[31] Selanjutnya, Jeroen van den Hoven, menyampaikan argumentasi moralitas mengapa privasi layak dilindungi menjadi 4 (empat) aspek: [32]

1. Kerugian berbasis informasi *(Informational Harm)*
   Semakin banyak transaksi penting yang dimediasi melalui Internet atau telepon, misalnya, perbankan, perjalanan, interaksi dengan lembaga pemerintah, dan belanja. Pada saat yang sama ketersediaan informasi yang tidak terbatas seperti nomor Jaminan Sosial, nama gadis ibu, kata sandi, dan alamat rumah memungkinkan konstruksi identitas palsu dalam kejahatan yang sekarang biasa disebut pencurian identitas. Kerugian bagi korban berkisar dari keuangan hingga reputasi, termasuk waktu yang terbuang, frustrasi, ketakutan, kecemasan, dan akhirnya keengganan untuk terlibat dalam kegiatan yang bermanfaat secara sosial. Informasi yang terlalu bebas diperoleh dari catatan sekolah dan pemerintah atau laporan media terkadang jatuh ke tangan penguntit, pedofil, dan lain-lain dengan maksud yang merugikan;

[29] Helen Nissenbaum, *Op.Cit.*, hlm. 70-71.
[30] Adam D. Moore, *Op.Cit*, hlm. 17.
[31] Helen Nessenbaum, *Op.Cit.*, hlm. 84-85.
[32] *Ibid*., hlm. 78-80.

2. Informasional dalam kesetaraan *(Informational Inequality)*
   ketidaksetaraan informasi terjadi ketika arus informasi pribadi tidak dibatasi secara sistematis sehingga manfaat mungkin diperoleh secara tidak proporsional bagi beberapa pihak dibandingkan pihak lain. Oleh karena itu, pasar informasi tidak mendapatkan perlindungan yang tidak memadai untuk memastikan bahwa pertukaran diatur oleh dengan keterbukaan, transparansi, partisipasi, dan pemberitahuan di pihak perusahaan bisnis dan pemasar langsung untuk mengamankan kontrak yang adil.

3. Ketidakadilan informasi *(Informational Injustice)*
   Informasi termasuk dalam satu bidang tidak boleh diizinkan untuk bermigrasi ke bidang lain atau yang lain karena jika demikian maka ketidakadilan informasi berpotensi terjadi;

4. Pelanggaran otonomi moral (*Encroachment on Moral Autonomy*)
   Alasan keempat untuk perlindungan data adalah otonomi moral. Jeroen van den Hoven menegaskan bahwa perlindungan data berkaitan dengan otonomi moral karena menjadi bagian dari kapasitas untuk membentuk biografi moral, merefleksikan riwayat moral, mengevaluasi dan mengidentifikasi pilihan moral kita sendiri, tanpa pertimbangan kritis. Intervensi, dan gangguan orang lain dan tekanan untuk menyesuaikan diri dengan identitas normal atau yang diinginkan secara sosial.

Lebih jauh, privasi apabila dipahami sebagai klaim atau hak untuk mengontrol atau menentukan akses ke informasi tentang diri sendiri, dan otonomi dipahami sebagai penentuan nasib sendiri, maka privasi merupakan bagian dari otonomi. Dengan kata lain, dalam hubungan antara privasi dan otonomi bukan merupakan hubungan kausal. Sebaliknya, privasi harus dipahami sebagai bentuk otonomi dan penentuan nasib sendiri sehubungan dengan informasi tentang diri sendiri. Pada titik ini, privasi merupakan kapasitas untuk membentuk bagaimana individu mendefinisikan diri mereka sendiri dan menampilkan diri mereka kepada orang lain dalam berbagai keadaan kehidupan. Dengan demikian, privasi merupakan kapasitas untuk mengekspresikan dimensi penting dari otonomi, atau penentuan nasib sendiri. *Kedua,* privasi juga penting dipahami sebagai batasan akses ke orang melalui informasi, membebaskan kita dari efek pengawasan dan persetujuan (atau penolakan) yang menghambat sehingga dapat berkontribusi pada kondisi material untuk pengembangan dan pelaksanaan otonomi dan kebebasan dalam berpikir dan tindakan. *Ketiga,* hubungan antara privasi dan otonomi, mengacu pada pemahaman otonomi yang berbeda atau lebih, mengacu tidak hanya pada kapasitas untuk meninjau prinsip-prinsip tindakan secara kritis dan kebebasan untuk bertindak berdasarkan prinsip-prinsip tersebut, tetapi juga pada prinsip-prinsip tindakan, kapasitas atau sarana untuk menindaklanjuti keotonomian diri.[33]

[33] *Ibid*., hlm. 81-82.

Priscilla Regan memperluas cakupan privasi tidak hanya bernilai bagi individu tetapi juga bagi masyarakat secara umum. Lebih jauh, konsepsi privasi individualistis, yang populer pada 1960-an dan 1970-an yang tidak memberikan dasar yang bermanfaat bagi perumusan kebijakan untuk melindungi privasi.[34] Nilai privasi menjadi penting bagi masyarakat menjadi basis argumentasi Priscilla Regan. Argumentasi ini tidak terlepas dari dekade regulasi privasi di Amerika Serikat bahwa:

> Privasi memang beririsan dengan kepentingan individu, namun pada akhirnya melebihi kebutuhan sosial yang berlawanan, misalnya, efisiensi bisnis, keamanan nasional, penegakan hukum, atau kemakmuran ekonomi.

Oleh karena itu, perlindungan yang hanya difokuskan pada nilai privasi bagi individu, maka gagal untuk mengenali pentingnya privasi sebagai (1) nilai bersama; (2) nilai publik; dan (3) nilai kolektif.[35]

Selanjutnya Anita Allen menggabungkan kontrol dan akses dalam mendefinisikan privasi dengan melibatkan 3 (tiga) dimensi, meliputi (1) privasi fisik, yang dicirikan sebagai pengasingan dan kesendirian; (2) privasi informasi, yang dicirikan sebagai kerahasiaan, perlindungan data, dan kontrol atas informasi pribadi; dan (3) privasi hak milik, yang dicirikan sebagai kontrol atas nama, penyalahgunaan kemiripan nama, dan penyimpanan informasi pribadi.[36] William Prosser memisahkan kasus privasi menjadi 4 (empat) kasus yang berbeda tetapi terkait: (1) intrusi, gangguan baik secara fisik atau sebaliknya pada kesendirian orang lain dengan cara yang sangat ofensif; (2) fakta pribadi, memublikasikan informasi pribadi yang ofensif tentang seseorang yang menjadi perhatian publik secara tidak sah; (3) keterangan palsu, memublikasikan kesan yang sangat ofensif dan salah tentang orang lain; dan (4) apropriasi, menggunakan nama atau rupa orang lain untuk beberapa keuntungan tanpa persetujuan orang lain.[37]

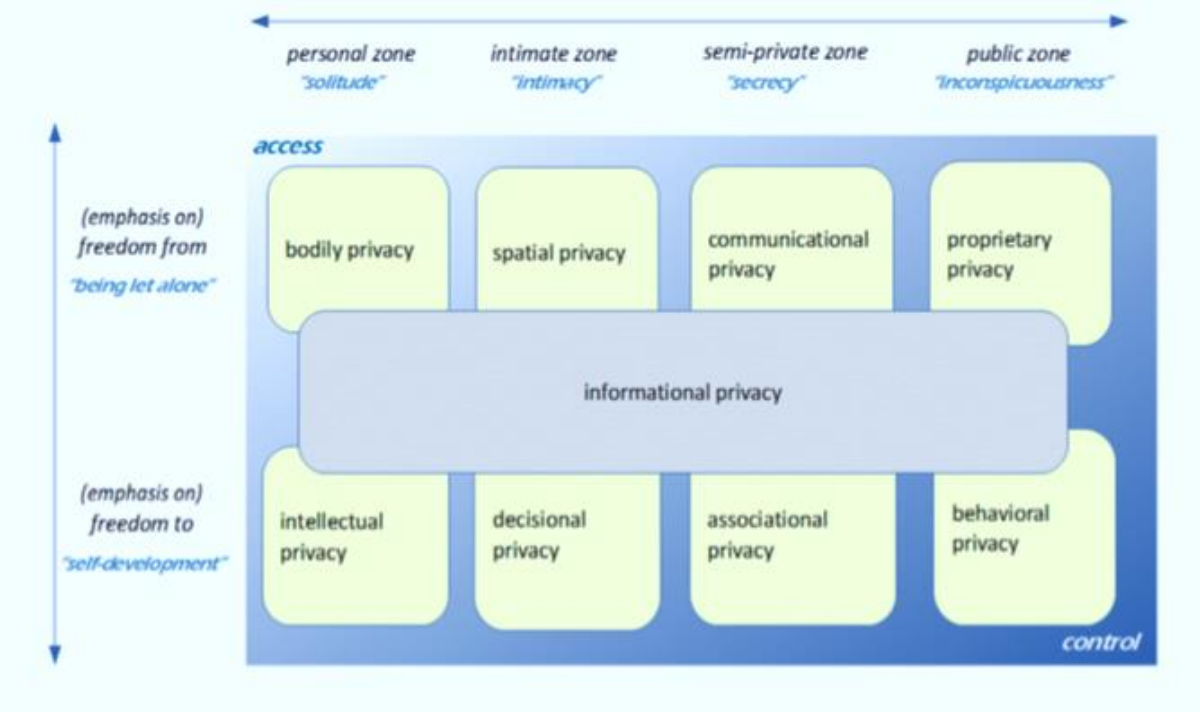
Berkaitan dengan isu konsep privasi sendiri, isu pelindungan data privasi sangat berkaitan dengan privasi ketubuhan, meskipun tidak terbatas pada hal tersebut. Pada tahun 2013, Rachel L Finn mengidentifikasikan 7 (tujuh) jenis privasi yang eksis dalam kehidupan bermasyarakat, yakni (1) privasi tubuh; (2) privasi perilaku dan tindakan; (3) privasi komunikasi; (4) privasi dan dan gambar; (5) privasi pemikiran dan perasaan; (6) privasi lokasi dan ruang; serta (7) privasi asosiasi atau kelompok. Menurutnya, privasi tubuh mencakup privasi terhadap jasmani seseorang, termasuk

---

[34] Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy,* dalam Bart van der Sloot & Aviva de Groot, (eds.), The Handbook of Privacy Studies *An Interdisciplinary Introduction, (*Amsterdam: Amsterdam University Press, 2018), hlm. 57.
[35] *Ibid*., hlm. 86.
[36] Helen Nissenbaum, *Loc.Cit*.
[37]Adam D. Moore, *Loc.Cit*.

atas biometrik dan genetik seorang individu.[38] Jika mengacu pada definisi kesehatan menurut WHO dan kategorisasi privasi ini, konsep privasi tidak terbatas pada ketubuhan, melainkan juga perilaku dan tindakan, termasuk pemikiran dan perasaan. Bahkan dalam konteks sisten informasi digital, informasi kesehatan juga dalam bentuk gambar.

Hal ini sejalan dengan klasifikasi jenis privasi yang dibentuk oleh Berta-Jaap Koops, dkk di tahun 2017. Kajian terkait penggolangan privasi yang termutakhir ini mengklasifikasikan privasi ke dalam 9 (sembilan) jenis privasi, dan privasi atas informasi memiliki keterikatan dengan 8 (delapan) jenis privasi lainnya, termasuk privasi tubuh.[39]



Sumber: Koops, 2017: 484

Pada awalnya privasi didefinisikan sebagai sesuatu yang berkaitan dengan ruang pribadi sebagai lawan dari ruang publik. Pelanggaran privasi, menurut dikotomi semacam itu, berkaitan dengan fakta-fakta pribadi milik ranah privat yang dipublikasikan secara tidak tepat. Konseptualisasi ini menimbulkan pertanyaan tentang demarkasi tentang publikasi yang tepat/tidak tepat. Hal ini selanjutnya dikaitkan dengan persetujuan dan kontrak, dan hak dianalogikan dengan kepemilikan

[38] Rachel L. Finn, et al, "Seven Types of Privacy" dalam Serge Gutwirth, et al (eds.), *European Data Protection: Coming of Age*, (Dordrecht: Springer, 2013) hal.6-8.
[39] Bert-Jaap Koops, et al, "A Typology of Privacy", 38 *U. Pa. J. Int'l L.* 2 (2017) hal.484.

dan kontrol. Helen Nissenbaum menolak dikotomi klasik anatara privat-publik tradisional dan mengusulkan kalkukasi alternatif privasi yang berkaitan dengan norma dan ekspektasi terhadap privasi dalam berbagai konteks spasial dan fungsional. Helen Nissenbaum menetapkan diferensiasi tentang keragaman konteks sosial dan pengenalannya tentang konsep integritas kontekstual sebagai perlindungan privasi yang efektif. Helen Nissenbaum mendefinisikan integritas kontekstual sebagai kepatuhan terhadap norma-norma terkait konteks. Dengan demikian, integritas dinilai bukan dengan nilai fungsional dari konteks tertentu, melainkan melalui gagasan deskriptif tentang norma dan ekspektasi. Lebih jauh Helen Nissenbaum menggambarkan integritas kontekstual sebagai penghormatan terhadap norma-norma lokal yang ada terkait dengan konteks tertentu. Oleh karena itu, karena memungkinkan adanya ekspektasi yang wajar, maka norma-norma tersebut akan dipatuhi.[40]

Helen Nissenbaum meletakkan isu privasi dalam konteks sistem sosio-teknikal *(socio- technical system)*. Apapun perangkat teknologi informasi dan komunikasi, maka ketika hendak menyigi mengapa dan bagaimana perangkat dan sistem teknologi memprovokasi kecemasan, protes, kekhawatiran, dan perlawanan atas nama privasi. Situasi ini beririsan dengan dimensi sosio-teknis. Pengaruh perangkat ini tidak hanya semata-mata karena sifat fisik atau material, tetapi oleh sifat yang melekat sebagai sistem dan perangkat yang tertanam dalam jaringan material dan sosial dan jaringan makna yang lebih luas. Penempatan dimensi sosio-teknis ini tidak terlepas dari pemaknaan privasi dalam bahasa sehari-hari dan dalam konteks hukum dan kebijakan privasi yang berarti informasi yang sensitif atau intim, informasi apa pun tentang seseorang, atau hanya informasi pengenal personal seseorang. [41]

Lebih jauh oleh karena ancaman dan pelanggaran privasi tidak hanya secara individu, kasus per kasus, tetapi secara agregat menjadi krisis sosial karena serangannya mengarah pada nilai sosial. Pada titik ini privasi beririsan dengan norma sosial, kebijakan, hukum, dan desain teknis. Kerangka integritas kontekstual *(framework of contextual integrity)* kemudian dijadikan sebagai landasan untuk mengartikulasikan kebijakan, keputusan pengadilan, hukum, serta desain dan implementasi teknologi. Integritas kontesktual berakar pada pertimbangan moral dan kemanusiaan humanistik dan berasal dari tradisi politik demokrasi liberal kontemporer. Dimensi lain yang perlu menjadi pertimbangan untuk memperkuat justifikasi integritas kontekstual adalah meletakan privasi secara eksplisit sebagai prinsip dan nilai kemanusiaan yang universal. Pembelaan privasi sebagai HAM dan menghubungkannya dengan nilai-nilai lain, seperti menunjukkan privasi sebagai

[40] Maria Brincker**,** Privacy in public and the contextual conditions of agency, dalam *Tjerk Timan, Bryce Clayton Newell and Bert-Jaap Koops* (eds.), Privacy in Public Space: Conceptual and Regulatory Challenges, (Cheltenham: Edward Elgar Publishing Limited, 2017), hlm. 66-72.

[41] Helen Nissenbaum merujuk pada ketentuan Direktif Uni Eropa yang memaknai data pribadi sebagai informasi apa pun yang berkaitan dengan orang perseorangan yang dapat diidentifikasi atau diidentifikasi (subjek data); orang yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, secara langsung atau tidak langsung, terutama dengan mengacu pada sejumlah identitas atau pada satu atau lebih faktor yang spesifik pada identitas fisik, fisiologis, mental, ekonomi, budaya, atau sosialnya. Lihat: *Ibid*. hlm. 4.

bentuk dan ekspresi kepemilikan diri, aspek hak untuk dibiarkan sendiri, landasan kebebasan dan otonomi, atau kondisi yang diperlukan untuk kepercayaan, persahabatan, kreativitas, dan otonomi moral menunjukkan bahwa privasi berisian dengan isu moralitas, politik, dan hukum.[42] Dalam konteks ini, Helen Nissenbaum merujuk secara bergantian klaim privasi yang sah secara moral (*morally legitimate claim to privacy)* dan hak privasi (*right to privacy*) untuk menentukan status hukum suatu klaim atau hak yang melekat sebagai hak hukum untuk privasi, atau klaim privasi yang diakui dalam hukum.[43]

Adam D. Moore memperkuat dimensi moralitas untuk menjustifikasi privasi:[44]

> Privasi adalah nilai inti manusia *(privacy is a core human value),* hak untuk mengontrol akses ke diri sendiri bersama dengan hak penggunaan dan kontrol atas informasi dan tempat pribadi adalah bagian penting dari perkembangan manusia.

Lon L. Fuller mengembangkan pendekatan etika kebajikan untuk privasi dan regulasi perlindungan data melengkapi paradigma hukum saat ini melalui 2 (dua) cara. Pertama, fokus pada prinsip-prinsip *rule of law* bahwa perlindungan terhadap penyalahgunaan kekuasaan yang perlu dihormati bahkan jika tidak ada hak individu atau kepentingan pribadi yang dipertaruhkan. *Kedua,* ini menetapkan pengontrol data tugas khusus menjalankan secara berhati-hati *(specifies duties of care for data controllers).* Dalam konteks ini, negara dapat berada di bawah kewajiban hukum tidak hanya untuk mencegah bahaya atau menahan diri dari menyalahgunakan kekuasaannya, tetapi juga untuk menjadi negara yang baik, negara yang menggunakan kekuatannya dengan cara terbaik.[45]

Paradigma privasi saat ini memberikan hak subjektif kepada seseorang untuk mengklaim haknya atas privasi. Hak ini melindungi kepentingannya yang sah atas martabat manusia, otonomi pribadi atau kebebasan individu. Dalam kasus-kasus konkret, kepentingan pribadi ini seimbang dengan kepentingan bersama. Fokus pada hak-hak individu dan kepentingan individu individu tidak lagi berlaku di *big data* saat ini atau istilah lain apa pun yang digunakan untuk menangkap kapasitas untuk mengumpulkan, menyimpan, menganalisis, dan menggunakan sejumlah besar data untuk semua jenis tujuan. Dalam konteks ini, meskipun hak subjektif dan kepentingan individu akan tetap penting karena seseorang harus selalu memiliki hak subjektif untuk melindungi kepentingan pribadinya. Namun demikian, perkembangan teknologi baru pada akhirnya menempatkan bahwa

---

[42] *Ibid*., hlm. 4-9
[43] *Ibid.*, hlm. 74
[44] Adam D. Moore, *Op.Cit*, hlm. 33
[45] Bart van der Sloot, Privacy As Virtue: Moving Beyond the Individual in the Age of Big Data, (Cambridge: Intersentia, 2017), hlm. 2.

privasi tidak berputar di sekitar individu dan kepentingan spesifiknya, tetapi perlu diletakkan dalam konteks yang lebih luas.[46]

A. Konsep Data Kesehatan

Berangkat dari irisan konsep privasi dan kesehatan tersebut, data atau informasi kesehatan memiliki dimensi yang cukup luas, tidak sebatas keadaan sehat atau sakit dari sudut pandang medis. Melainkan segala informasi yang berkaitan tentang bagaimana individu secara fisik dan mental. Health Insurance Portability and Accountability Act (HIPAA) atau yang sering dikenal sebagai hukum pelindungan data kesehatan di Amerika Serikat mendefiniskan data kesehatan atau informasi kesehatan: [47]

> Sebagai informasi yang dapat diidentifikasi secara individu terkait dengan status kesehatan di masa lalu, sekarang atau masa depan dari individu yang dibuat, dikumpulkan, atau ditransmisikan, dikelola oleh entitas yang mencakup HIPAA yakni terkait dengan penyediaan perawatan kesehatan, pembayaran untuk layanan perawatan kesehatan, atau penggunaan dalam operasi perawatan kesehatan (termasuk penggunaan perawatan kesehatan sektor swasta). Informasi kesehatan ini juga termasuk hasil diagnosa, informasi perawatan, hasil tes medis, dan informasi resep (dokter). Pada perkembangannya, informasi kesehatan tidak terbatas pada informasi medis melainkan juga nomor identitas nasional dan data demografi seperti tanggal lahir, gender, etnisiti, dan kontak.

Asosiasi Pengelolaan Informasi Kesehatan Amerika (AHIMA) menegaskan bahwa rekam medis, juga termasuk riwayat pasien, hasil laboratorium, X-rays, informasi klinis, informasi demografi, dan catatan dari tenaga medis. Pemantauan informasi kesehatan pasien secara individual untuk melihat kondisi dan perubahan kesehatan pasien. Sedangkan di skala besar, pengumpulan data dapat dilihat untuk melihat situasi kesehatan suatu populasi untuk mempertimbangkan bentuk intervensi medis yang dapat mengubah kondisi kesehatan.[48]

Tidak berbeda dengan definisi dan konsep dari HIPAA, Komisi Informasi Australia juga mendefinisikan informasi kesehatan sebagai data pribadi yang berkaitan dengan kesehatan dan disabilitas seorang individu. Termasuk informasi dan opini terkait dengan penyakit, cidera, dan kondisi disabilitas. Beberapa contoh data yang terkait dengan informasi kesehatan adalah: (1) Catatan berkaitan dengan diagnose dan gejala; (2) informasi berkaitan dengan layanan kesehatan yang diterima atau dijalankan; (3) Hasil laporan dan tes medis dari spesialis; (4) Resep dokter dan

---

[46] *Ibid*.
[47] https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/
[48] https://www.ahima.org/certification-careers/certifications-overview/career-tools/career-pages/health-information-101/

pembelian farmasi; (5) Riwayat layanan dokter gigi; (6) Informasi genetik; (7) rencana layanan kesehatan diri di masa depan; (8) keputusan individu terkait potensi donasi organ; (9) rincian kunjungan dokter dan penagihannya; (10) serta data pribadi lainnya yang dikumpulkan dan diproses oleh penyedia layanan kesehatan.[49]

Robin Pierce merujuk pada Beate Roessler yang mengonstruksi privasi dalam konteks medis dengan menggabungkan setidaknya 3 (tiga) konsep umum privasi, mencakup informasional, keputusan, dan lokal atau spasial. Privasi informasional telah dikodifikasikan dalam dokumen kontemporer. Perlindungan informasi kesehatan dan asal-usul privasi informasi dalam konteks medis dapat ditemukan sejauh 300 SM dalam Sumpah Hipokrates.[50] Berbagai jenis kepentingan terkandung dalam gagasan privasi keputusan dalam konteks medis. Persetujuan dari pasien semestinya didasari kapasitas, yaitu kemampuan untuk memahami sifat intervensi dan membuat keputusan yang beralasan mengenai penggunaannya. Kapasitas pasien merupakan persyaratan untuk pemberian pengobatan dan perawatan pasien. Privasi medis juga harus memperhatikan sensitivitas paparan fisik dan psikologis yang sering dialami oleh pencari perawatan di lingkungan medis. Bahkan untuk orang sehat, menjalani pemeriksaan tubuh yang merupakan bagian dari perawatan klinis rutin, individu harus mengekspos diri mereka sendiri dan menjadi rentan dengan cara yang sangat bergantung pada budaya kepercayaan. Di samping itu, juga terdapat dimensi martabat dalam privasi spasial atau lokal, yang dapat diambil dari berbagai sumber mulai dari HAM hingga prinsip dasar bioetika yang disebut sebelumnya tentang penghormatan terhadap manusia. Privasi spasial, dengan cara ini, dapat berdiri sendiri terlepas dari nilai instrumentalnya dalam memfasilitasi pemberian perawatan dengan cara yang mendukung dan mempromosikan pencarian perawatan yang tepat.[51]

Wouter Koelewijn menyatakan terdapat 3 (tiga) aspek hak atas privasi dan perlindungan data dalam konteks perawatan kesehatan seperti terlihat melalui diagram di bawah ini:[52]

---

[49] https://www.oaic.gov.au/privacy/health-information/what-is-health-information/

[50] Sumpah ini mengharuskan dokter bersumpah tidak akan mengungkapkan informasi dari setiap pasien dan menjaga rahasia pasien ini. Sumpah ini dari waktu ke waktu telah dimasukkan ke dalam etika profesi, pedoman, dan kode etik, serta memunculkan kemungkinan tindakan hukum jika terjadi pelanggaran. Lihat, Robin Pierce**,** Medical Privacy: Where Deontology and Consequentialism Meet, dalam Bart van der Sloot & Aviva de Groot, (eds.), The Handbook of Privacy Studies *An Interdisciplinary Introduction, (*Amsterdam: Amsterdam University Press, 2018), hlm. 328.

[51] *Ibid*., hlm. 328-330.

[52] Wouter Koelewijn**,** Privacy from a Medical Perspective, dalam Bart van der Sloot & Aviva de Groot, (eds.), The Handbook of Privacy Studies *an Interdisciplinary Introduction, (*Amsterdam: Amsterdam University Press, 2018), hlm. 333.



Dari ruang lingkup definisi data di atas, aktivitas dan perilaku sebenarnya tidak hanya sebatas rekam medis yang dikelola layanan kesehatan, seperti rumah sakit atau petugas medis. Selain hal tersebut rekam medis juga mencakup kehidupan fisik dan mental, serta aktivitas dan perilaku diri menyangkut dengan kesehatan, denyut detak jantung, seperti pencatatan konsumsi makanan dan minuman per hari, jam tidur, aktivitas olahraga, bobot tubuh, siklus menstruasi, tumbuh kembang janin, atau perekaman jurnal terkait kondisi mental. Dewasa ini seluruh data tersebut dapat dikelola dan diproses oleh aplikasi-aplikasi ponsel pintar atau jam tangan pintar yang semakin mudah diakses masyarakat.

B. Hak Privasi Pasien

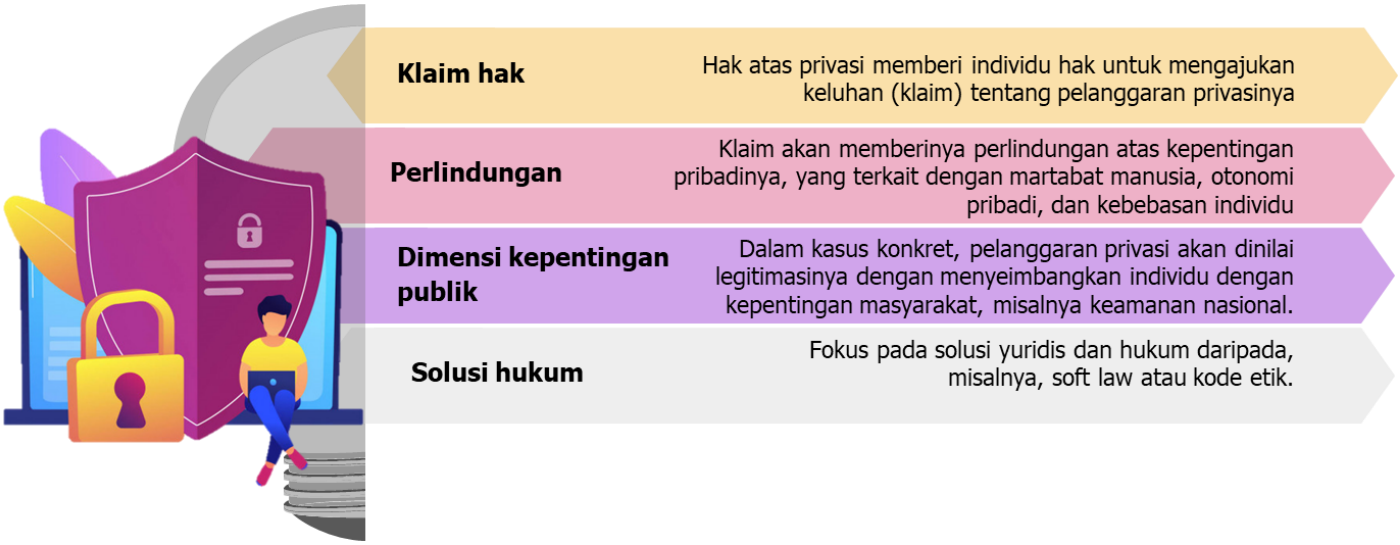
Dalam beberapa literatur berkaitan dengan hukum kesehatan, hak pasien atas kerahasiaan rekam medisnya merujuk pada perlindungan konsumen dan etika kedokteran. Sebagaimana telah disebutkan sebelumnya, kesehatan adalah bagian dari HAM. Akses terhadap pelayanan dan mendapatkan pemeliharaan tertentu merupakan bagian dari hak kesehatan yang biasanya diimplementasikan dalam bentuk penentuan standar umum mutu pelayanan kesehatan. Dalam pandangan hukum, pasien adalah subjek hukum mandiri yang dianggap dapat mengambil keputusan untuk kepentingan dirinya. Oleh karena itu, beberapa pendapat menegaskan bahwa anggapan bahwa pasien tidak dapat mengambil keputusan dikarenakan kondisi penyakit. Meskipun dalam beberapa kondisi misalnya tak sadarkan diri, dibutuhkan persetujuan dari pihak lain seperti keluarga.

Salah satu hak dan kewajiban pasien berdasarkan Surat Edaran Kementerian Kesehatan adalah berkaitan dengan hak privasi pasien yang tertuang dalam Surat Edaran Dirjen yanmed No.YM.02.04.3.5.2504 tahun 1997 yang berisikan tentang hak dan kewajiban pasien. Hak pasien adalah hak-hak pribadi yang dimiliki manusia sebagai person (pribadi indivi du): [53]

> Pasien berhak atas "*privacy*" dan kerahasiaan penyakit yang diderita termasuk data-data medisnya. Selain itu, privasi dokter yang mengobatinya juga harus dihormati. Selain itu, hak privasi atas perjanjian terapi juga menjadi salah satu bagian konsep pelindungan data pribadi di bidang kesehatan.

Secara garis besar, meskipun hak privasi dan pasien atas kerahasiaan data diakui, namun dalam konteks tata kelola data kesehatan menegaskan bahwa rekam medis adalah kepemilikan dari rumah sakit atau penyedia layanan kesehatan, meskipun terikat pada kode etik kerahasiaan dalam tata kelolanya.

Oleh karena itu, hak pasien semestinya diletakkan dalam konteks dan menjadi bagian integral dari hak atas privasi *(right to privacy).* Bart van der Sloot memaknai hal atas privasi yang dikonstruksikan berdasarkan pada individu dan kepentingannya melalui 4 (empat) elemen:[54]



[53] Y.A Triana Ohoiwutun, Bunga Rampai Hukum Kedokteran, Bayumedia Publishing, Malang, 2007, hlm.17.
[54] Bart van der Sloot, *Op.Cit.*, hlm. 7-8.

Kelompok Kerja International Dual Loyalty yang diadakan oleh Dokter untuk Hak Asasi Manusia (Physicians for Human Rights) pada 1993, menggambarkan 6 (enam) jenis umum pelanggaran HAM yang berasal dari konflik loyalitas ganda, khususnya populasi yang terpinggirkan:[55]

1. Menggunakan keterampilan atau keahlian medis atas nama negara untuk menimbulkan rasa sakit atau kerugian fisik atau psikologis yang bukan merupakan bagian yang sah dari perawatan medis;
2. Mengalihkan penilaian independen, baik dalam pengaturan terapeutik atau evaluatif, untuk mendukung kesimpulan yang menguntungkan negara atau pihak ketiga lainnya;
3. Membatasi atau menolak perawatan medis atau informasi yang berkaitan dengan perawatan individu untuk menjalankan kebijakan atau praktik negara atau pihak ketiga lainnya;
4. Mengungkapkan informasi rahasia pasien kepada otoritas negara atau pihak ketiga lainnya dalam keadaan yang melanggar HAM;
5. Melakukan evaluasi untuk kepentingan negara atau swasta dengan cara yang memfasilitasi pelanggaran HAM;
6. Tetap diam dalam menghadapi pelanggaran HAM yang dilakukan terhadap individu dan kelompok dalam perawatan profesional kesehatan.

Dalam konteks ini, konsep HAM dalam perawatan pasien *(concept of human rights in patient care)* dengan demikian meluas dari hubungan individu pasien-penyedia untuk memeriksa faktor-faktor sistemik dan tanggung jawab negara dalam penyediaan perawatan pasien. *Health and Human Rights: A Reader,* menyatakan bahwa perspektif HAM menganggap hak individu atas informasi, privasi, dan integritas tubuh secara serius dan memperlakukan semua orang secara setara mengubah pendekatan pemerintah terhadap hubungan dokter-pasien *(government approaches to the physician-patient relationship).* Konsep HAM dalam perawatan pasien mengacu tidak hanya

[55] Kelompok Kerja mengamati bahwa, baik dalam masyarakat yang represif maupun terbuka:

> Pemerintah dan pihak ketiga lainnya sering menuntut agar profesional kesehatan mengesampingkan kesetiaan kepada pasien mereka, untuk menghormati tuntutan aktor-aktor kuat ini seringkali dengan cara yang melanggar hak asasi pasien.

Kelompok Kerja memberikan contoh konteks yang dapat menimbulkan konflik loyalitas ganda, termasuk praktik kesehatan di bawah pemerintahan yang represif; institusi tertutup seperti penjara dan militer; dan masyarakat terbuka dengan bias yang dilembagakan terhadap perempuan, etnis dan agama minoritas, imigran dan pengungsi, dan pasien dengan stigma sosial. Lihat, Jonathan Cohen and Tamar Ezer Human rights in patient care: A theoretical and practical framework**,** Health and Human Rights 15/2, December 2013, https://www.hhrjournal.org/2013/12/human-rights-in-patient-care-a-theoretical-and-practical-framework/

pada hak pasien yang sebenarnya, tetapi juga pada standar HAM dalam penyediaan perawatan yang menyangkut penyedia layanan kesehatan dan seluruh masyarakat. Lebih jauh pendekatan ini menyerukan kerangka HAM yang meresap untuk mengatur pemberian perawatan kepada pasien dalam semua aspeknya, termasuk kesetaraan, partisipasi, transparansi, dan akuntabilitas.[56]

C. Pemrosesan Data Kesehatan: Potensi Ekspolitasi dan Diskriminasi

Di satu sisi, praktik eksploitasi data (kesehatan) dapat mengakibatkan diskriminasi dan berkurangnya penikmatan hak atas kesehatan ini. Praktik global menunjukan bahwa sistem perawatan kesehatan saat ini sangat bergantung pada pengumpulan dan pemrosesan data pribadi dalam jumlah besar.[57]

Sementara itu, perkembangan baru *big data* menurut Bart van der Sloot mengarah pada 4 (empat) situasi capaian berikut:[58]

1. Semakin sulit untuk menunjukkan kerugian pribadi dan untuk mengklaim hak individu,
2. Nilai yang dipertaruhkan dalam jenis proses ini sering melampaui individu;
3. Keseimbangan kepentingan yang berbeda tidak lagi memberikan instrumen eksaminasi (uji) yang memadai untuk menentukan hasil kasus karena kepentingan individu dan masyarakat yang terlibat sangat kabur;
4. Semakin sulit untuk mengatur proses *big data* dan konsekuensinya melalui doktrin hukum dan yuridis.

Padahal akses layanan kesehatan dan hak ekonomi sosial lainnya sangat bergantung pada ketersediaan identitas digital, membuat profil berdasarkan pengumpulan data tersebut, dan menggunakan model pengambilan keputusan yang bersifat otomatis. Otomatisasi dan pemanfaatan *artificial intelligence (AI)* atau kecerdasan buatan menjadi isu penting di Australia, India, Inggris dan Amerika Serikat sebab sudah mulai mengadopsi teknologi dalam program kesejahteraan digital. Kekhawatiran yang muncul adalah bagaimana peran kemajuan teknologi akan memutuskan apakah seseorang layak untuk mendapatkan layanan kesehatan. Permasalahan yang mendesak adalah realita yang menunjukan sistem AI yang masih bias dan menciptakan permasalahan serius bagi kelompok rentan dan sudah terdiskriminasi. Di Indonesia misalnya, permasalahan aksesibilitas teknologi dan identitas nasional masih merupakan tantangan tersendiri, khususnya terhadap kelompok minoritas dan daerah terpinggir yang belum terkoneksi dengan

[56] ibid
[57] https://www.privacyinternational.org/news-analysis/3619/international-health-day-during-pandemic-opportunity-reflect
[58] Bart van der Sloot, loc.cit

sistem digital. Konsekuensinya, layanan kesehatan itu belum mampu terdistribusi dengan setara dan adil.

Komunitas yang termarjinalisasi lebih memiliki risiko mengalami pelanggaran privasi dari praktik sistem data intensif. Praktik-praktik di seluruh dunia menunjukan tingkat bahaya sistem identitas dan kekerasan *online* terhadap perempuan dan komunitas LGBTQ, serta komunitas lainnya yang menjadi target pemantauan. Dalam konteks data kesehatan, tata kelola data seperti status orang dengan HIV/AIDS dan pengidap gangguan mental, dan penyakit lainnya kerap kali mengalami stigmatisasi di masyarakat sehingga meningkatkan risiko dan kerugian lebih tinggi ketika terjadi pengambilan keputusan secara otomatis dan kebocoran data terjadi.

Di India misalnya, sejak tahun 2011 dikembangkan sistem kesehatan yang memroses 120 juta data perempuan hamil dan 111 juta data anak yang telah teregistrasi pada sistem *Mother and Child Tracking System (MCTS).* Basis data ini mengumpulkan semua data setiap kunjungan perempuan, dari masa konsepsi hingga 42 hari pra-persalinan, termasuk rincian transfer dan manfaat dari skema tunjangan persalinan. Meskipun tujuan dari pemantauan ini ditujukan untuk meningkatkan layanan kesehatan yang lebih memadai. Namun demikian dalam praktiknya, MCTS menunjukan langkah-langkah pelindungan data pribadi yang kurang memadai sehingga risiko terkait kebocoran data semakin meningkat karena stigma mengenai aborsi bagi perempuan yang belum menikah atau korban perkosaan.[59] Di Argentina, komunitas anti aborsi melakukan eksploitasi data pengguna aplikasi pencatat siklus menstruasi untuk menjalankan kampanye kepentingan mereka.[60] Di masa pandemi, upaya menekan penyebaran COVID-19 kerap kali justru mengabaikan pelindungan privasi, kebijakan seperti paspor imunitas yakni sertifikasi penerima vaksin berpotensi menjadi praktik diskriminatif.[61] Di Indonesia sendiri, hak untuk berpergian antar kota diwajibkan menunjukan hasil test bebas COVID-19.

Privacy International juga mengeluarkan hasil investigasi yang menunjukan situs-situs berkaitan dengan gangguan mental menjual data pribadi pengunjungnya. 75% situs tersebut menanamkan *marketing trackers* atau pemantauan data pengunjung untuk pemasaran. Data yang disimpan adalah berkaitan dengan jawaban pengunjung situs atas pertanyaan kuis yang biasanya merupakan informasi terkait perasaan individu yang sedang merasakan kecemasan berlebih dan kombinasi data berkaitan dengan kebiasaan serta minatnya.[62] Kajian lainnya menemukan bahwa sejumlah

[59] https://www.privacyinternational.org/news-analysis/3262/mother-and-child-tracking-system-understanding-data-trail-indian-healthcare
[60] https://www.privacyinternational.org/long-read/3856/country-case-study-sexual-and-reproductive-rights-argentina
[61] https://www.privacyinternational.org/long-read/4350/anytime-and-anywhere-vaccination-passports-immunity-certificates-and-permanent
[62] https://www.privacyinternational.org/campaigns/your-mental-health-sale

aplikasi pencatat siklus menstruasi membagikan data pribadi sesitif, termasuk data pengguna yang terdiri dari aktivitas seksualnya kepada pihak ketiga tanpa persetujuan penggunanya.[63]

D. Memahami Dasar Hukum Pemrosesan Data Kesehatan

Standar yang paling relevan dalam adopsi teknologi kesehatan digital dalam konteks COVID-19 adalah hak atas kesehatan, nondiskriminasi, manfaat dari kemajuan ilmiah, dan privasi. [64] Diskriminasi dan kesetaraan menjadi elemen inti dari hukum HAM internasional. Pasal 2 Deklarasi Universal Hak Asasi Manusia 1948 menyatakan bahwa setiap manusia berhak atas semua hak dan kebebasan tanpa pembedaan dalam bentuk apa pun, seperti ras, warna kulit, jenis kelamin, bahasa, agama, pandangan politik atau pendapat lain, kebangsaan, atau asal-usul sosial, properti, kelahiran atau status lainnya. Demikian pula, Kovenan Hak-Hak Sipil dan Politik dan Kovenan Hak-Hak Ekonomi, Sosial dan Budaya mewajibkan negara pihak untuk menjamin penikmatan semua hak tanpa diskriminasi dalam bentuk apa pun. Dalam perkembangan HAM kemudian juga akan terlihat upaya melindungi privasi individu, yang termanifestasikan dalam Deklarasi Universal Hak Asasi Manusia dan pada Kovenan Hak-Hak Sipil dan Politik yang menciptakan suatu keharusan hukum bagi negara-negara untuk memastikan bahwa tidak seorang pun dikenakan gangguan sewenang-wenang atau tidak sah atas privasi, keluarga, rumah atau korespondensinya, atau serangan yang tidak sah terhadap kehormatan dan reputasinya.

Dalam konteks negara menghadapi krisis nasional, seperti keadaan darurat kesehatan masyarakat mengemuka perdebatan pembatasan atau menangguhkan hak dan kebebasan individu, termasuk privasi. Negara mulai mengakui bahwa kesehatan masyarakat dapat digunakan sebagai dasar untuk membatasi hak-hak tertentu. Prinsip Siracusa, menjadi prinsip rujukan untuk memastikan bahwa setiap pembatasan hak-hak sipil dan politik hanya dapat dilakukan dalam kondisi berikut: (1) bila diterapkan sebagai upaya terakhir; (2) ketika ditentukan oleh hukum, yaitu, tidak dipaksakan secara sewenang-wenang); (3) ketika terkait dengan kepentingan publik, misalnya, perlindungan kesehatan masyarakat); dan (4) bila dianggap perlu, proporsional dengan kepentingan publik, dan tanpa tindakan yang tidak terlalu mengganggu atau membatasi.[65]

---

[63] https://www.privacyinternational.org/video/3197/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data-video

[64] Nina Sun, et. al., Human Rights and Digital Health Technologies Volume 22/2, December 2020, https://www.hhrjournal.org/2020/12/human-rights-and-digital-health-technologies/

[65] Prinsip-prinsip Siracusa menjadi prinsip rujukan pengurangan HAM, khususnya di bidang kesehatan yang harus selaras dengan tata kelola kesehatan global sesuai dengan Peraturan Kesehatan Internasional (nternational Health Regulations). Tujuan Peraturan Kesehatan Internasional adalah untuk mencegah, melindungi, mengendalikan, dan memfasilitasi tanggapan kesehatan masyarakat terhadap penyebaran penyakit internasional, dan mereka menjadikan pengawasan sebagai pusat untuk membimbing masyarakat terhadap ancaman penyakit lintas batas. Upaya menyeimbangkan manfaat sosial dari pengawasan kesehatan masyarakat terhadap pelanggaran negara terhadap hak-hak individu. Selanjutnya revisi Peraturan Kesehatan Internasional pada 2005 untuk pertama kalinya memasukkan HAM ke dalam pengendalian penyakit menular, dengan fokus pada pertimbangan HAM dalam pengawasan

Pelindungan data pribadi menjadi penting karena menurut Nina Sun dan kawan-kawan terdapat 3 (tiga) potensi bahaya yang terkait dengan teknologi kesehatan digital yang dapat berhubungan dengan privatisasi, serta sistem kesehatan masyarakat, termasuk pelanggaran data, bias, dan fungsi yang merembet. Ketiga potensi bahaya tersebut sebagai berikut:[66]

1. Pelanggaran data *(data breach)*
   Pelanggaran data mengacu pada setiap pelanggaran keamanan yang mengarah pada penghancuran, kehilangan, perubahan yang tidak disengaja atau melanggar hukum, pengungkapan yang tidak sah atau akses ke data pribadi. Pelanggaran data umum terjadi di sektor kesehatan dan memiliki berbagai penyebab, misal dari *malware* dan peretasan hingga pengungkapan informasi kesehatan pribadi yang tidak disengaja atau disengaja oleh karyawan perawatan kesehatan;

2. Bias dan diskriminasi *(bias and discrimination)*[67]
   Dalam perawatan kesehatan, aplikasi AI menunjukkan penggunaan algoritma tidak memberikan prediksi yang sama akuratnya terkait hasil kesehatan lintas ras, jenis kelamin, atau status sosial ekonomi. Hal ini menimbulkan kekhawatiran bahwa AI akan semakin membudayakan diskriminasi dan prasangka terhadap individu berdasarkan alasan ini. Untuk menyoroti keprihatinan ini, Pelapor Khusus Perserikatan Bangsa-Bangsa tentang bentuk-bentuk rasisme kontemporer sedang mengembangkan laporan tentang teknologi informasi baru, nondiskriminasi, dan kesetaraan ras. Selain itu, jenis keputusan algoritma tertentu menghindari undang-undang nondiskriminasi saat ini, yang mengarah ke diferensiasi tidak adil yang secara teknis legal. Misalnya, menawarkan harga yang berbeda untuk produk yang sama berdasarkan kecepatan akses internet) tetapi dapat merusak tujuan pencapaian hak atas kesehatan bagi semua.

3. Fungsi yang merembet (*Function creep)*
   Fungsi yang merembet terjadi ketika data yang dikumpulkan untuk tujuan tertentu, misalnya, informasi pribadi yang diberikan sebagai bagian dari pemeriksaan medis kemudian digunakan untuk tujuan lain, seperti untuk memeriksa status imigrasi. Kekhawatiran tentang fungsi *creep* relevan untuk semua bentuk teknologi kesehatan digital, terutama berkaitan dengan biometric. Sebagai contoh data biometrik yang dikumpulkan untuk tujuan kesehatan digital dapat digunakan untuk forensik atau

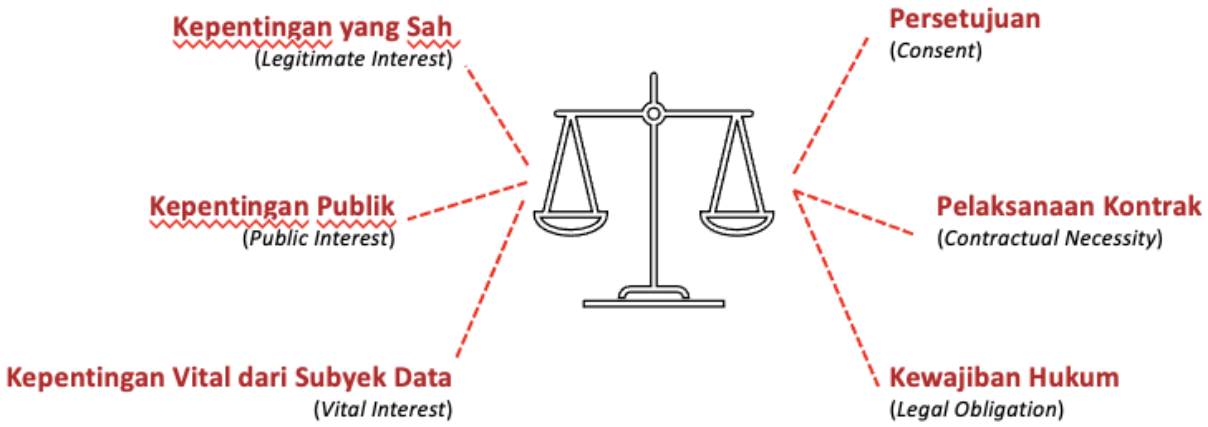
penyakit. Peraturan tersebut menyusun tanggapan negara terhadap keadaan darurat kesehatan masyarakat yang menjadi perhatian internasional dengan cara yang sepadan dengan, dan terbatas pada, risiko kesehatan masyarakat dan menghindari campur tangan yang tidak perlu dengan lalu lintas internasional, perdagangan, dan HAM. Lihat, Sharifah Sekalala, et.al, op.cit

[66] Nina Sun, et. al, op.cit

[67] Perlakuan yang berbeda telah berulang kali didokumentasikan sebagai akibat dari bias algoritmik dalam AI dan proses otomatis lainnya. Fenomena ini dapat memperkuat diskriminasi dalam proses peradilan pidana dan pendekatan prediktif pada kepolisian, memfasilitasi keputusan perekrutan yang diskriminatif, atau menghasilkan kampanye *microtargeting* yang memiliki efek diskriminatif. Lihat: *Ibid*.

proses pidana. Fungsi *creep* juga dapat menyebabkan pelanggaran data. Misalnya, perangkat aplikasi kebugaran mengungkapkan informasi yang dapat digunakan untuk mengidentifikasi rumah individu, tempat kerja dan ibadah, atau bisnis yang sering dikunjungi. Kemitraan pemerintah dengan perusahaan swasta, termasuk perusahaan teknologi besar, juga telah meningkatkan kekhawatiran terkait potensi fungsi *creep* dengan eksploitasi data untuk pengawasan atau tujuan komersial.

Dalam prinsip pelindungan data pribadi, setiap pemrosesan data pribadi harus didasari pada dasar hukum atau *legal ground.* Adapun dasar hukum bisa diperoleh pengendali dan pemroses data dari: (1) Persetujuan Subjek Data; (2) Pelaksanaan Kontrak; (3) Kewajiban hukum; (4) Kepentingan Vital dari Subjek Data; (5) Kepentingan Publik; (6) Kepentingan yang sah.



Dalam konteks data kesehatan, biasanya pengumpulan data pribadi sektor ini berkaitan dengan: (1) Kewajiban Hukum; (2) Kepentingan Vital dari Subjek Data; (3) Kepentingan Publik. Dalam hal kewajiban hukum, biasanya kewenangan pemrosesan data didasarkan karena pengaturan perundangan-undangan. Misalnya dalam berkaitan dengan Karantina Wilayah untuk penanggulangan penyebaran penyakit menular, biasanya memiliki UU khusus yang memberikan kewenangan terkait penutupan wilayah dan pemrosesan serta kontrol data kesehatan dan data pribadi pasien. Sedangkan alasan kepentingan publik, biasanya berkaitan dengan upaya menjaga kesehatan masyarakat secara luas, sehingga diperlukan pengawasan dan kontrol yang memungkinkan pemrosesan data pribadi yang cukup ketat.

Sebagai contoh di masa pandemic COVID-19, dalam rangka menekan angka penyebaran, beberapa negara mengeluarkan sejumlah kebijakan yang mengharuskan pengumpulan data kesehatan termasuk hasil test COVID-19 untuk penanggulangannya. Misalnya, Riwayat perjalanan pasien COVID-19. Alasan 'Kepentingan Vital Subjek Data atau *vital interest* merupakan salah satu poin penting sebagai dasar hukum pemrosesan suatu data. Pemrosesan data kesehatan, kerap kali mendasarkan *vital interest* sebagai pada *legal ground* yang menyangkut berkaitan hidup-matinya pasien; atau dalam hal keanggotan secara terus menerus berhubungan dengan suatu organisasi non-profit sehingga organisasi yang bersangkutan bisa melakukan pemrosesan data pasien, termasuk mengakses data pribadi (sensitif) pasien. Meskipun demikian, keseluruhan akses data kesehatan tidak serta merta dapat diidentifikasikan sebagai *vital interest.*

Dalam pengelolaan data kesehatan sebagai bagian dari sistem informasi kesehatan, mereka pengendali data juga dapat menunjuk prosesor data, yaitu orang-perseorangan *(natural persoon)* atau badan hukum *(natural legal person),* otoritas publik, agensi atau badan lain yang memproses data pribadi atas nama pengendali. Artinya, pengendali data dapat melakukan pemrosesan data secara mandiri (dilakukan pada institusinya sendiri) atau dapat pula menunjuk orang atau pihak lain, yang bertindak atas nama pengendali. Secara umum dalam kapasitas sebagai pengendali maupun prosesor data, berbagai institusi yang terlibat dalam pengelolaan sistem informasi kesehatan setidaknya memiliki 6 (enam) bentuk kewajiban: (1) tanggung jawab dan kepatuhan; (2) memastikan keamanan pemrosesan; (3) merekam kegiatan pemrosesan; (4) kerahasiaan data pribadi (pasien); (5) pemberitahuan jika terjadi pelanggaran/kebocoran); (6) penilaian dampak perlindungan data *(data protection impact assessment).* Dalam hal tanggung jawab dan kepatuhan, kewajiban dari pengendali, prosesor, maupun juga pengendali gabungan, dapat diidentifikasi berikut ini:

Pengendali	Menerapkan langkah-langkah teknis dan organisasi untuk kepatuhan undang-undang
	Memastikan pelaksanaan seluruh prinsip dalam pemrosesan data pribadi
	Mematuhi pedoman perilaku
	Menerapkan *privacy by design* dan *privacy by default*
	Memastikan sistem keamanan dalam pemrosesan data pribadi

Prosesor	Bertindak berdasarkan perintah tertulis dari pengendali data. kecuali atas perintah undang-undang.
	Menerapkan langkah teknis dan organisasi
	Menunjuk sub-prosesor hanya dilakukan jika ada persetujuan dan pengendali data
Pengendali Gabungan	Secara transparan menentukan tanggung jawab masing-masing untuk kepatuhan dengan kewajiban berdasarkan UU.
	Melakukan pengaturan mekanisme bersama
	Subjek data dapat menggunakan haknya terhdap masing-masing pengendali data

E. Instrumen panduan dalam tata kelola data kesehatan

Secara konseptual, pelindungan data pribadi terdiri dari beberapa prinsip-prinsip utama berkaitan dengan pelindungan data pribadi adalah:[68]

1. Adil, Sah dan Transparan *(fair, lawful, and transparent)*
   Data pribadi harus diproses secara adil dan transparan untuk memastikan bahwa data pribadi tidak digunakan untuk tujuan yang tidak dipahami oleh Subjek Data. Penting bagi Subjek Data untuk mengetahui bagaimana dan oleh siapa data pribadinya diproses. Selain itu, pemrosesan data pribadi juga harus dilakukan berdasarkan dasar hukum pemrosesan data pribadi yang sah;

[68] Privacy International, "The Keys to Data Protection", 2018, hlm.36-47, https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf.

2. Pembatasan Tujuan *(purpose limitation)*
   Data pribadi hanya diperbolehkan untuk dikumpulkan untuk tujuan yang telah ditetapkan, spesifik dan sah. Pemrosesan data pribadi lanjutan lainnya tidak boleh bertentangan dengan tujuan pemrosesan yang telah ditentukan saat pengumpulan data pribadi. Secara singkat, prinsip ini bertujuan untuk mencegah pemrosesan data pribadi untuk tujuan lain yang tidak disetujui oleh Subjek Data saat memberikan persetujuan tanpa pemberitahuan yang jelas;

3. Minimisasi Data *(data minimization)*
   Pemrosesan hanya diperbolehkan terhadap data pribadi yang diperlukan dan relevan untuk memenuhi tujuan pemrosesan data pribadi tersebut. Oleh karenanya, minimisasi data mensyaratkan pengendali data untuk melakukan pemrosesan terhadap jumlah minimum data pribadi yang diperlukan;

4. Akurasi Data *(data accuracy)*
   Data pribadi harus dijaga agar tetap akurat dalam keseluruhan siklus pemrosesan data. Hal ini dapat dilakukan dengan mengimplementasikan beberapa hal seperti memastikan bahwa data pribadi yang dikumpulkan merupakan data yang lengkap dan merupakan data terbaru;

5. Pembatasan Penyimpanan *(storage limitation)*
   Data pribadi hanya boleh disimpan untuk jangka waktu yang dibutuhkan untuk mencapai tujuan pemrosesan yang ditentukan saat pengumpulan data. Prinsip ini memiliki keterkaitan erat dengan kewajiban pengendali data untuk menghapus data pribadi pada saat berakhirnya pemrosesan data.

6. Integritas dan Kerahasiaan *(integrity and confidentiality)*
   Prinsip ini menitikberatkan pada kewajiban pengendali data untuk mengimplementasikan tindakan-tindakan untuk memastikan keamanan data pribadi. Hal ini dilakukan untuk mencegah adanya akses tidak sah, kerusakan dan kebocoran data pribadi yang disimpan oleh pengendali data. Adapun tindakan keamanan yang harus diimplementasikan oleh pengendali data mencakup tindakan keamanan fisik, misalnya pengamanan terhadap akses masuk ke dalam infrastruktur fisik, menerapkan kartu akses khusus, keamanan organisasi (menerapkan kontrol akses terhadap individu tertentu), keamanan informasi dan teknis, misalnya menerapkan enkripsi, pseudonimisasi, anonimisasi, pengawasan risiko, dan seterusnya.

7. Akuntabilitas *(accountability)*
8. Baik pengendali maupun prosesor data pribadi harus bertanggung jawab dan pelindungan data pribadi. Dalam hal terjadinya kegagalan pelindungan data pribadi,

pengendali dan prosesor data pribadi juga memiliki kewajiban untuk memberikan pemulihan terhadap subjek data pribadi yang terlanggar haknya.

Prinsip-prinsip pelindungan data pribadi tersebut umumnya dituangkan ke dalam sebuah regulasi komprehensif mengenai pelindungan data pribadi yang bertujuan untuk mengembalikan kontrol data pribadi kepada subjek data. Regulasi-regulasi pelindungan data pribadi yang ada saat ini baik di tingkat regional maupun nasional memberikan pelindungan yang lebih tinggi bagi pemrosesan data pribadi yang bersifat sensitif. Hal ini didasari oleh pemikiran bahwa data pribadi, khususnya yang bersifat sensitif, memiliki keterkaitan yang erat terhadap pemenuhan HAM subjek data pribadi sehingga memerlukan perlindungan khusus. Kondisi ini yang melahirkan sejumlah instrumen dan prinsip yang dikembangkan secara khusus untuk meningkatkan pelindungan data pribadi pada sektor kesehatan, baik di tingkat regional tertentu maupun organisasi internasional.

III. Instrumen Pelindungan Data dari World Health Organization (WHO)

A. Pemaknaan Pengaturan Privasi dan Data Pribadi Berdasarkan Konstitusi WHO

Konstitusi WHO yang telah diadopsi oleh *International Health Conference* pada 1946 pada dasarnya tidak menyebutkan secara khusus mengenai privasi dan pelindungan data pribadi. Substansi di dalamnya lebih banyak membahas mengenai keorganisasian WHO. Meski begitu, setidaknya terdapat 1 (satu) prinsip yang dapat dijadikan sebagai rujukan dalam konteks pembahasan privasi dan pelindungan data pribadi. Disebutkan bahwa:

> Kesehatan adalah keadaan fisik, mental, dan kesejahteraan sosial secara menyeluruh yang tidak terbatas hanya pada ketiadaan penyakit atau kelemahan fisik atau mental.

Berangkat dari pemaknaan tersebut, maka dapat ditarik benang merah bahwa data kesehatan adalah data yang terkait dengan keadaan fisik, mental, dan kesejahteraan sosial secara menyeluruh yang tidak terbatas hanya pada ketiadaan penyakit atau kelemahan fisik atau mental. Dengan begitu, data-data tersebutlah yang perlu dipertimbangkan terkait dengan bagaimana pengumpulan, pengelolaan, dan pelindungannya agar tidak melanggar hak atas privasi.

Tentu, keberadaan Konstitusi WHO tidak cukup untuk menyelenggarakan hak atas privasi dan pelindungan data pribadi. Sebagai pelengkap ketentuan dalam Konstitusi WHO, terdapat berbagai upaya, regulasi, kebijakan, dan lainnya yang telah dilakukan oleh WHO. Sampai saat ini, paling tidak WHO telah menggunakan keamanan informasi yang didasarkan pada standar ISO 27001[69] dalam melakukan keamanan data yang disimpan.[70] Lebih lanjut, WHO memiliki kebijakan keamanan informasi yang resmi dan komprehensif dengan masing-masing pedoman implementasi.[71] Kebijakan tersebut meliputi keamanan informasi, akses terhadap informasi dan sistem, *cloud computing*, keamanan aplikasi, klasifikasi informasi, dan standar keamanan yang terkait.[72]

Mengenai regulasi, WHO memiliki *International Health Regulation 2005* (IHR) yang telah mengakomodir ketentuan terkait data pribadi. Dalam regulasi ini, dinyatakan bahwa:[73]

---

[69] Lihat: ISO, "ISO/IEC 27001 Information Security Management", *ISO*, https://www.iso.org/isoiec-27001-information-security.html diakses pada 7 Januari 2021.
[70] WHO, "WHO policy on the use and sharing of data collected by WHO in Member States outside the context of public health emergencies", *WHO*, https://www.who.int/about/who-we-are/publishing-policies/data-policy diakses pada 7 Januari 2021.
[71] *Ibid.*
[72] *Ibid.*
[73] Pasal 1 *International Health Regulation 2005*.

> Data pribadi berarti setiap informasi yang terkait dengan orang yang teridentifikasi atau dapat diidentifikasi.

Berkaca dari definisi ini, WHO telah memiliki pandangan data pribadi secara lebih terbuka, yakni yang teridentifikasi atau dapat diidentifikasi. Hal ini menjadi relevan dengan kebutuhan pelindungan data, bahkan jika diterapkan saat ini.

Selain itu, telah dikenal juga istilah surveilans, yang berarti pengumpulan, pemeriksaan, dan analisis data secara sistematis dengan tujuan kesehatan masyarakat dan penyebaran informasi kesehatan masyarakat secara tepat waktu untuk pengkajian dan respon kesehatan masyarakat sesuai dengan kebutuhan.[74] Lebih lanjut, terdapat pasal khusus yang mengatur mengenai pelindungan data pribadi, yakni Pasal 45 IHR. Bahkan, negara yang mengumpulkan dan menerima data dari negara lain atau WHO harus menjaga kerahasiaan data dan pemrosesan yang dilakukan harus dilakukan secara anonim. Meski begitu, negara dapat membuka dan memproses data pribadi yang diperlukan untuk tujuan penilaian dan pengelolaan risiko kesehatan publik, dengan memastikan beberapa hal berikut:

1. Diproses secara adil dan sah, serta tidak dilakukan pemrosesan lanjutan yang tidak sejalan dengan tujuan—yang ditentukan di awal;

2. Memenuhi syarat, relevan, dan tidak berlebihan dalam kaitannya dengan tujuan;

3. Akurat dan diperbaharui ketika diperlukan; setiap langkah yang masuk akal harus diambil untuk memastikan bahwa data yang tidak akurat atau tidak lengkap dihapus atau diubah; dan

4. Tidak disimpan terlalu lama dari yang dibutuhkan.

Tidak hanya itu, jika terdapat permintaan, WHO juga sedapat mungkin menyediakan seseorang data pribadinya dalam bentuk yang dapat dimengerti, tanpa penundaan atau biaya yang tidak semestinya, dan memungkinkan adanya koreksi pada saat diperlukan.

Adanya berbagai ketentuan yang telah diatur dalam IHR pada dasarnya telah sejalan dengan beberapa prinsip yang ada dalam pelindungan data pribadi, yakni terkait dengan prinsip keabsahan (*lawfulness*), prinsip batasan tujuan (*purpose limitation*), prinsip akurasi (*accuracy*), prinsip batasan penyimpanan (*storage limitation*), serta prinsip kerahasiaan dan keamanan (*confidentiality and*

[74] *Ibid*.

security). Tentu, adanya keselarasan ini menjadi satu bekal baik bagi WHO untuk mengembangkan pelindungan data pribadi, yang merupakan bentuk penghargaan terhadap hak atas privasi. Terlebih, terdapat salah satu prinsip IHR yang menyatakan bahwa implementasi IHR harus sepenuhnya menghormati martabat, hak asasi manusia, dan kebebasan dari seseorang. Jika kita mencoba menginterpretasikan prinsip tersebut, maka "hak atas privasi" merupakan salah satu aspek yang seharusnya dihormati.

Pada 2016, WHO merilis "*Policy Statement on Data Sharing by the World Health Organization in the Context of Public Health Emergencies*" yang secara eksplisit menyatakan bahwa pernyataan ini hanya terkait data, bukan sampel biologis.[75] Tujuan utama pembagian data oleh WHO selama keadaan darurat kesehatan masyarakat adalah untuk mengizinkan analisis yang memungkinkan pemahaman sepenuhnya tentang keadaan darurat dan untuk memastikan bahwa keputusan didasarkan pada bukti terbaik yang tersedia.[76] Adapun, pernyataan kebijakan ini dibuat untuk menjelaskan posisi WHO dalam menyediakan akses data dalam 3 (tiga) kategori[77]:

1. Respon terhadap surveilans, epidemiologi, dan keadaan darurat

   Sejalan dengan Pasal 11 IHR mengenai ketentuan informasi oleh WHO, WHO akan membuka dan menerbitkan informasi yang diterima dalam Bagian II IHR (Informasi dan Respon Kesehatan Masyarakat), ketika persyaratan untuk pembukaan (Pasal 11ayat 2 dan 4[78]) telah terpenuhi. Dalam pernyataan ini, yang dimaksud dengan data termasuk data hasil surveilans dan pemantauan (menginformasikan epidemiologi), dari respon keadaan darurat, misalnya pelacakan kontak, vaksinasi, dan perawatan; dan data terkait fasilitas kesehatan, misalnya jumlah dan lokasi dari pusat pasien rawat inap dan rawat jalan serta staf dan fasilitas medis yang tersedia di pusat-pusat tersebut. Untuk melindungi privasi dan memastikan kerahasiaan data, data akan dianonimisasi. Anonimisasi akan menghapus seluruh pengidentifikasi dan pencari lokasi pribadi. Mengenai hal ini, tunduk pada persyaratan pelindungan data pribadi yang ada pada Pasal 45 IHR sebagaimana telah dijelaskan sebelumnya. Upaya juga dilakukan untuk mengkurasi data sehingga meningkatkan kegunaannya, serta analisis, dan laporan lanjutan dari data baru yang dihasilkan akan didorong. Dalam kasus pengecualian, dimungkinkan untuk tidak membagikan sub-kumpulan data, jika terdapat alasan yang kuat. Selain itu, WHO akan konsultasi dengan negara-negara yang terdampak untuk menginformasikan kepada mereka terkait dengan pembukaan data. WHO menekankan bahwa negara-negara harus memberikan keuntungan yang didapat dari pemanfaatan data

[75] WHO, "Policy Statement on Data Sharing by the World Health Organization in the Context of Public Health Emergencies", *WHO*, 13 April 2017, https://www.who.int/docs/default-source/publishing-policies/who-policy-statement-on-data-sharing.pdf?sfvrsn=71a41493_0 diakses pada 6 januari 2021.
[76] *Ibid*.
[77] *Ibid*.
[78] Lihat: *International Health Regulations 2005*

yang diterima melalui WHO dengan negara asal, sejalan dengan komitmen internasional yang berlaku.

2. Data/informasi urutan genetik

   WHO akan menganjurkan urutan genom patogen untuk dibuat tersedia secara publik secepat mungkin melalui database yang relevan. Adapun, keuntungan yang didapat dari pemanfaatan urutan-urutan tersebut dibagikan secara adil dengan negara dimana urutan genom patogen berasal. Ini mengacu hanya pada pembagian publik mengenai urutan, bukan sampel biologis. Mengenai sampel biologis, akan menjadi pembahasan pada kebijakan WHO yang terpisah yang sedang disiapkan[79].

3. Studi observasi dan percobaan klinis

   Seluruh perlakuan (intervensi) uji klinis harus diregistrasi secara prospektif dalam sebuah pendaftaran uji klinis utama, menyesuaikan dengan standar yang disetujui oleh *Platform* Pendaftaran Uji Klinis Internasional WHO (who.int/ictrp). Selama keadaan darurat kesehatan masyarakat, sebelum setiap uji dimulai, setiap protokol penelitian harus membuat sebuah komitmen khusus untuk membagikan hasil pada percepatan linimasa yang telah ditentukan sebelumnya. WHO berpandangan bahwa pengungkapan hasil kepada publik akan menjadi norma, dalam percepatan linimasa seperti yang ditentukan oleh protokol penelitian. Di luar keadaan darurat kesehatan masyarakat, normanya adalah pengungkapan hasil kepada publik dalam waktu 12 (dua belas) bulan setelah penyelesaian uji coba. Selain itu, transparansi tentang pelaksanaan percobaan hewan juga penting untuk pengembangan obat dan vaksin. WHO akan mengkomunikasikan pentingnya transparansi dan catatan publik dari semua model hewan dengan hasil utama harus diurus dan diperbarui.

Selanjutnya pada 2017, WHO mengeluarkan sebuah kebijakan *Policy on Use and Sharing of Data Collected in Member States by the World Health Organization (WHO) Outside the Context of Public Health Emergencies (Provisional)*. Kebijakan ini dibuat untuk menjelaskan kebijakan dan praktik penggunaan dan berbagi data yang dikumpulkan Negara Anggota oleh WHO di luar konteks keadaan darurat kesehatan publik. Melalui kebijakan ini, disebutkan bahwa tujuan utama dari pembagian data adalah untuk[80]:

---

[79] Lihat: WHO, "Sharing biological samples and data during public health emergencies", *WHO,* https://www.who.int/blueprint/what/norms-standards/sample-and-data-sharing/en/ diakses pada 6 Januari 2021.

[80] WHO, "The Policy on the Use and Sharing of Data Collected by WHO in Member States Outside the Context of Public Emergencies", *WHO,* https://www.who.int/docs/default-source/publishing-policies/who-data-sharing-policy-collected-by-

1. Meningkatkan kesehatan publik melalui analisis guna menciptakan pemahaman yang komprehensif terkait tantangan kesehatan;

2. Membantu mengembangkan solusi baru; dan

3. Memastikan bahwa pilihan telah didasarkan pada bukti terbaik yang ada.

Kebijakan ini diterapkan terhadap data yang disediakan oleh Negara Anggota kepada WHO, lain daripada data yang diterbitkan oleh Negara Anggota tanpa batasan apa pun dalam penggunaannya. Kebijakan berbagi data ini dijabarkan, sebagai berikut:[81]

1. Mencakup penggunaan dan berbagi data saja, bukan sampel biologis;

2. Mencakup penggunaan dan berbagi data yang dikumpulkan oleh WHO dan/atau diberikan kepada WHO oleh Negara Anggota di luar konteks kesehatan masyarakat dalam keadaan darurat;

3. Tidak termasuk berbagi data dalam konteks kesehatan masyarakat dalam keadaan darurat, termasuk deklarasi PHEICs secara resmi dibawah IHR 2005;

4. Tidak termasuk data dan laporan dari uji klinis;

5. Memperbolehkan, tetapi tidak ada kewajiban, WHO atau Negara Anggota untuk mengumpulkan, menganonimkan, menganalisis, atau membagikan data kesehatan selain yang sudah dikumpulkan, dianonimkan, dianalisis, dan dibagikan;

6. Tidak akan diimplementasikan secara retrospektif terhadap data yang telah disediakan oleh Negara Anggota kepada WHO dan/atau yang telah dibagikan oleh WHO kepada pihak ketiga.

Selain itu, melalui kebijakan berbagi data diluar kedaruratan kesehatan publik, terdapat 6 (enam) ketentuan dalam melakukan pembagian data. Ketentuan-ketentuan ini dibuat dalam rangka

member-states-outside-of-public-health-emergencies61d03608e6134ba786ad94403e947013.pdf?sfvrsn=bb52b31d_31 diakses pada 18 November 2020.

[81] *Ibid*.

mencegah adanya konsekuensi-konsekuensi yang tidak diinginkan. Berikut merupakan ketentuan tersebut: [82]

1. Menjaga keamanan data sensitif, yang mungkin berpengaruh terhadap perjalanan dan perdagangan;

2. Menjaga privasi dan anonimitas individu;

3. Menjaga orang dan populasi dari adanya stigmatisasi atau penargetan yang tidak adil;

4. Menjaga kepentingan Negara Anggota yang membagikan data;

5. Mendorong penguatan kapasitas diantara Negara Anggota yang mengumpulkan dan membagikan data;

6. Menyesuaikan dengan kepastian yang dibuat untuk pasien, peserta penelitian, dan pihak terkait lainnya tentang bagaimana data akan digunakan, dibagikan, disimpan atau dilindungi, dan dengan harapan yang sah yang mungkin dimiliki individu tersebut tentang berbagi data.

Adanya berbagai ketentuan di atas patut diapresiasi, mengingat adanya upaya WHO dalam rangka pelindungan data pribadi. Namun demikian, dalam hal ini WHO belum memberikan adanya kejelasan mengenai maksud data sensitif, *apakah seluruh atau hanya sebagian data kesehatan yang dinilai sensitif?* Jika kita merujuk pada GDPR dan legislasi-legislasi terkait pelindungan data pribadi di berbagai negara, misalnya Korea dan Filipina, disebutkan bahwa data kesehatan termasuk dalam data pribadi sensitif sehingga diperlukan adanya penjelasan data sensitif yang lebih mendalam oleh WHO.

Dalam Perkembangannya, pada 10 Agustus 2020, WHO mengeluarkan *WHO Data Principles*.[83] *WHO Data Principles* lahir berdasarkan proses konsultasi internal dan telah diulas dalam konsultasi dengan ahli dari eksternal, yang diselenggarakan oleh WHO pada Mei-Juni 2020. Prinsip tersebut merupakan sebuah pondasi untuk menegaskan kembali kepercayaan masyarakat terhadap informasi dan bukti yang dimiliki WHO terkait kesehatan publik. *WHO Data Principles* ini ditujukan bagi seluruh staf yang terlibat dalam kerja-kerja WHO agar dapat memaknai nilai dan

[82] *Ibid*.
[83] WHO, "World Health Organization Data Principles", *WHO*, 10 Agustus 2020, https://www.who.int/data/principles diakses pada 12 November 2020.

standar yang digunakan mengenai bagaimana arus data di dalam dan di luar WHO dikumpulkan, diproses, dibagikan, dan digunakan.

Adapun, pokok-pokok substansi dalam *WHO Data Principles* adalah sebagai berikut:[84]

1. Organisasi Kesehatan Dunia (WHO) harus menilai data sebagai barang public.
   Organisasi Kesehatan Dunia (WHO) harus berusaha untuk merilis data secara publik dan membagikannya dengan aman dan sesuai etik. Adapun, ketentuan tersebut boleh dikesampingkan dengan keadaan-keadaan sebagai berikut:

   a. Permintaan spesifik dari Negara Anggota untuk tidak membagikan data;

   b. Data yang dibagikan antara WHO dan pihak ketiga, termasuk Negara Anggota dan mitra yang mengimplementasikan, terdapat sebuah pengecualian kerahasiaan;

   c. Data yang jika dibuka dapat membahayakan keselamatan dan keamanan dari tiap-tiap individu atau memiliki sebuah akibat pada terlaksananya hak asasi mereka;

   d. Data yang jika dibuka dapat membahayakan keamanan dari Negara Anggota atau kerugian keamanan atau pelaksanaan operasi atau aktivitas apa pun yang dilakukan oleh WHO;

   e. Data dibagikan, baik secara internal maupun eksternal, dengan tujuan hanya digunakan untuk keperluan organisasi (misalnya draf dokumen, email, dan lainnya);

   f. Data keuangan yang jika dibuka akan membahayakan kepentingan keuangan WHO atau mitranya;

   g. Data yang jika dibuka akan merusak dialog kebijakan dengan Negara Anggota atau mitra yang mengimplementasikan;

[84] *Ibid*.

h. Jenis data lain yang karena kontennya atau keadaan-keadaan dibentuknya, harus dianggap rahasia.

Prinsip ini juga berlaku terhadap data registrasi vital, data survei, dan hasil dari perhitungan atau penelitian, dan situasi dimana data telah dibagikan dengan WHO oleh entitas bukan Negara Anggota, termasuk produsen data sektor privat yang bekerja sama dengan WHO dalam proyek bersama. Dalam menjalankan prinsip ini, WHO akan menyediakan panduan yang jelas dan memastikan transparansi. Mengenai transparansi, WHO akan melakukan transparansi mengenai bagaimana data dikumpulkan dan digunakan. Menelaah pokok substansi di atas, sangat nampak implementasi prinsip integritas dan kerahasiaan (*integrity and confidentiality*) serta prinsip transparansi (*transparency*) yang ada dalam pelindungan data pribadi.

Dalam menjalankan prinsip yang pertama ini, WHO juga bertindak untuk menyediakan panduan yang jelas terhadap situasi yang memperbolehkan adanya pencegahan atas alasan yang sah terhadap pembagian data. Panduan yang dibuat tersebut, akan konsisten dengan aturan dan kebijakan WHO yang berlaku, termasuk kebijakan berbagi data, kebijakan pengungkapan informasi, dan kebijakan pelindungan data pribadi. Persetujuan yang diinformasikan (*informed consent*) hampir selalu dibutuhkan untuk data yang ditujukan untuk penelitian. Untuk pengumpulan data rutin dengan tujuan surveilans kesehatan masyarakat, *informed consent* tidak selalu diperlukan. Untuk data pribadi, persetujuan (*consent*) subjek data harus menjadi dasar untuk memproses data. Penggunaan frasa subjek data (bukan pemilik data) oleh WHO tersebut telah sejalan dengan konsep pelindungan data pribadi. Jika dihubungkan dengan pemaknaan subjek data yang ada dalam hukum pelindungan data pribadi, maka subjek data merupakan orang-perorangan yang dalam dirinya melekat data-data yang mengidentifikasi/dapat mengidentifikasi dirinya. Hal ini tentu berimplikasi pada bagaimana cakupan pelindungan terhadap hak-hak subjek data nantinya.

a. *Information Disclosure Policy*[85]

Kebijakan ini memuat prinsip-prinsip dalam akses informasi yang meliputi:

1) Informasi yang dapat diakses publik harus tersedia, sepanjang masuk akal dan berguna, melalui laman WHO;

[85] WHO, "Information Disclosure Policy", *WHO,* Maret 2017, https://www.who.int/docs/default-source/documents/about-us/infodisclosurepolicy.pdf?sfvrsn=c1520275_10 diakses pada 18 November 2020.

2) Kebijakan ini dilandaskan pada prinsip-prinsip keterbukaan dan transparansi, seperti informasi apapun tentang WHO dapat diakses publik, atau tersedia atas permintaan, kecuali satu atau lebih dari pengecualian terhadap Kebijakan, atau alasan kuat lainnya, berlaku.

Kebijakan ini juga mengkategorikan informasi menjadi tiga, yakni Informasi yang secara publik tersedia, informasi yang tersedia atas permintaan, dan informasi rahasia.

b. *The Policy on the Use and Sharing of Data Collected by WHO in Member States Outside the Context of Public Emergencies*[86]

Kebijakan ini diterapkan terhadap data[87] yang dibagikan oleh Negara Anggota kepada WHO. Mengenai pembagian data tersebut merupakan keharusan bagi Negara Anggota untuk segera menyampaikan kepada WHO mengenai undang-undang, peraturan, laporan resmi dan statistik penting yang berkaitan dengan kesehatan yang telah dipublikasikan di Negara yang bersangkutan.[88] Selanjutnya, kebijakan berbagi data ini dijabarkan sebagai berikut:

1) Mencakup penggunaan dan berbagi data saja, bukan sampel biologis;

2) Mencakup penggunaan dan berbagi data yang dikumpulkan oleh WHO, dan/atau diberikan kepada WHO oleh Negara Anggota di luar konteks kesehatan masyarakat dalam keadaan darurat;

3) Tidak termasuk berbagi data dalam konteks kesehatan masyarakat dalam keadaan darurat, termasuk deklarasi PHEICs secara resmi dibawah *International Health Regulation* (2005);

4) Tidak termasuk data dan laporan dari uji klinis;

---

[86] WHO, "The Policy on the Use and Sharing of Data Collected by WHO in Member States Outside the Context of Public Emergencies", *Op.Cit*.

[87] Data yang dimaksud adalah data: Survei rumah tangga yang didukung WHO, data kematian catatan unit, data agregat kematian, data agregat fasilitas kesehatan, data fasilitas kesehatan berbasis kasus, data pengeluaran kesehatan, survei fasilitas kesehatan, data penelitian kesehatan (selain uji klinis), survei informan kunci, laporan survei nasional, data surveilans penyakit, dan surveilans penyakit yang wajib dilaporkan. Lihat: Lampiran 3 "The Policy on the Use and Sharing of Data Collected by WHO in Member States Outside the Context of Public Emergencies", *Op.Cit*.

[88] Lihat: Pasal 63 Konstitusi WHO.

5) Memperbolehkan, tetapi tidak ada kewajiban, WHO atau Negara Anggota untuk mengumpulkan, menganonimkan, menganalisis, atau membagikan data kesehatan selain yang sudah dikumpulkan, dianonimkan, dianalisis, dan dibagikan;

6) Tidak akan diimplementasikan secara retrospektif terhadap data yang telah disediakan oleh Negara Anggota kepada WHO, dan/atau yang telah dibagikan oleh WHO kepada pihak ketiga.

c. *The Policy Open Access*[89]

Dalam melaksanakan kebijakan ini, terdapat berbagai tindakan yang dilakukan oleh WHO:

1) Mewajibkan semua karya yang ditulis WHO atau didanai WHO untuk tersedia secara gratis dibawah lisensi publikasi yang sesuai dengan tujuan yang diuraikan, seperti lisensi *Creative Commons IGO*;

2) Mewajibkan salinan elektronik dari karya yang ditulis WHO atau didanai WHO untuk tersedia melalui *Europe PMC* dan IRIS, dalam waktu 6 (enam) bulan dan paling lambat 12 (dua belas) bulan dari tanggal publikasi resmi;

3) Termasuk biaya akses terbuka, sebagai perkiraan, dalam penerapannya kepada donor untuk dukungan proyek;

4) Mengenali biaya biaya akses terbuka, sebagai perkiraan, dalam aplikasi untuk proyek dukungan yang diterimanya dari entitas luar untuk mendukung proyek mereka, yaitu dimana WHO bertindak sebagai lembaga pendanaan.

2. Kewajiban WHO Menjunjung Tinggi Kepercayaan Negara Anggota terhadap Data.
Organisasi Kesehatan Dunia (WHO) harus menjunjung tinggi kepercayaan yang diberikan oleh Negara Anggota ketika WHO memproses data Negara Anggota yang telah dibagi dan ditempatkan dibawah kendali WHO. Berdasarkan hal tersebut, WHO akan menyediakan konsultasi yang imparsial dan inklusif, pemrosesan dan penyimpanan yang aman, serta mengimplementasikan HAM, khususnya hak atas privasi. Dalam rangka

[89] WHO, "WHO Policy on Open Access", *WHO*, https://www.who.int/about/who_policy.pdf diakses pada 18 November 2020.

mengimplementasikan HAM, khususnya hak atas privasi, WHO menegakkan standar tertinggi pelindungan data dan menghormati HAM, khususnya hak atas privasi, terkait dengan data pribadi apa pun dan kumpulan data kelompok individu, termasuk dalam kumpulan data yang dikontrol WHO. Hal ini khususnya penting untuk kumpulan data yang mengharuskan penanganan secara hati-hati dan perhatian khusus, seperti data kesehatan serta data individu dan kelompok rentan dan termarjinalkan, termasuk anak-anak. Hal tersebut mengharuskan Negara Anggota dan bukan Negara Anggota yang berbagi data dengan WHO untuk mengkonfirmasi bahwa data yang telah dikumpulkan sesuai dengan hukum nasionalnya, termasuk hukum pelindungan data yang bertujuan melindungi kerahasiaan orang yang dapat diidentifikasi.

3. <u>WHO Harus Mendukung Data Negara Anggota dan Kapasitas Sistem Informasi Kesehatan.</u>
Organisasi Kesehatan Dunia (WHO) harus mendukung aktivitas peningkatan kapasitas dari Negara Anggota, bertujuan untuk keberlanjutan dan berbagi praktik terbaik kapanpun dimungkinkan, secara spesifik untuk pengembangan tata kelola data, sistem informasi manajemen kesehatan, statistik kesehatan publik, ilmu data terkait kesehatan, dan inovasi data kesehatan. Berangkat dari prinsip tersebut, WHO akan merespon permintaan Negara Anggota untuk pendukung; memajukan pengambilan keputusan berbasis bukti dengan berfokus pada informasi sistem manajemen yang berkelanjutan (HMIS) dan sistem pengembangan digital; serta selaras dengan proses, struktur, dan anggaran pemantauan dan evaluasi milik nasional.

4. <u>WHO Harus Bertanggung Jawab Sebagai Manajer dan Pengurus Data.</u>
Organisasi Kesehatan Dunia (WHO) akan memastikan semua data tersedia untuk diproses, dikelola, dianalisis, didiseminasi, dan digunakan sesuai dengan standar internasional dan praktik terbaik dalam manajemen data kesehatan. Hal tersebut meliputi standar tata kelola data PBB yang relevan dan panduan yang berlaku untuk WHO sesuai dengan mandatnya, termasuk standar yang dirujuk dalam pembukaan. Lebih lanjut, WHO harus memastikan bahwa semua data yang dihasilkannya secara konsisten memenuhi standar audit yang transparan dan tahun referensi umum, serta tepat waktu, akurat, sebanding, dan dapat diakses, jika memungkinkan secara teknis dan hukum. Berangkat dari prinsip ini, WHO akan mengaplikasikan standar data spesifik internasional, menjaga dan memperkuat persekutuan dengan pemangku kepentingan yang terkait, memperkuat kualitas upaya pengawasan SDG, dan mengadaptasi konteks yang spesifik.

5. <u>WHO harus Berusaha Keras Untuk Memenuhi Kesenjangan Data Kesehatan Publik.</u>
Organisasi Kesehatan Dunia (WHO) akan mendukung Negara Anggota untuk memenuhi kesenjangan data kesehatan publik. Hal tersebut dilakukan melalui pengumpulan data empiris dan prediktif, transparan dan metode pemodelan yang koheren dengan validitas yang telah terbukti. Oleh karenanya, WHO akan menggunakan model dan metode

transparan. Dengan begitu, Negara Anggota menggunakan berbagai indikator kesehatan untuk mengawasi kesehatan masyarakat dan memandu alokasi sumber daya. Namun, tantangan timbul dari ketiadaan data, metode yang tidak konsisten dan seringkali tata kelola dan standar data yang belum berkembang di semua tingkat ekonomi. Organisasi Kesehatan Dunia (WHO) akan mendukung Negara Anggota untuk menghasilkan estimasi yang koheren (yang mungkin didasarkan pada data yang sumbernya berlainan atau tidak lengkap) yang semuanya terbuka untuk pemeriksaan, transparansi, tersedia untuk publik, dan terbukti kebenarannya.

Selanjutnya pada 2020 untuk memperkuat respons menghadapi COVID-19, WHO merilis *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing* yang memuat 17 (tujuh belas) prinsip WHO dalam teknologi pelacakan berbasis digital.[90] Pedoman ini dimaksudkan untuk mendorong tanggung jawab dan pendekatan berbasis HAM bagi pihak-pihak yang melakukan pengembangan atau penerapan teknologi pelacakan kontak COVID-19.

Tabel berikut merupakan pedoman singkat mengenai 17 (tujuh belas) prinsip yang direkomendasikan:

No	Prinsip	Penjelasan
1.	Batasan Waktu	Segala tindakan dalam pelacakan kontak COVID-19 harus bersifat sementara dan memiliki cakupan batasan.
2.	Melakukan Tes dan Evaluasi	Teknologi wajib dites dan dievaluasi sebelum digunakan.
3.	Proporsional	Pemrosesan data harus dilakukan secara proporsional dan berlandaskan hukum.
4.	Minimalisasi Data	Pemrosesan data harus terbatas pada data yang diperlukan.
5.	Menggunakan Pembatasan	Data yang digunakan harus terbatas pada tujuan kesehatan masyarakat.

[90] WHO, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing", *WHO*, 28 Mei 2020, h. 3-5.

6.	Kesukarelaan	Penggunaan aplikasi dilakukan secara sukarela dan diberitahukan.
7.	Transparansi dan Kejelasan	Pemrosesan data wajib dilakukan secara transparan dan diuraikan secara jelas.
8.	Penyimpanan Data dengan Melindungi Privasi	Penyimpanan data wajib dilakukan secara efektif, aman, dan melindungi privasi.
9.	Keamanan	Memiliki keamanan tinggi, termasuk enkripsi, wajib dipastikan setiap saat.
10.	Penyimpanan Terbatas	Penyimpanan data hanya boleh dilakukan selama periode respon pandemi.
11.	Melaporkan Infeksi	Pelaporan harus dilakukan dengan persetujuan atau melalui pelaporan sendiri.
12.	Pemberitahuan	Pemberitahuan kontak wajib dilakukan secara jelas, informatif, mudah diakses, dan melindungi privasi.
13.	Pelacakan Kasus COVID-19	Pengguna yang berstatus pasien tidak boleh dilacak saat dirawat dan sedang dalam pemulihan.
14.	Ketepatan	Kualitas data wajib dijaga untuk menghindari akibat yang tidak diinginkan.
15.	Akuntabilitas	Wajib ada mekanisme pengaduan dan perlindungan terhadap penyalahgunaan data.
16.	Pengawasan Independen	Wajib ada pengawasan independen terhadap entitas yang terlibat.
17.	Keterlibatan Masyarakat Sipil dan Publik	Harus ada upaya untuk melibatkan berbagai pihak.

IV. Instrumen Pelindungan Data Menurut *General Data Proection Regulation (GDPR)*

Pasal 4 ayat (15) GDPR menggunakan istilah 'data mengenai kesehatan', bukan 'data kesehatan'. Penggunaan istilah tersebut tentu berkonsekuensi pada cakupan data yang dimaksud, yakni lebih luas dari hanya sekadar data kesehatan, melainkan data-data yang juga berhubungan dengan kesehatan. Mengacu pada pasal tersebut data mengenai kesehatan didefinisikan sebagai:

> Data pribadi yang berkaitan dengan kesehatan fisik dan mental manusia, termasuk ketentuan jasa perawatan kesehatan, yang mengungkapkan informasi tentang status kesehatannya.

Memaknai pasal tersebut, kiranya perlu dirujuk *Recital 35 concerning Health Data*. Di dalamnya memberikan penjelasan berikut:

> Data pribadi tentang kesehatan harus mencakup semua data yang berkaitan dengan status kesehatan subjek data yang mengungkapkan informasi yang berkaitan dengan status kesehatan fisik atau mental subjek data di masa lalu, saat ini, atau masa depan. Ini termasuk informasi tentang orang yang dikumpulkan selama pendaftaran, atau penyediaan, layanan perawatan kesehatan seperti yang dirujuk dalam *Directive* 2011/24/EU kepada orang tersebut; nomor, lambang atau hal tertentu yang diberikan kepada seseorang untuk secara unik mengidentifikasi orang tersebut untuk tujuan kesehatan; informasi yang diperoleh dari pengujian atau pemeriksaan bagian tubuh atau bahan tubuh, termasuk dari data genetik dan sampel biologis; dan setiap informasi tentang, misalnya, penyakit, kedisabilitasan, risiko penyakit, riwayat medis, perawatan klinis atau keadaan fisiologis atau biomedis dari subjek data yang tidak bergantung pada sumbernya, misalnya dari dokter atau profesional kesehatan lain, rumah sakit, perangkat medis atau tes diagnostik *in vitro*.

Dalam GDPR data kesehatan masuk dalam kategori data pribadi khusus. Pengkategorian tersebut berkonsekuensi pada bagaimana sebuah data harus diproses. Secara umum, GDPR memuat berbagai prinsip dalam melakukan pemrosesan data pribadi. Prinsip tersebut, meliputi prinsip keabsahan dan transparansi (*lawfulness, fairness and transparency*); prinsip batasan tujuan (*purpose limitation*); prinsip minimalisasi data (*data minimization*); prinsip akurasi *(accuracy)*; prinsip retensi/batasan penyimpanan (*retention/storage limitation*); prinsip integritas dan kerahasiaan (*integrity and security*); dan prinsip akuntabilitas (*accountability*).

Pemrosesan data pribadi khusus pada dasarnya dilarang, kecuali jika:[91]

1. Subjek data memberikan '*explicit consent*' untuk pemrosesan data pribadinya dengan satu atau lebih tujuan spesifik, kecuali hukum Uni Eropa atau Negara Anggota menyatakan bahwa larangan pemrosesan data yang terkategorikan khusus tersebut tidak dapat dicabut oleh subjek data;

2. Pemrosesan diperlukan untuk tujuan melaksanakan kewajiban dan menjalankan hak-hak spesifik pengendali atau subjek data dalam ruang lingkup pekerjaan dan keamanan sosial dan hukum pelindungan sosial sejauh disahkan oleh hukum Uni Eropa atau Negara Anggota atau persetujuan bersama berdasarkan hukum Negara Anggota menyediakan pengamanan yang sesuai untuk hak-hak dasar dan kepentingan subjek data;

3. Pemrosesan diperlukan untuk melindungi kepentingan vital subjek data atau orang lain, dimana subjek data secara fisik atau secara hukum tidak mampu memberikan '*consent*';

4. Pemrosesan dilakukan dalam kegiatannya yang sah dengan pengamanan yang sesuai oleh yayasan, asosiasi, atau badan nirlaba lainnya dengan tujuan politik, filosofis, agama, atau serikat pekerja dan dengan syarat bahwa pemrosesan hanya berkaitan dengan anggota atau kepada mantan anggota badan atau orang-orang yang secara teratur berhubungan dengannya sehubungan dengan tujuannya dan bahwa data pribadi tidak diungkapkan di luar badan itu tanpa persetujuan dari subjek data;

5. Pemrosesan berkaitan dengan data pribadi yang secara nyata dibuat publik oleh subjek data;

6. Pemrosesan diperlukan untuk membentuk, menjalankan, atau mempertahankan klaim hukum atau kapanpun pengadilan bertindak dalam kapasitasnya;

7. Pemrosesan diperlukan untuk alasan substansial kepentingan publik, dengan dasar hukum Uni Eropa atau Negara Anggota yang seharusnya proporsional untuk tujuan yang diikuti, menghormati esensi hak pelindungan data dan menyediakan pengukuran yang tepat dan spesifik untuk pengamanan hak-hak fundamental dan kepentingan-kepentingan subjek data;

[91] Pasal 9 ayat (2) *General Data Protection Regulation*.

8. Pemrosesan diperlukan untuk tujuan pengobatan preventif atau okupasi, untuk penilaian kapasitas kerja karyawan, diagnosis medis, penyediaan perawatan atau perawatan kesehatan atau sosial atau manajemen sistem dan layanan perawatan kesehatan atau sosial berdasarkan undang-undang Uni Eropa atau Negara Anggota atau sesuai dengan kontrak dengan kesehatan profesional dan tunduk pada kondisi dan pengamanan:

   > *Ketika data-data tersebut diproses oleh atau dibawah tanggung jawab profesional tunduk pada kewajiban kerahasiaan profesional dibawah hukum Uni Eropa atau Negara Anggota atau peraturan yang ditetapkan oleh badan nasional atau oleh orang lain yang merupakan subjek dari kewajiban kerahasiaan di bawah hukum Serikat atau Negara Anggota atau peraturan yang ditetapkan oleh badan nasional*;

9. Pemrosesan diperlukan untuk alasan kepentingan publik dalam bidang kesehatan masyarakat, seperti melindungi dari ancaman lintas batas yang serius terhadap kesehatan atau memastikan standar kualitas dan keamanan yang tinggi dari perawatan kesehatan dan produk obat atau perangkat medis, berdasarkan hukum Uni Eropa atau Negara Anggota yang mengatur tindakan yang sesuai dan spesifik untuk melindungi hak dan kebebasan subjek data, khususnya kerahasiaan profesional; dan

10. Pemrosesan diperlukan untuk tujuan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau sejarah atau tujuan statistik sesuai dengan Pasal 89 (1) berdasarkan undang-undang Uni Eropa atau Negara Anggota yang harus proporsional dengan tujuan yang dikejar, menghormati esensi hak untuk perlindungan data dan menyediakan langkah-langkah yang sesuai dan spesifik untuk melindungi hak-hak dasar dan kepentingan subjek data.

Atas ketentuan pelarangan dan kondisi-kondisi di atas, negara-negara anggota dapat mempertahankan atau memperkenalkan kondisi lebih lanjut, termasuk pembatasan, yang berkaitan dengan pemrosesan data genetik, data biometrik, atau data tentang kesehatan.

Adanya pemrosesan terhadap data pribadi khusus, harus diproses untuk tujuan yang berhubungan dengan kesehatan untuk kepentingan perorangan dan masyarakat secara keseluruhan, khususnya dalam konteks pengelolaan layanan dan sistem kesehatan atau perawatan sosial.[92] Hal ini termasuk pemrosesan oleh manajemen dan otoritas kesehatan nasional pusat untuk: [93]

[92] Recital 53 tentang Pemrosesan Data Sensitif dalam Sektor Kesehatan dan Sosial dan Recital 54 tentang Pemrosesan Data Sensitif dalam Sektor Kesehatan dan Sosial.
[93] *Ibid*.

1. Tujuan pengendalian kualitas, informasi manajemen, dan pengawasan nasional dan lokal dari sistem perawatan kesehatan atau sosial, dan memastikan kesinambungan perawatan kesehatan atau sosial dan lintas-perawatan kesehatan perbatasan atau keamanan kesehatan;
2. Tujuan pemantauan dan peringatan;
3. Tujuan pengarsipan untuk kepentingan publik;
4. Tujuan penelitian ilmiah atau sejarah atau tujuan statistik, berdasarkan hukum Uni Eropa atau Negara Anggota yang harus memenuhi tujuan kepentingan publik; serta
5. Untuk studi yang dilakukan untuk kepentingan umum di bidang kesehatan masyarakat.

Selanjutnya, pengolahan kategori khusus data pribadi mungkin diperlukan untuk alasan kepentingan publik di bidang kesehatan masyarakat tanpa persetujuan subjek data.[94] Proses tersebut harus tunduk pada tindakan yang sesuai dan spesifik untuk melindungi hak dan kebebasan orang perseorangan.[95] Dalam konteks tersebut, "kesehatan masyarakat" harus diartikan sebagaimana didefinisikan dalam *Regulation No 1338/2008 of the European Parliament and the Council*:[96]

> Semua unsur yang terkait dengan kesehatan, yaitu status kesehatan, termasuk morbiditas dan disabilitas, faktor penentu yang berpengaruh pada status kesehatan, kebutuhan perawatan kesehatan, sumber daya yang dialokasikan untuk perawatan kesehatan, penyediaan dan akses universal terhadap perawatan kesehatan serta pengeluaran dan pembiayaan perawatan kesehatan, dan penyebab kematian.

Proses data yang berkaitan dengan kesehatan untuk alasan kepentingan publik tidak boleh mengakibatkan data pribadi diproses untuk tujuan lain oleh pihak ketiga, seperti pemberi kerja atau perusahaan asuransi dan perbankan.[97]

---

[94] Recital 54 tentang Pemrosesan Data Sensitif dalam Sektor Kesehatan dan Sosial.
[95] *Ibid*.
[96] *Ibid*.
[97] *Ibid*.

V. PRAKTIK PELINDUNGAN DATA KESEHATAN DI BERBAGAI NEGARA

A. Korea Selatan

Korea Selatan memiliki *Personal Information Protection Act* 2011 (PIPA) yang telah diamandemen pada 4 Februari 2020. Mengacu pada undang-undang ini, data kesehatan dikategorikan sebagai informasi sensitif. Meski begitu, tidak terdapat adanya klausula lanjutan yang mengatur mengenai data kesehatan. Selain regulasi umum mengenai pelindungan data pribadi tersebut, Korea Selatan juga memiliki beberapa peraturan perundang-undangan yang berkaitan dengan data kesehatan, diantaranya adalah *Bioethics and Safety Act, Act on the Promotion of the Provision and Use of Public Data, Medical Service Act*, dan *Framework Act on Health and Medical Services*.

Berdasarkan *Bioethics and Safety Act*, penelitian "*biospecimen*"[98] diperbolehkan hanya ketika sebuah rencana penelitian disetujui oleh *Institutional Review Board* (IRB) dan dengan kesepakatan tertulis dari donatur *biospecimen*.[99] Sementara itu, dalam dominasi publik, *Act on the Promotion of the Provision and Use of Public Data* memegang peran penting. Berdasarkan undang-undang ini, *National Health Insurance Services* (NHIS) dan *Health Insurance Review & Assessment Service* (HIRA) menyediakan akses terhadap data yang dipegang untuk tujuan penelitian.[100] Lebih dari itu, *National Evidence-Based Healthcare Collaborating Agency* mempunyai kewenangan untuk membuat permintaan kepada instansi pemerintah dan organisasi publik untuk menyerahkan data terkait kesehatan, dan instansi serta organisasi tersebut wajib untuk menyerahkan data tersebut setelah menyunting informasi yang dapat diidentifikasi secara pribadi.[101]

Di Korea Selatan, terdapat berbagai instansi yang terlibat dalam rangka pengumpulan (dan seharusnya pelindungan) data kesehatan, mereka memiliki tugas dan fungsi yang berbeda-beda, meliputi:[102]

---

[98] Sebuah sampel material, seperti urin, darah, jaringan seluler, sel, DNA, RNA, atau protein, dari manusia, hewan, atau tumbuhan. Biospecimen dapat digunakan untuk tes laboratorium atau disimpan di "*biorepository*" yang akan digunakan untuk penelitian. Lihat: https://www.cancer.gov/publications/dictionaries/cancer-terms/def/biospecimen diakses pada 7 Januari 2021.
[99] Dongjin Lee, dkk., "Protecting and Utilizing Health and Medical Big Data: Policy Perspectives from Korea", *Healthcare Information Research*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6859269/ diakses pada 4 Januari 2021.
[100] *Ibid*.
[101] *Ibid*.
[102] *Ibid*.

1. NHIS

    a. Mengelola *big data* asuransi kesehatan;

    b. Mengurus *database* yang besar, mencakup hampir semua penduduk di Korea Selatan. Bahkan telah dibangun sebuah sistem *database* tambahan untuk tujuan penelitian. Adapun, *database* dalam kategori ini termasuk data kelompok sebagaimana 'data khusus' tertentu.

    c. Mengurus sebuah prosedur untuk memberikan akses terhadap *database* tersebut.

2. HIRA

    Memiliki tugas untuk menyediakan akses terhadap data untuk peneliti melalui sistem terbuka *big data* kesehatan dan medis.

3. *National Cancer Center*

    Mengurus sebuah pusat data nasional untuk kanker dan mengadakan aktivitas penelitian mengenai, antara lain, membangun platform *big data* untuk pengobatan terhadap kanker yang tepat.

4. *Korea Centers for Disease Control and Prevention*

    Mengurus sebuah bank sumber daya manusia sebagai bagian dari usaha keras secara nasional untuk membangun dan mengurus bank *biospecimen*. Pada saat bersamaan menjadi pusat sumber daya untuk patogen saat melakukan Studi Genom dan Epidemiologi Korea.

Selanjutnya mengenai *Medical Service Act*, yang mengatur mengenai pemeliharaan rekam medis.[103] Walaupun merupakan kewajiban untuk menyimpan catatan medis di dalam lokasi masing-masing rumah sakit dan klinik, ketentuan terkait dari *Medical Services Act* yang diubah pada tahun 2016, menjadikan rekam medis dapat disimpan di luar lokasi.[104] Melalui amandemen ini, penggunaan

[103] Lihat: *Medical Service Act*, 29 Mei 2016, https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=39874&type=abc&key=MEDICAL%20SERVICE%20ACT&param=M diakses pada 7 Januari 2021.
[104] *Ibid*.

layanan komputasi awan juga diizinkan.[105] Saat ini, beberapa rumah sakit besar mengurus pusat *big data*-nya sendiri.[106] Beberapa dari mereka telah mengembangkan prosedur dan sistem internal untuk de-identifikasi data medis dan untuk memberikan akses terhadap data-data tersebut dalam kerangka tujuan penelitian.[107] Secara terpisah, rumah sakit dengan orientasi penelitian tertentu berusaha keras untuk membangun *platform* untuk melakukan penelitian tentang penyakit tertentu dan bidang khusus.[108]

Dalam kerangka ini *Framework Act on Health and Medical Services*, istilah informasi pelayanan kesehatan dan medis berarti pengetahuan yang berkaitan dengan pelayanan kesehatan dan medis atau seluruh jenis data yang dinyatakan dalam bentuk kode, angka, surat, suara, bunyi, gambar, dan lainnya.[109] Disebutkan di dalam kerangka ini bahwa pengungkapan informasi rahasia tentang tubuh, kesehatan, atau kehidupan pribadi warga negara yang berkenaan dengan layanan kesehatan dan medis pada dasarnya tidak diperbolehkan.[110] Selain itu, terdapat 2 (dua) kewenangan penting yang dimiliki oleh pemerintah berkaitan dengan data kesehatan:

1. Negara dan pemerintah lokal harus merumuskan dan mengimplementasikan kebijakan yang dibutuhkan untuk mengumpulkan dan mengelola statistik dan informasi pelayanan kesehatan dan medis dan memanfaatkan statistik dan informasi tersebut untuk kebijakan mengenai pelayanan kesehatan dan medis.[111]

2. Menteri Kesehatan, Kesejahteraan, dan Keluarga harus merumuskan kebijakan untuk melakukan standarisasi pelayanan kesehatan dan medis, untuk mengoperasikan informasi secara efektif mengenai pelayanan kesehatan dan medis dan kesesuaian yang aman, dan lainnya.[112]

Berangkat dari ketentuan-ketentuan yang ada pada *Framework Act on Health and Medical Services*, diketahui bahwa terdapat kesadaran pemerintah Korea Selatan dalam rangka melakukan perlindungan data kesehatan. Terlihat adanya prinsip batasan tujuan (*purpose limitation*) yang direpresentasikan melalui salah satu kewenangan negara, yakni:

---

[105] *Ibid*.
[106] *Ibid*.
[107] *Ibid*.
[108] *Ibid*.
[109] Pasal 3 angka 6 *Framework Act on Health and Medical Services*
[110] Pasal 13 *Framework Act on Health and Medical Services*
[111] Pasal 53 *Framework Act on Health and Medical Services*
[112] Pasal 57 *Framework Act on Health and Medical Services*

> ... informasi tersebut untuk kebijakan mengenai pelayanan kesehatan dan medis. Selain itu, adanya frasa ...kesesuaian yang aman, dan lainnya" memungkinkan adanya upaya perketatan pelindungan.

B. Filipina

Pada 2008, terjadi "*cebu canister scandal*" di Vincente Sotto Memorial Medical Center (VSMMC), Filipina.[113] Kasus tersebut terjadi lantaran terdapat tenaga medis yang merekam (sambil menertawakan) proses operasi rektal seorang pasien gay yang kemudian diunggah ke YouTube.[114] Tindakan perekaman dan pengunggahan tersebut dilakukan tanpa sepengetahuan atau persetujuan pasien.[115] Atas tindakan tersebut, Departemen Kesehatan Filipina menjatuhkan skorsing selama tiga bulan kepada tenaga medis yang terlibat. Kejadian ini tentu erat kaitannya dengan kurangnya pelindungan terhadap data kesehatan.

Mengenai data pribadi secara umum, Filipina memiliki *Republic Act 10173 – Data Privacy Act of 2012* sebagai rujukan yang utama. Undang-undang ini telah mengakomodir pengklasifikasian informasi pribadi sensitif, termasuk di dalamnya adalah informasi kesehatan dan catatan kesehatan sebelumnya atau *cm-rent*. Pengklasifikasian sebuah data menjadi data sensitif tersebut mengantarkan pada adanya pemrosesan yang juga tidak bisa dilakukan secara biasa. Di Filipina, pemrosesan informasi pribadi akan diizinkan hanya jika tidak dilarang oleh hukum, dan jika setidaknya telah terdapat kondisi-kondisi yang telah ditentukan.[116] Misalnya ketika subjek data telah memberikan *consent*, dilakukan karena diperlukan dan berkaitan dengan pemenuhan kontrak dengan subjek data, dan diperlukan untuk melakukan kewajiban hukum.[117] Jika informasi pribadi secara umum saja pada dasarnya dilarang, bisa dikatakan bahwa pemrosesan informasi pribadi sensitif sangatlah dilarang. Meski begitu, terdapat kondisi-kondisi tertentu yang masih memperbolehkan data sensitif diproses dengan ketentuan:[118]

---

[113] Ghio Ong dan Helen Flores, "Canister Scandal: 90-day suspensions of 2 docs, nurse ends" *Philstar Global*, 6 September 2008, https://www.philstar.com/nation/2008/09/06/398622/canister-scandal-90-day-suspension-2-docs-nurse-ends diakses pada 30 November 2020.
[114] OutRight Action, "Philippines: Will Hospital Be Held Accountable for Violating Gay Man?", *OutRight Action*, 6 Mei 2008, https://outrightinternational.org/content/philippines-will-hospital-be-held-accountable-violating-gay-man diakses pada 30 November 2020
[115] *Ibid*.
[116] Bagian 12 *Data Privacy Act of 2012*.
[117] *Ibid*.
[118] Bagian 13 *Data Privacy Act of 2012*.

1. Subjek data telah memberikan persetujuannya, khusus untuk tujuan diadakannya pemrosesan, atau dalam hal informasi khusus, semua pihak dalam pertukaran telah memberikan persetujuan mereka sebelum data diproses;

2. Pemrosesan yang sama diatur oleh hukum dan regulasi yang ada:

    a. Regulasi yang diberlakukan menjamin pelindungan informasi pribadi sensitif dan informasi khusus.

    b. Persetujuan subjek data tidak diwajibkan oleh peraturan perundang-undangan yang mengizinkan pemrosesan informasi pribadi sensitif atau informasi khusus.

3. Pemrosesan diperlukan untuk melindungi kehidupan dan kesehatan subjek data atau orang lain, dan subjek data secara hukum atau fisik tidak dapat mengungkapkannya persetujuannya sebelum pemrosesan data;

4. Pemrosesan diperlukan untuk mencapai tujuan yang sah dan non-komersial dari sebuah organisasi publik dan asosiasinya:

    a. Pemrosesan hanya terbatas dan terkait dengan anggota organisasi *bonafide* atau asosiasinya;

    b. Informasi pribadi sensitif tidak ditransfer kepada pihak ketiga.

    c. Persetujuan subjek data diperoleh sebelum data diproses;

5. Pengolahan diperlukan untuk tujuan pengobatan medis, dilakukan oleh praktisi medis atau institusi perawatan medis, dan dipastikan tingkat perlindungan informasi pribadinya memadai; atau

6. Pemrosesan menyangkut informasi pribadi yang diperlukan untuk perlindungan hak dan kepentingan orang perseorangan atau badan hukum di pengadilan, atau pembentukan, pelaksanaan atau pembelaan pendapat hukum, atau ketika diberikan kepada pemerintah atau otoritas publik.

Dengan mengacu pada ketentuan tersebut, maka data kesehatan tetap dapat diproses sepanjang memenuhi kualifikasi pada huruf a-f tersebut.

C. Tiongkok

Pada 2012, *Standing Committee of the National People's Congress* mengeluarkan Keputusan tentang Penguatan Pelindungan Informasi Internet, yang memuat beberapa prinsip umum untuk penyedia jasa jaringan dalam rangka melindungi informasi pribadi elektronik warga negara Tiongkok.[119] Berdasarkan prinsip-prinsip tersebut, berbagai departemen di bawah *State Council* mengeluarkan regulasi-regulasi administratif yang mengatur pengumpulan dan pemrosesan informasi pribadi dalam bidang masing-masing.[120] Misalnya, Kementerian Industri dan Teknologi Informasi (MIIT) mengeluarkan Ketentuan tentang Pelindungan Informasi Pribadi Pengguna Telekomunikasi dan Internet pada tahun 2013, *State Post Bureau* mengeluarkan Ketentuan tentang Manajemen Keamanan Informasi Pribadi Pengguna Layanan Pengiriman dan Pengantaran pada tahun 2014, dan *People's Bank of China* mengeluarkan *Implementing Measures* untuk Pelindungan Hak dan Kepentingan Konsumen Keuangan pada tahun 2016.[121]

Selanjutnya pada 7 November 2016, *Cybersecurity Law* disahkan dan mulai berlaku pada 1 Juni 2017.[122] Implementasi resmi dari *Cybersecurity Law* menandakan adanya peningkatan kerangka hukum baru di Tiongkok mengenai keamanan siber dana pelindungan data.[123] Undang-undang tersebut menjadi salah satu undang-undang rujukan dalam pelindungan data pribadi karena salah satu substansinya adalah mengatur pelindungan informasi pribadi.[124] Selebihnya, rezim hukum Tiongkok mengenai privasi dan pelindungan data tersebar dalam berbagai peraturan perundang-undangan, diantaranya adalah *The Measures for the Management of Population Health Information (on Trial), Law on Licensed Doctors of the PRC, Nurses Ordinance, Regulations for Medical Institutions on Medical Records Management, The Interim Administrative Measures for the Management of Human Genetic Resources, The Pharmaceutical Data Management Specification (Draft for Comments), The Guidelines for Technical Review of Network Security Registration for Medical Devices, The Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation),* dan *The Measures for the Management of Scientific Data*.[125] Berikut merupakan substansi beberapa peraturan perundang-undangan di atas:

---

[119] Alan Charles Raul (Ed), *The Privacy, Data Protection and Cybersecurity Law Review Sixth Edition*, Law Business Research Ltd, London, 2019, h. 115.
[120] *Ibid*.
[121] *Ibid*.
[122] *Ibid*.
[123] *Ibid*.
[124] Lihat: Rogier Creemers, dkk., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)", *New America*, 29 Juni 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ diakses pada 4 Januari 2021.
[125] Lihat: Hongquan (Samuel) Yang, *Op.Cit*., h. 117 dan Carol B. Sun dan Jenny Z.N. Sun, "Health Care Data Compliance in China: FAQ", *The National Law Review*, 11 Juni 2019, https://www.natlawreview.com/article/health-care-data-compliance-china-faq diakses pada 4 Januari 2021.

1. *The Measures for the Management of Population Health Information (on Trial)*

   Pasal 10 *Measures for the Administration of Population Health Information* menyatakan bahwa unit yang bertanggung jawab seharusnya tidak mengumpulkan informasi mengenai populasi.

2. *Law on Licensed Doctors of the PRC*[126]

   Pasal 23 jo. Pasal 37 *Law on Licensed Doctors of the PRC* menyatakan bahwa dokter tidak diperkenankan menyembunyikan, memalsukan, atau menghancurkan file medis atau data yang relevan. Jika diketahui demikian, maka dokter yang bersangkutan diberikan peringatan pendisiplinan atau diperintahkan untuk dihentikan praktiknya tidak kurang dari 6 (enam) bulan tetapi tidak lebih dari 1 (satu) tahun oleh pemerintah. Bahkan, jika situasinya serius akan ada pencabutan izin praktik. Adapun, jika perbuatan yang dilakukan oleh dokter yang bersangkutan merupakan kejahatan, maka akan ada pemeriksaan untuk pertanggungjawaban pidana.

3. *Regulations for Medical Institutions on Medical Records Management*[127]

   Peraturan ini memuat ketentuan bagi institusi dan staf medis untuk melindungi informasi pribadi pasien. Selain itu, *Regulations for Medical Institutions on Medical Records Management* mempersyaratkan bahwa, 'institusi dan staf medis harus dengan tegas melindungi privasi pasien'. Adanya kebocoran rekaman medis pasien untuk tujuan non-medis, non-pengajaran, atau non-penelitian adalah dilarang.[128] Regulasi tersebut juga menyediakan penyimpanan, penyelamatan, peminjaman, dan penggandaan rekaman medis.[129] Adapun, dalam peraturan ini yang dimaksud dengan rekam medis adalah sejumlah teks, simbol, grafis, gambar, dan slide yang diproduksi dari aktivitas medis oleh personil medis, termasuk rekaman pasien rawat luar (darurat) dan rawat inap medis. Rekaman medis adalah bagian dari riwayat kesehatan.[130] Lebih jauh lagi, terdapat kewajiban institusi medis untuk membentuk dan meningkatkan sistem pengelolaan rekam medis, mengatur departemen manajemen rekam medis, atau menentukan staf profesional khusus untuk bertanggung jawab terhadap manajemen rekam medis.[131] Selanjutnya, institusi medis juga

[126] Lihat: Law on Licensed Doctors of the PRC, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/11/content_1383574.htm diakses pada 4 Januari 2021.
[127] Lihat: Regulation on Medical Records Management in Medical Institutions, http://english.www.gov.cn/policies/latest_releases/2014/08/23/content_281474983027052.htm diakses pada 8 Januari 2020.
[128] Pasal 6 *Regulations for Medical Institutions on Medical Records Management*.
[129] Pasal 16 *Regulations for Medical Institutions on Medical Records Management*.
[130] Pasal 2 *Regulations for Medical Institutions on Medical Records Management*.
[131] Pasal 5 *Regulations for Medical Institutions on Medical Records Management*.

harus mengadakan inspeksi kualitas rekam medis secara rutin, sistem evaluasi dan masukan. Departemen medis pada institusi medis harus bertanggung jawab mengenai kualitas manajemen dari rekam medis.[132]

D. Inggris

Pada 1998, Inggris telah memiliki *Data Protection Act* yang di dalamnya telah mengkategorikan kesehatan atau kondisi fisik atau mental sebagai data pribadi sensitif. Perkembangannya, Inggris mengikuti ketentuan-ketentuan dalam GDPR dalam pelindungan data pribadi. GDPR pada dasarnya merupakan produk legislasi Uni Eropa, akan tetap memiliki arti penting bagi Inggris meskipun telah terjadi Brexit. Sampai saat ini (2020), Inggris masih menggunakan *Data Protection Act 2018* yang merupakan implementasi dari GDPR. Dalam GDPR, terdapat perlindungan hukum yang lebih kuat untuk data sensitif, yang diantaranya adalah data genetika, biometrik, kesehatan, dan kehidupan atau orientasi seksual. Pembahasan detail mengenai konsepsi pelindungan data kesehatan dalam GDPR telah dibahas dalam bagian GDPR. Pada bagian kali ini, akan lebih memfokuskan bahasan pada bagaimana pelindungan privasi secara khusus di Inggris.

Dalam dunia kesehatan, *Health and Social Care Act of 2012*[133] merupakan satu instrumen penting yang mengatur mengenai banyak hal yang terkait dengan kesehatan. Bahkan, undang-undang ini juga sudah disesuaikan dengan keberadaan undang-undangan pelindungan data. Meskipun, undang-undang yang dirujuk adalah *Data Protection Act 1998* belum *Data Protection Act 2018*. *Health and Social Care Act of 2012* memaknai pemrosesan data sebagaimana yang ada dalam *Data Protection Act 1998*, yakni memperoleh, merekam, atau menahan informasi atau data atau melakukan prngoperasian terhadap data atau informasi, termasuk:

1. Mengatur, menyesuaikan, atau mengubah informasi atau data;

2. Memulihkan, mengkonsultasikan, atau menggunakan informasi atau data;

3. Membuka informasi atau data melalui transmisi, diseminasi, atau menjadikannya tersedia; atau

4. Menjajarkan, mengombinasikan, memblokir, menghapus atau merusak informasi atau data.

[132] *Ibid*.
[133] Lihat: Health and Social Care Act 2012, https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted diakses pada

Selanjutnya, pada 2018 lahir *Health and Social Care (National Data Guardian) Act 2018*[134]. Undang-undang ini tidak mencabut keberadaan *Health and Social Care Act of 2012*, melainkan menambahkan adanya ketentuan mengenai *National Data Guardian* (NDG) dan tujuan-tujuan yang berkaitan. Masih senada dengan *Health and Social Care Act of 2012*, *Health and Social Care (National Data Guardian) Act 2018* juga memaknai pemrosesan data sebagaimana apa yang ada dalam *Data Protection Act 1998*. Selanjutnya, terdapat ketentuan mengenai pengertian "data kesehatan dan perawatan sosial orang dewasa", yakni informasi (bagaimanapun direkam):[135]

1. Berkaitan dengan:

    a. kesehatan fisik atau mental atau kondisi dari seseorang, diagnosis kondisinya atau perawatannya atau pengobatannya;

    b. perawatan sosial orang dewasa disediakan untuk seorang individu (atau sebuah penilaian untuk perawatan yang demikian);

    c. dukungan pengasuh dewasa disediakan untuk seorang individu (atau sebuah penilaian untuk dukungan yang demikian),

    apakah identitas individu dapat dipastikan atau tidak, atau

2. Sejauh mana pun diperoleh, secara langsung atau tidak langsung, dari informasi tersebut.

Lebih jauh, *Health and Social Care (National Data Guardian) Act 2018* mengatur mengenai keorganisasian dan tata kelola NDG. Salah satunya disebutkan bahwa NDG dapat menerbitkan pedoman tentang pemrosesan data kesehatan dan perawatan sosial orang dewasa di Inggris.[136] NDG pada dasarnya merupakan lembaga independen yang didukung oleh *Department of Health and Social Care*, yang merepresentasikan kepentingan pasien dan masyarakat.[137] NDG juga memiliki tanggungjawab menjaga Prinsip Caldicott.[138] Prinsip Caldicott, pertama kali dikenalkan pada 1997, merupakan kumpulan dari pedoman praktik-praktik baik yang diterapkan secara luas dalam bidang

---

[134] Lihat: Health and Social Care (National Data Guardian) Act 2018, https://www.legislation.gov.uk/ukpga/2018/31/pdfs/ukpga_20180031_en.pdf diakses pada 8 Januari 2021.
[135] Pasal 2 ayat (6) *Health and Social Care (National Data Guardian) Act 2018*.
[136] Pasal 1 ayat (2) *Health and Social Care (National Data Guardian) Act 2018*.
[137] National Data Guardian, "About Us", *National Data Guardian*, https://www.gov.uk/government/organisations/national-data-guardian/about diakses pada 8 Januari 2020.
[138] *Ibid*.

tata kelola informasi kesehatan dan kepedulian sosial untuk memastikan bahwa data masyarakat disimpan dengan baik dan digunakan dengan tepat.[139]

Selain NDG, terdapat pula *UK Caldicott Guardian Council* (UKCGC) yang merupakan sub-kelompok dari NDG.[140] Keberadaan UKCGC adalah wajib bagi seluruh organisasi dan otoritas lokal yang menyediakan pelayanan sosial.[141] UKCGC sendiri adalah sebuah badan nasional untuk *Caldicott Guardians* yang bertanggung jawab untuk melindungi kerahasiaan informasi kesehatan dan perawatan masyarakat serta memastikan data tersebut digunakan dengan tepat.[142]

Selain itu, Inggris juga memiliki beberapa peraturan perundang-undangan yang secara detail mengatur terkait dengan kesehatan dan yang dalamnya mengandung ketentuan mengenai pengumpulan dan pemrosesan data, diantaranya:

1. *The Health Service (Control of Patient Information) Regulations 2002*[143]

   Segala pemberitahuan yang berkaitan dengan yang diatur dalam regulasi ini harus dalam bentuk tertulis atau ditransmisikan dengan alat elektronik dalam bentuk yang dapat dibaca dan digunakan untuk referensi selanjutnya.

2. *The Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010*[144]

   Dalam peraturan ini, "informasi dilindungi yang dibuka" berarti informasi yang termasuk dalam bagian 31 (2) *Human Fertilisation and Embryology Act 2008*, yakni:

   a. ketentuan untuk setiap individu yang dapat diidentifikasi dari layanan perawatan selain layanan perawatan pasangan dasar (*basic partner treatment services*);

---

[139] *Ibid*.
[140] *Ibid*.
[141] *Ibid*.
[142] *Ibid*.
[143] Lihat: The Health Service (Control of Patient Information) Regulations 2002 https://www.legislation.gov.uk/uksi/2002/1438/contents/made diakses pada 6 Januari 2021.
[144] Lihat: The Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010, https://www.legislation.gov.uk/uksi/2010/995/made#f00008 diakses pada 6 Januari 2021.

b. pengadaan atau distribusi sperma apapun, selain sperma yang merupakan sperma sumbangan pasangan dan belum disimpan, dalam rangka memberikan layanan kesuburan non-medis untuk individu yang dapat diidentifikasi;

c. penyimpanan gamet individu yang dapat diidentifikasi atau embrio yang diambil dari perempuan yang dapat diidentifikasi;

d. penggunaan gamet dari setiap individu yang dapat diidentifikasi selain penggunaannya untuk tujuan layanan perawatan pasangan dasar (*basic partner treatment services*);

e. penggunaan embrio yang diambil dari wanita yang dapat diidentifikasi; atau

f. jika hal itu menunjukkan bahwa individu yang dapat diidentifikasi adalah individu yang yang bersangkutan.

Informasi a-f di atas tersebut belum dapat dikatakan sebagai "informasi dilindungi yang dibuka", melainkan harus juga dimasukkan oleh *Human Fertilisation and Embryology Authority* pada pendaftaran selama periode 1 Agustus 1991 sampai 30 September 2009 (kedua tanggal inklusif).[145] Adapun, berikut merupakan informasi-informasi yang dikecualikan dari pemaknaan di atas:

a. Mengidentifikasi atau berkaitan dengan individu yang menyumbangkan gamet (sel sperma atau sel telur) selain untuk tujuan penelitian;

b. Mengidentifikasi atau berhubungan dengan individu (atau orang yang dirawat dengan individu tersebut) yang telah menerima layanan pengobatan dengan gamet yang disumbangkan;

    1) Untuk tujuan ini, informasi dikecualikan jika[146]:

        a) berkenaan dengan individu yang bersangkutan telah mencapai usia 16 (enam belas) tahun, kecuali individu yang bersangkutan telah menyetujui pengungkapan informasi oleh *Human Fertilisation and Embryology Authority* untuk tujuan penelitian sesuai dengan peraturan yang dibuat berdasarkan

[145] Pasal 2 ayat (2) *The Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010*.
[146] Pasal 2 ayat (4) *The Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010*.

bagian 33D *Human Fertilisation and Embryology Act 1990* (pengungkapan untuk tujuan penelitian medis atau lainnya);

b) sehubungan dengan individu yang bersangkutan yang telah memberikan pemberitahuan tertulis kepada *Human Fertilisation and Embryology Authority* bahwa mereka tidak menyetujui pengungkapan untuk tujuan penelitian oleh *Human Fertilisation and Embryology Authority* mengenai informasi tentang mereka yang diberikan pada saat memberikan pemberitahuan bahwa individu yang relevan kompeten untuk memberikan;

c) berkaitan dengan individu yang bersangkutan dimana seseorang yang memiliki tanggung jawab sebagai orang tua untuk individu yang bersangkutan telah memberikan pemberitahuan tertulis kepada *Human Fertilisation and Embryology Authority* bahwa mereka tidak menyetujui pengungkapan untuk tujuan penelitian oleh *Human Fertilisation and Embryology Authority* mengenai informasi tentang individu yang bersangkutan;

d) berkenaan dengan individu yang bersangkutan dimana pada saat layanan perawatan atau layanan kesuburan non-medis diberikan kepada orang-orang yang menjadi orang tua dari individu yang bersangkutan, orang-orang yang disebutkan secara tertulis bahwa informasi yang berkaitan dengan setiap anak yang dilahirkan sebagai akibat dari layanan perawatan tersebut tidak dapat diungkapkan oleh *Human Fertilisation and Embryology Authority* untuk tujuan penelitian sesuai dengan peraturan yang dibuat berdasarkan bagian 33D *Human Fertilisation and Embryology Act 1990* (pengungkapan untuk tujuan penelitian medis atau lainnya);

e) mengidentifikasi atau berhubungan dengan individu yang telah menyumbangkan (baik sendiri atau dengan individu) embrio selain untuk tujuan penelitian saja; atau

f) mengidentifikasi atau berhubungan dengan individu yang telah menyumbangkan gamet selain untuk tujuan penelitian saja.

2) Mengidentifikasi atau berhubungan dengan individu yang telah menyumbangkan (baik sendiri atau dengan orang lain) embrio selain untuk tujuan penelitian;

3) Mengidentifikasi atau berhubungan dengan individu (atau orang yang dirawat dengan individu tersebut) yang telah menerima layanan pengobatan dengan embrio yang disumbangkan;

4) Mengidentifikasi atau berhubungan dengan individu yang dikandung sebagai hasil dari konsepsi terbantu menggunakan gamet yang disumbangkan atau embrio yang disumbangkan; atau

5) sehubungan dengan:

   a) individu yang menolak memberikan persetujuan pengungkapan untuk tujuan penelitian;

   b) seorang individu yang belum mencapai usia 16 (enam belas) tahun, di mana orang tua atau orang lain yang memiliki tanggung jawab sebagai orang tua anak tersebut menyatakan secara tertulis bahwa informasi yang berkaitan dengan anak tersebut tidak dapat diungkapkan untuk tujuan penelitian; atau

   c) seorang individu yang belum mencapai usia 16 (enam belas) tahun, dimana pada saat layanan pengobatan atau layanan kesuburan non-medis sedang diberikan kepada orang-orang yang menjadi orang tua dari anak tersebut, orang-orang tersebut menunjukkan secara tertulis bahwa informasi terkait kepada setiap anak yang lahir sebagai hasil dari layanan perawatan tersebut tidak dapat diungkapkan untuk tujuan penelitian.

Berdasarkan ketentuan tersebut informasi-informasi yang termasuk dalam poin a-f di atas adalah informasi yang tidak termasuk dalam "informasi dilindungi yang dibuka". Berkaca dari berbagai ketentuan yang diatur dalam *The Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010* di atas, dapat dilihat adanya prinsip kerahasiaan (*confidentiality*). Bahkan, nampak juga adanya penghargaan terhadap hak untuk menolak bagi subjek data, sebagaimana dapat diketahui melalui berbagai pengecualian di atas.

Selanjutnya, saat *Human Fertilisation and Embryology Authority* memberikan otorisasi, *Human Fertilisation and Embryology Authority* harus mengungkapkan informasi dilindungi yang dapat diungkapkan yang diminta oleh pemohon kepada lembaga penelitian dalam jangka waktu 90 (sembilan puluh) hari dimulai dengan tanggal pembayaran biaya

diterima.[147] Dimana informasi dilindungi yang dapat diungkapkan tersebut, diungkapkan sesuai dengan *The Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010*.[148] Adapun, segala sesuatu yang dilakukan oleh *Human Fertilisation and Embryology Authority* dalam mengungkapkan atau memproses informasi tersebut harus dianggap dilakukan secara sah meskipun terdapat kewajiban kerahasiaan yang dimiliki oleh otoritas berkenaan dengan itu.[149] Selain itu, *Human Fertilisation and Embryology Authority* dapat memberikan otorisasi kepada lembaga penelitian untuk memproses informasi dilindungi yang dapat diungkapkan sesuai dengan peraturan ini.[150]

3. *The Abortion Regulations 1991*[151]

Pemberitahuan yang diberikan atau informasi apa pun yang diberikan kepada Kepala Petugas Medis sesuai dengan *The Abortion Regulations 1991* tidak boleh diungkapkan kecuali pengungkapan tersebut dapat dilakukan dengan tujuan tertentu diantaranya untuk tujuan melakukan tugasnya, tujuan penelitian *bona fide*, dan ketika diminta oleh *President of the General Medical Council* untuk tujuan investigasi apakah telah terjadi kesalahan profesional yang serius oleh seorang praktisi, kepada *President of the General Medical Council* atau anggota stafnya yang diberi wewenang olehnya.

E. Belgia

Peraturan pelindungan data pribadi di Belgia tersebar dalam berbagai peraturan perundang-undangan, diantaranya *Act of 28 November 2000 on Cybercrime*, *Act of 3 December 2017 on the establishment of the Data Protection Authority*, GDPR, dan *Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data* (*Data Protection Act*, yang menggantikan *Belgian Data Protection Act of 8 December 1992*, yang diberlakukan sejak 5 September 2018).[152] *Data Protection Act* menyangkut implementasi lebih lanjut dari GDPR dan *EU Directive 2016/680* mengenai implementasi ketentuan-ketentuan GDPR terkait definisi, pembatasan, dan persyaratan tambahan lebih lanjut; dan tentang pemrosesan data oleh otoritas yang kompeten untuk tujuan pencegahan, investigasi, deteksi, atau penuntutan tindak pidana.[153]

---

[147] Pasal 14 *Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010*.
[148] *Ibid*.
[149] *Ibid*.
[150] Pasal 3 *Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010*.
[151] Lihat: The Abortion Regulations 2021, https://www.legislation.gov.uk/uksi/1991/499/contents/made diakses pada 6 Januari 2021.
[152] Alan Charles Raul (Ed), *Op.Cit*., h. 79.
[153] *Ibid*.

Mengenai pemrosesan data genetik, biometrik, dan kesehatan, atau data yang berkaitan dengan hukuman dan pelanggaran kriminal, legislator Belgia telah mengatur langkah-langkah yang harus dilakukan, seperti memelihara daftar orang yang berhak untuk mengkonsultasikan data, bersama dengan uraian fungsinya, terkait dengan pengolahan data tersebut, yang terikat oleh kewajiban hukum atau kontrak kerahasiaan.[154] Pengontrol atau pemroses data harus membuat daftar orang-orang tersebut untuk *Data Protection Authority* berdasarkan permintaan.[155] Meskipun kewajiban tersebut bukan bagian dari GDPR, kewajiban tersebut sebelumnya telah ada dalam *Belgian Data Protection Act of 8 December 1992* dan peraturan pelaksananya.[156] Secara khusus, Belgia juga memiliki *Patient Rights Act of 22 August 2002* yang memerintahkan, antara lain, penggunaan data pasien dan informasi yang perlu diterima pasien.[157]

Melalui *Patient Rights Act of 22 August 2002*, setidaknya terdapat 3 (tiga) pasal yang berkaitan dengan perlindungan privasi pasien, yakni Pasal 10, Pasal 15, dan Pasal 18. Bahkan, dinyatakan secara eksplisit bahwa "Pasien berhak atas perlindungan privasinya dalam setiap intervensi/campur tangan dari praktisi kesehatan, khususnya, berkaitan dengan informasi kesehatannya".[158] Dalam rangka menjaga privasi, tunduk pada izin pasien, hanya orang yang keberadaannya dibenarkan dalam lingkup penyediaan layanan praktisi perawatan kesehatan yang dapat hadir selama perawatan, pemeriksaan, dan pengobatan.[159] Informasi yang berkaitan dengan kesehatan pasien tidak boleh dikomunikasikan kepada orang ketiga, misalnya untuk tujuan mengambil polis asuransi jiwa), kecuali dalam kasus pengurangan hukum dan jika ini penting untuk melindungi kesehatan masyarakat atau hak dan kebebasan orang lain, misalnya risiko infeksi.[160] Disebutkan juga bahwa interferensi oleh praktisi kesehatan diperbolehkan berkenaan dengan pelaksanaan hak atas perlindungan privasi, hanya selama diatur oleh undang-undang dan sejauh itu penting untuk melindungi kesehatan masyarakat atau hak dan kebebasan orang lain.[161] Ketentuan-ketentuan tersebut mencerminkan adanya penghargaan terhadap hak atas privasi dan pelindungan data kesehatan pasien.

Melalui undang-undang yang lahir pada 2002 ini, terdapat pula revisi atas *Law of 8 December 1992* tentang perlindungan privasi dalam kaitannya dengan pemrosesan data pribadi yang telah diamandemen melalui *Law of 11 December 1998*. Revisi yang ada dalam *Patient Rights Act of 22 August 2002* menyebutkan bahwa setiap orang memiliki hak, baik langsung atau dengan didampingi praktisi kesehatan, untuk memperoleh informasi mengenai data pribadi yang diproses

---

[154] *Ibid*., h. 82.
[155] *Ibid*.
[156] *Ibid*.
[157] *Ibid*., h. 86.
[158] Pasal 10 *Patient Rights Act of 22 August 2002*.
[159] *Ibid*.
[160] The Federal Commission on Patients' Rights, *An Invitation to Dialogue Law on Patients' Rights*, Federal Public Service Public Health, Food Chain and Environment, Brussels, 2007, h. 9.
[161] *Ibid*.

terkait dengan kesehatannya. Ketentuan ini sejalan dengan adanya hak atas informasi yang ada dalam hukum pelindungan data pribadi. Secara sederhana, hak atas informasi adalah hak subjek data untuk menerima informasi/diberitahukan terkait bagaimana data pribadinya diolah.

Selain itu, terdapat ketentuan mengenai keluarga terdekat dari pasien meninggal yang ingin mengakses catatan kesehatan pasien tersebut. Diatur bahwa jika pasien tidak keberatan selama hidupnya, maka suami/istri, pasangan, orang tua, anak-anak, saudara laki-laki dan perempuan, kakek-nenek dan cucu yang dapat menyebutkan alasan yang sah, misalnya kecurigaan kesalahan medis atau melacak riwayat keluarga, dapat menunjuk praktisi kesehatan, misalnya dokter umum keluarga yang membaca catatan kesehatan almarhum, termasuk catatan pribadi.[162] Selanjutnya, untuk melindungi privasi pasien, pembacaan tidak langsung dan terbatas hanya pada data yang secara langsung terkait dengan alasan yang diminta oleh kerabat terdekat.[163]

Dalam tataran instansi, Belgia juga telah mendirikan *Information Security Committee* yang kompeten untuk mengontrol secara preventif mengenai apakah komunikasi data pribadi dalam pemerintah telah mentaati prinsip-prinsip dasar GDPR.[164] Dalam hal ini, salah satu yang menjadi objek kontrol adalah data kesehatan.[165]

F. Kanada

Hukum privasi di Kanada diatur melalui konstitusi, undang-undang, dan hukum kebiasaan.[166] Kanada memiliki *Personal Information Protection and Electronic Documents Act* 2000 (PIPEDA)[167] sebagai legislasi utama yang mengatur mengenai pelindungan data pribadi. Dalam PIPEDA, informasi kesehatan pribadi diartikan sebagai:[168]

1. Informasi terkait kesehatan fisik atau mental seseorang;

2. Informasi terkait pelayanan kesehatan apapun yang disediakan untuk seseorang;

---

[162] *Ibid*., h. 8.
[163] *Ibid*., h. 8.
[164] Alan Charles Raul (Ed), *Op.Cit*., h. 82.
[165] *Ibid*.
[166] *Ibid*., h. 99.
[167] Lihat: Personal Information Protection and Electronic Documents Act, https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html diakses pada 8 Januari 2021.
[168] Pasal 2 *Personal Information Protection and Electronic Documents Act 2000*.

3. Informasi mengenai sumbangan oleh individu dari setiap bagian tubuh atau setiap unsur tubuh dari individu atau informasi yang diperoleh dari pengujian atau pemeriksaan bagian tubuh atau unsur tubuh individu;

4. Informasi yang dikumpulkan dalam rangka memberikan layanan kesehatan kepada individu; atau

5. Informasi yang dikumpulkan sekali-kali/tidak dengan sengaja kepada penyedia layanan untuk kesehatan individu.

Di sektor kesehatan, kegiatan inti rumah sakit umum atau fasilitas perawatan jangka panjang yang didanai publik tidak tunduk pada PIPEDA.[169] Namun, penyedia layanan kesehatan dalam praktik swasta seperti dokter, dokter gigi, dan ahli tulang terlibat dalam aktivitas komersial dan karenanya tunduk pada PIPEDA, kecuali peraturan provinsi yang pada secara substansi serupa juga berlaku.[170]

Provinsi Alberta, Provinsi New Brunswick,[171] Provinsi Newfoundland,[172] Provinsi Nova Scotia,[173] Saskatchewan, Provinsi Manitoba, dan Provinsi Ontario[174] telah memberlakukan undang-undang informasi kesehatan pribadi yang berlaku untuk sektor perawatan kesehatan, termasuk rumah sakit.[175] Provinsi Quebec juga memiliki undang-undang tentang layanan kesehatan dan layanan sosial yang memuat ketentuan penting terkait informasi kesehatan pribadi.[176] Selanjutnya, Provinisi British Columbia memiliki beberapa undang-undang yang mengatur privasi informasi kesehatan.[177] Wilayah Barat Laut, Provinisi Prince Edward Island dan Provinsi Yukon telah mengadopsi undang-undang informasi kesehatan pribadi yang belum diberlakukan.[178]

---

[169] Office of the Privacy Commissioner of Canada, "The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals", *Office of the Privacy Commissioner of Canada*, 2015, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/ diakses pada 4 Januari 2021
[170] *Ibid*.
[171] Lihat: Personal Health Information Custodians in New Brunswick Exemption Order, https://laws-lois.justice.gc.ca/PDF/SOR-2011-265.pdf diakses pada 8 Januari 2020.
[172] Lihat: Personal Health Information Custodians in Newfoundland and Labrador Exemption Order, https://laws-lois.justice.gc.ca/PDF/SI-2012-72.pdf diakses pada 8 Januari 2020.
[173] Lihat: Personal Health Information Custodians in Nova Scotia Exemption Order, https://laws-lois.justice.gc.ca/PDF/SOR-2016-62.pdf diakses pada 8 Januari 2020.
[174] Lihat: Health Information Custodians in the Province of Ontario Exemption Order, https://laws-lois.justice.gc.ca/PDF/SOR-2005-399.pdf diakses pada 8 Januari 2020.
[175] Office of the Privacy Commissioner of Canada, *Op.Cit*.
[176] *Ibid*.
[177] *Ibid*.
[178] *Ibid*.

G. Amerika Serikat

Health Insurance Portability and Accountability Act of 1996 (HIPAA) merupakan legislasi utama di Amerika Serikat yang mengatur mengenai privasi dan pelindungan data pribadi dalam tata kelola data kesehatan. HIPAA memberikan pasien hak atas informasi kesehatannya, termasuk hak untuk memeriksa dan mendapatkan salinan dari informasi kesehatan mereka, meminta koreksi, dan mengetahui siapa yang melihat.[179] Pada 2003, *Health and Human Services* (HHS) mengeluarkan *HIPAA Privacy Rules*. Peraturan tersebut memberikan hak-hak individu dengan penghormatan kepada pelindungan informasi kesehatan mereka.[180] Tercermin bahwa di dalam *HIPAA Privacy Rules* telah menggunakan istilah "pelindungan informasi kesehatan" bukan terbatas pada "rekam medis". Hal tersebut mengindikasikan bahwa ruang lingkup data yang dimaksud dan dilindungi lebih luas. Bukan hanya rekam medis yang ada pada fasyankes, tetapi juga data kesehatan yang ada di luar fasyankes. *HIPAA Privacy Rule* menetapkan standar nasional untuk melindungi rekam medis seseorang dan informasi pribadi kesehatan lainnya. *HIPAA Privacy Rules* berlaku untuk perencana kesehatan, *clearinghouse* kesehatan, dan penyedia kesehatan yang melakukan transaksi kesehatan tertentu secara elektronik.

Dalam *HIPAA Privacy Rules,* terdapat persyaratan pengamanan yang tepat untuk melindungi privasi informasi kesehatan pribadi dan mengatur batasan-batasan serta kondisi-kondisi pada penggunaan dan pembukaan yang mungkin membuat informasi demikian tanpa otorisasi pasien.[181] Secara umum, informasi kesehatan seseorang tidak bisa digunakan untuk tujuan yang tidak secara langsung berkaitan dengan perawatan orang tersebut tanpa adanya izin.[182]

---

[179] Lihat: HHS, "The HIPAA Privacy Rule", *HHS*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html dan HHS, "Your Health Information Privacy Rights", *HHS*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf diakses pada 22 Maret 2021

[180]

[181] HHS, "The HIPAA Privacy Rule", *HHS*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html diakses pada 22 Maret 2021.

[182] HHS, "Your Health Information Privacy Rights", *HHS*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf diakses pada 22 Maret 2021.

Perkembangannya, terdapat *Electronic Health Records* (EHRs) yang menjadikan penyedia layanan dapat menggunakan informasi secara lebih efektif dalam rangka meningkatkan kualitas dan efisiensi perawatan, tetapi EHRs tidak akan mengubah pelindungan privasi atau pengamanan keamanan yang diterapkan pada informasi kesehatan.[183] Hukum yang telah mengatur pelindungan informasi data diterapkan juga pada informasi dalam EHRs. EHRs sendiri merupakan versi elektronik dari bagan kertas yang ada pada dokter atau kantor penyedia perawatan kesehatan lainnya. Adapun, EHRs dapat memuat riwayat medis, catatan medis, dan informasi lainnya tentang kesehatan termasuk gejala, diagnosis, pengobatan, hasil lab, tanda vital, imunisasi, dan laporan dari tes diagnosis seperti x-ray. Informasi di EHRs dapat dibagikan dengan organisasi lain yang terlibat dalam perawatan jika sistem komputer diatur untuk berinteraksi satu dengan lainnya. Informasi pada rekaman tersebut harus hanya dibagi untuk tujuan yang diperbolehkan oleh hukum dan subjek data.

HIPAA sendiri mengharuskan dokter, rumah sakit, dan penyedia kesehatan lainnya untuk memberitahu subjek data jika terjadi "kebocoran data". HIPAA juga mengharuskan penyedia kesehatan untuk memberitahukan Sekretaris HHS. Jika sebuah kebocoran berpengaruh pada lebih dari 500 penduduk dari sebuah negara atau yurisdiksi, penyedia kesehatan juga harus memberitahukan outlet media terkemuka di negara atau yurisdiksi. Keharusan ini membantu pasien mengetahui jika suatu hal telah berjalan dengan salah terkait dengan pelindungan informasi dan membantu menjaga penyedia kesehatan bertanggung jawab atas pelindungan EHRs.[184]

---

[183] HHS, "Privacy, Security, and Electronic Health Records", *HHS*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf diakses pada 22 Maret 2021.

[184] *Ibid*.

VI. PEMETAAN KEBIJAKAN DAN AKTOR PELINDUNGAN DATA PRIBADI DALAM SEKTOR KESEHATAN

A. Tata Kelola Data Kesehatan Secara Umum

Dalam sub-bab ini kita akan melihat mengenai regulasi mengatur mengenai tata kelola data kesehatan secara umum sekaligus mengidentifikasi aktor beserta kewenangan masing-masing. Setidaknya kami menemukan 12 regulasi dan kebijakan yang mengatur mengenai tata kelola data kesehatan di Indonesia. Secara lebih khusus, regulator mengeluarkan 12 kebijakan yang mengatur mengenai tata kelola data kesehatan terkait penyakit menular. Berikut adalah ringkasan singkat dari tiap-tiap aturan dalam memaknai privasi, perlindungan data kesehatan.

1. Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran

   Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran (UU 29/2004) secara umum mengatur mengenai standar praktik kedokteran termasuk standar pelayanan kepada pasien, prosedur administratif yang harus ditempuh untuk berpraktik, hak dan kewajiban dokter, hingga pengawasan dan sanksi bagi para dokter. Melalui undang-undang ini ditegaskan bahwa setiap kinerja kedokteran mengakui adanya privasi terkait rekam medis pasien yang dikelolanya. Hal ini tertuang dalam Pasal 47 ayat (2) dan Pasal 48 ayat (1) yang menyebutkan bahwa:[185]

   > Rekam medis harus disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan, sebagai salah satu hak dari pasien yang harus dilindungi. Kewajiban dokter untuk merahasiakan rekam kesehatan pasien dilakukan seumur hidup bahkan setelah pasien itu meninggal dunia.

   Dalam Pasal 47 ayat (1) disebutkan bahwa dokumen rekam medis merupakan milik dokter, dokter gigi, atau sarana pelayanan kesehatan, sedangkan isi rekam medis merupakan milik pasien. Hal ini dituangkan kembali dalam Pasal 52 huruf (e) yang menyebutkan bahwa:

   > Isi rekam medis tersebut merupakan bagian dari hak pasien untuk diketahui secara pribadi. Mengenai arti rekam medis, dinyatakan bahwa rekam medis

[185] Pasal 51 huruf c UU 29/2004.

> adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien.

Pembatasan terhadap hak privasi atau kerahasiaan data pasien dalam undang-undang ini diatur dalam Pasal 48 ayat (2) yang menyebutkan sejumlah syarat atau kondisi yang membuat hak atas kerahasiaan rekam kesehatan pasien dapat dikecualikan. Kondisi yang dimaksud adalah jika untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum, permintaan pasien sendiri atau berdasarkan ketentuan perundang-undangan.

Berkaitan dengan mekanisme akuntabilitas, berdasarkan Pasal 64 disebutkan bahwa Majelis Kehormatan Disiplin Kedokteran Indonesia dapat menerima pengaduan, serta memeriksa dan memutuskan kasus pelanggaran dokter. Termasuk kasus kebocoran data pasien. Mekanisme pengaduan tersebut diatur dalam Pasal 67-70 UU 29/2004. Dalam Pasal 79 huruf (c) ditegaskan adanya ancaman pidana paling lama 1 tahun dan denda lima puluh juta rupiah (Rp 50.000.000, bagi yang tidak menjalankan kewajiban menjaga rahasia kesehatan pasien.

2. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (UU 36/2009) merupakan salah satu dasar hukum yang menjadi koridor praktik dunia medis di Indonesia, termasuk referensi dalam pengaturan privasi dan pelindungan pribadi. Dalam konsiderannya, undang-undang ini dimaksudkan untuk memelihara dan meningkatkan derajat kesehatan masyarakat berdasarkan prinsip non diskriminatif dan partisipatif.

Prinsip privasi dan pelindungan data pribadi dalam UU 36/2009 menggunakan istilah rahasia, sebagaimana dituangkan dalam Pasal 57. Dalam Pasal 57 ayat (1) tertulis:

> Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.

Meskipun demikian, dalam ayat (2) disebutkan bahwa hak atas rahasia kondisi kesehatan pribadi yang dimaksud dapat dikecualikan atau tidak berlaku dalam hal: (1)

perintah undang-undang; (2) perintah pengadilan; (3) izin yang bersangkutan; (4) kepentingan masyarakat; atau (5) kepentingan orang tersebut.[186]

Adapun yang dimaksud dengan penyelenggara kesehatan adalah seluruh pihak yang melakukan upaya pelayanan kesehatan baik promotif, preventif, kuratif maupun rehabilitatif.[187] Dalam Pasal 34 ayat (2) disebutkan bahwa penyelenggara fasilitas pelayanan kesehatan dilarang mempekerjakan tenaga medis yang tidak memiliki kualifikasi dan izin melakukan pekerjaan profesi.

Jika mengacu pada UU 36/2009 tersebut, istilah privasi dan pelindungan data pribadi diartikan sebagai kerahasiaan dalam dunia medis. Model perlindungannya ditekankan dalam Pasal 57 secara umum dan perlu diturunkan dalam langkah implementatif yang menyangkut pada kode etik dari tenaga kesehatan. Khususnya mengacu pada Pasal 55 yang menyebutkan bahwa Pemerintah wajib menetapkan standar mutu pelayanan kesehatan[188] yang seyogyanya termasuk internal dari seluruh penyelenggara kesehatan dalam pemrosesan dan pengelolaan data pribadi kesehatan pasien.

Berkaitan dengan Pasal 57 ayat (2) diatur mengenai pengecualian dalam pelindungan hak atas rahasia kondisi kesehatan memenuhi salah satu syarat, mulai dari perintah undang-undang, perintah pengadilan, izin yang bersangkutan, kepentingan masyarakat, atau kepentingan orang tersebut. Meskipun demikian belum dituangkan lebih spesifik baik di dalam penjelasan mengenai tolak ukur, uji konsekuensi, dan model penyajian pengungkapan data kondisi kesehatan pribadi pasien yang bersangkutan.

Dalam hal mekanisme pemulihan, dalam Pasal 58 disebutkan bahwa setiap orang berhak menuntut ganti rugi terhadap seorang tenaga kesehatan dan/atau penyelenggara kesehatan yang menimbulkan kerugian akibat kesalahan atau kelalaian dalam pelayanan kesehatan yang diterimanya.[189] Dalam Penjelasan Pasal disebutkan ketentuan kerugian yang tertulis dalam Pasal 58 juga termasuk pembocoran rahasia kedokteran.

---

[186] Pasal 57 ayat (1) dan (2) UU 36/2009.
[187] Definisi penyelenggara kesehatan tidak ditemukan secara langsung dalam ketentuan umum. Meskipun demikian, dapat diartikan sebagai pihak-pihak yang menyelenggarakan fasilitas pelayanan kesehatan.
[188] Pasal 55 UU 36/2009.
[189] Pasal 58 UU 36/2009.

3. Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit

Rumah sakit merupakan institusi penting yang menunjang pelayanan kesehatan masyarakat. Dalam konsideran disebutkan Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit (UU 44/2009) menyatakan bahwa undang-undang ini ditujukan untuk peningkatan mutu dan jangkauan pelayanan rumah sakit serta pengaturan hak dan kewajiban masyarakat dalam memperoleh pelayanan kesehatan. Berkaitan dengan data pribadi pasien, ruang lingkup data pasien adalah pelaksanaan kegiatan rekam medis yang dilakukan oleh rumah sakit. Dalam Pasal 29 ayat (1) huruf (h), (l), (m) UU 44/2009 menegaskan kewajiban rumah sakit untuk menyelenggarakan rekam medis, memberikan informasi yang benar, jelas dan jujur mengenai hak dan kewajiban pasien, dan melindungi serta menghormati hak-hak pasien.

Secara spesifik hak atas privasi dituangkan sebagai hak pasien yang ditegaskan dalam Pasal 32 huruf (i) yang menyebutkan bahwa:

> Salah satu hak pasien adalah mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya.

Dalam Pasal 44 juga menegaskan bahwa rumah sakit memiliki wewenang untuk menolak pengungkapan segala informasi kepada publik berkaitan dengan rahasia kedokteran.

Dengan demikian, rumah sakit memiliki kewajiban untuk melakukan mekanisme pelindungan terhadap data-data rekam medis pasiennya. Dalam Pasal 38 mengatur mengenai kewajiban Rumah Sakit untuk menyimpan rahasia kedokteran. Tetapi, rahasia kedokteran dapat dibuka untuk kepentingan kesehatan pasien, untuk pemenuhan permintaan aparat penegak hukum dalam rangka penegakan hukum, atas persetujuan pasien sendiri atau berdasarkan ketentuan peraturan perundang-undangan.

4. Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan

Secara umum Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan (UU 36/2014) ditujukan untuk meningkatkan kualitas pelayanan kesehatan khususnya yang harus dilakukan tenaga kesehatan yang bertanggung jawab dan memiliki etik dan moral tinggi, keahlian dan kewenangan yang harus ditingkatkan secara terus menerus. Adapun, yang dimaksud dengan tenaga kesehatan adalah:

> Setiap orang yang mengabdikan diri dalam bidang kesehatan serta memiliki pengetahuan dan/atau keterampilan melalui pendidikan di bidang kesehatan yang untuk jenis tertentu memerlukan kewenangan untuk melakukan upaya kesehatan.

Salah satu tanggung jawab dari tenaga medis adalah menjaga data pribadi kesehatan seseorang, mengingat dalam kerja-kerjanya tenaga kesehatan akan mengelola data kesehatan termasuk rekam medis. Hal ini dituangkan dalam Pasal 58 huruf (c) yang menegaskan bahwa:

> Salah satu kewajiban dari tenaga kesehatan dalam menjalankan praktik adalah menjaga kerahasiaan kesehatan penerima pelayanan kesehatan atau pasien.

Tenaga kesehatan dalam pelayanannya wajib membuat rekam medis, termasuk melengkapi setelah penerima pelayanan kesehatan selesai menerima pelayanan tersebut. Adapun metode dalam penulisan rekam medis adalah dengan membubuhi nama, waktu, dan tanda tangan atau paraf tenaga kesehatan yang memberikan layanan. Rekam medis tersebut kemudian harus disimpan dan dijaga kerahasiaannya oleh tenaga kesehatan dan fasilitas pelayanan kesehatan.[190] Hal ini ditegaskan Kembali dalam Pasal 73 yang menyebutkan bahwa:

> Dalam pelayanan kesehatan, setiap tenaga kesehatan wajib menyimpan rahasia kesehatan penerima pelayanan kesehatan.

Meskipun demikian, dalam Pasal 73 ayat (2) disebutkan bahwa rahasia kesehatan dapat dibuka ke publik dalam kondisi tertentu dengan tujuan dan kepentingan terbatas yakni kepentingan kesehatan penerima pelayanan kesehatan, pemenuhan permintaan aparatur penegak hukum bagi kepentingan penegakan hukum, permintaan penerima pelayanan kesehatan sendiri, atau pemenuhan ketentuan peraturan perundang-undangan.

Adapun terkait dengan mekanisme perlindungannya, undang-undang ini secara tegas mengatur sanksi jika terjadi pelanggaran dalam menjalankan seluruh kewajiban tenaga kesehatan termasuk kegagalan menjaga kerahasiaan rekam medis.[191] Pelaku akan diberikan sanksi administratif berupa teguran lisan, peringatan tertulis, denda

[190] Pasal 70 ayat (1), (2), (3), dan (4) UU 36/2014.
[191] Pasal 82 ayat (1) UU 36/2014.

administratif dan/atau pencabutan izin[192] oleh pemerintah, pemerintah daerah provinsi, dan pemerintah daerah kota/kabupaten sesuai dengan kewenangannya.

5. Undang-Undang Nomor 38 Tahun 2014 tentang Keperawatan

   Berdasarkan Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan (UU 36/2014), klien[193] memiliki hak untuk memperoleh keterjagaan kerahasiaan kondisi kesehatannya.[194] Pengungkapan kerahasiaan tersebut dapat dilakukan, namun terbatas atas dasar: [195]

   a. kepentingan kesehatan klien;
   b. pemenuhan permintaan aparatur penegak hukum dalam rangka penegakan hukum;
   c. persetujuan Klien sendiri;
   d. kepentingan pendidikan dan penelitian; dan
   e. ketentuan peraturan perundang-undangan.

   Keberadaan poin ke-lima pada dasarnya cukup menjadi pintu pembuka bagi kemungkinan-kemungkinan lain diungkapkannya rahasia kesehatan. Oleh karena, akan hal ini sebenarnya dibutuhkan adanya kepastian hukum yang lebih tepat, agar rahasia kesehatan klien tidak dengan mudah dibuka. Undang-undang ini juga menyebutkan bahwa rahasia kesehatan klien akan diatur lebih lanjut dalam Peraturan Menteri Kesehatan. Jika melihat peraturan perundang-undangan yang ada saat ini, maka satu-satunya peraturan yang ditemukan adalah Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran.

6. Peraturan Pemerintah Nomor 46 Tahun 2014 tentang Sistem Informasi Kesehatan
   Peraturan Pemerintah Nomor 46 Tahun 2014 tentang Sistem Informasi Kesehatan (PP 46/2014) dibentuk sebagai aturan pelaksana dari Pasal 168 UU 36/2009 yang menyebutkan bahwa penyelenggaraan upaya kesehatan yang efektif dan efisien diperlukan informasi kesehatan melalui sistem informasi dan melalui lintas sektor. Secara umum, PP 46/2014 ini merupakan bentuk pengamanan sistem informasi kesehatan dengan objek pengaturannya termasuk pula data dan informasi kesehatan.

---

[192] Pasal 82 ayat (4) U 36/2014.
[193] Klien merupakan perseorangan, keluarga, kelompok, atau masyarakat yang menggunakan jasa pelayanan keperawatan. Lihat: Pasal 1 angka 14 UU 38/2014.
[194] Lihat: Pasal 38 UU huruf e UU 38/2014.
[195] Pasal 39 ayat (1) UU 38/2014.

Menurut ketentuan regulasi ini yang dimaksud dengan data kesehatan adalah angka dan kejadian berupa keterangan dan tanda-tanda yang secara relatif belum bermakna bagi pembangunan kesehatan.[196] Sedangkan informasi kesehatan adalah data kesehatan yang telah diolah atau diproses menjadi bentuk yang mengandung nilai dan makna yang berguna untuk meningkatkan pengetahuan dalam mendukung pembangunan kesehatan.[197] Adapun pengumpulan data dan informasi kesehatan dilaksanakan melalui penyelenggaraan rekam medik, termasuk rekam medik elektronik dan nonelektronik[198] yang bersumber dari fasilitas pelayanan kesehatan.[199]

Secara khusus, dalam PP 46/2014 ini disebutkan pengaturannya dilaksanakan sesuai dengan ketentuan peraturan perundang-perundangan. Dalam pelaksanaannya, setiap fasilitas pelayanan kesehatan harus mengoperasikan sendiri sistem elektronik rekam medik yang tidak terintegrasi dengan sistem elektronik rekam medik fasilitas pelayanan kesehatan lain, tetapi harus mampu interkonektivitas dengan Sistem Elektronik Kesehatan dan sistem elektronik lainnya.[200] Data dan informasi kesehatan dapat bersifat terbuka dan tertutup sesuai dengan ketentuan peraturan perundang-undangan.

Regulasi ini menggunakan istilah pemilik data dan informasi kesehatan untuk mendefinisikan pengelola sistem informasi kesehatan baik di tingkat nasional, provinsi, kabupaten/kota, maupun fasilitas pelayanan kesehatan.[201] Dalam hal penyimpanan data dan informasi kesehatan, pemilik data dapat dilakukan dengan menggunakan jasa dan fasilitas milik pihak lain dalam negeri dengan tidak melepaskan tanggung jawab atas kerahasiaan informasi.[202] Pengamanan informasi kesehatan dilakukan untuk menjamin agar tetap terjaga keutuhan dan kesediaannya (integrity dan availability), termasuk menjaga kerahasiaan informasi kesehatan yang bersifat tertutup.

Dalam sistem informasi kesehatan, keamanan dan kerahasiaan informasi merupakan salah satu prinsip yang harus dijaga dan tujuan yang ingin dicapai dalam penyelenggaraan sistem informasi kesehatan.[203] Tujuan itu dicapai dengan sejumlah mekanisme internal, termasuk pengaturan mengenai hak akses. Dalam PP ini disebutkan pula bahwa keamanan dan kerahasiaan informasi kesehatan juga dilakukan

[196] Pasal 1 ayat (2) PP 46/2014.
[197] Pasal 1 ayat (3) PP 46/2014.
[198] Pasal 17 huruf b PP 46/2014.
[199] Pasal 14 PP 46/2014.
[200] Pasal 49 PP 46/2014.
[201] Penjelasan Pasal 22 PP 46/2014.
[202] Pasal 22 PP 46/2014.
[203] Pasal 23 PP 46/2014

dengan menetapkan kriteria dan batasan hak akses pengguna informasi kesehatan yang dibentuk oleh Menteri.[204]

Sementara Pasal 63 mengatur mengenai larangan penyebarluasan data dan informasi kepada publik yakni berupa: (1) salinan kartu pengguna fasilitas pelayanan kesehatan atau bukti identitas lain; (2) riwayat kesehatan; (3) tagihan dan bukti pembayaran biaya penggunaan fasilitas pelayanan kesehatan; (4) hasil pemeriksaan diagnostik; dan (5) data dan informasi terkait kegiatan penelitian. Berkaitan dengan subjek penelitian, data dan informasi hasil penelitian yang secara etika atau hasil kesepakatan dengan subjek penelitian bersifat rahasia atau dirahasiakan.[205]

Setiap pengelola sistem informasi kesehatan yang melakukan manipulasi data dan informasi kesehatan dan membuka data dan informasi yang bersifat tertutup atau rahasia tanpa izin dikenai sanksi sesuai dengan ketentuan peraturan perundang-undangan.[206]

7. Peraturan Presiden Nomor 72 Tahun 2012 tentang Sistem Kesehatan Nasional
Peraturan Presiden Nomor 72 Tahun 2012 tentang Sistem Kesehatan Nasional (Perpres 72/2012) mendefinisikan Sistem Kesehatan Nasional (SKN) sebagai:

> Pengelolaan kesehatan yang diselenggarakan oleh semua komponen bangsa Indonesia secara terpadu dan saling mendukung guna menjamin tercapainya derajat kesehatan masyarakat yang setinggi-tingginya.

Sistem Kesehatan Nasional ini dilaksanakan secara berkelanjutan, sistematis, terarah, terpadu, menyeluruh, dan tanggap terhadap perubahan dengan menjaga kemajuan, kesatuan, dan ketahanan nasional.[207] Pada dasarnya, peraturan ini sama sekali tidak menyinggung terkait bagaimana tata kelola pelindungan data pribadi. Di dalamnya, lebih banyak diatur mengenai pelaksanaan SKN, khususnya oleh pusat dan daerah.

9. Peraturan Menteri Kesehatan Nomor 269/MENKES/PER/III/2008 tentang Rekam Medis

Mengacu pada ketentuan Peraturan Menteri Kesehatan Nomor 269/MENKES/PER/III/2008 tentang Rekam Medis (Permenkes 269/2008) rekam

[204] Pasal 24 ayat (1) PP 46/2014.
[205] Pasal 63 ayat (1) PP 46/2014.
[206] Pasal 29 PP 46/2014.
[207] Pasal 4 ayat (2) Perpres 72/2012.

medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien.[208]

Isi rekam medis untuk pasien rawat jalan pada sarana pelayanan kesehatan, pasien rawat inap dan perawatan satu hari, dan pasien gawat darurat, terdapat paling tidak beberapa data berikut yang direkam: [209]

a. Identitas pasien;
b. Hasil anamnesis, mencakup sekurang-kurangnya keluhan dan riwayat penyakit;
c. Hasil pemeriksaan fisik dan penunjang medik;
d. Diagnosis; dan
e. Pengobatan dan/atau tindakan.

Permenkes 269/2008 juga secara khusus mengatur mengenai penyimpanan, pemusnahan, dan kerahasiaan rekam medis. Mengenai penyimpanan, rekam medis pasien rawat inap di rumah sakit wajib disimpan oleh petugas yang ditunjuk oleh pimpinan sarana pelayanan kesehatan sekurang-kurangnya untuk jangka waktu 5 (lima) tahun terhitung dari tanggal terakhir pasien berobat atau dipulangkan.[210] Setelah batas waktu 5 (lima) tahun dilampaui, rekam medis dapat dimusnahkan, kecuali ringkasan pulang dan persetujuan tindakan medik.[211] Adapun, rekam medis pada sarana pelayanan kesehatan non rumah sakit wajib disimpan sekurang-kurangnya untuk jangka waktu 2 (dua) tahun terhitung dari tanggal terakhir pasien berobat.[212] Setelah batas waktu dilampaui, rekam medis dapat dimusnahkan.[213] Ketentuan penyimpanan sebagaimana disebutkan, pada dasarnya mencerminkan adanya prinsip pembatasan penyimpanan (*storage limitation*) dalam pelindungan data pribadi.

Lebih dari itu, terdapat keharusan bagi dokter, dokter gigi, tenaga kesehatan tertentu, petugas pengelola dan pimpinan sarana pelayanan kesehatan untuk menjaga kerahasiaan informasi tentang identitas, diagnosis, riwayat penyakit, riwayat

[208] Pasal 1 angka 1 Permenkes 269/2008.
[209] Pasal 3 ayat (1), (2), dan (3) Permenkes 269/2008.
[210] Pasal 8 ayat (1) dan (4) Permenkes 269/2008.
[211] Pasal 8 ayat (2) Permenkes 269/2008.
[212] Pasal 9 ayat (1) Permenkes 269/2008.
[213] Pasal 9 ayat (2) Permenkes 269/2008.

pemeriksaan dan riwayat pengobatan pasien.[214] Adapun, informasi-informasi tersebut dapat dibuka dalam hal: [215]

a. Untuk kepentingan kesehatan pasien;
b. Memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum atas perintah pengadilan;
c. Permintaan dan/atau persetujuan pasien sendiri;
d. Permintaan institusi/lembaga berdasarkan ketentuan peraturan perundang-undangan; dan
e. Untuk kepentingan penelitian, pendidikan, dan audit medis, sepanjang tidak menyebutkan identitas pasien.
f. Mengenai permintaan pembukaan rekam medis tersebut, harus dilakukan secara tertulis kepada pimpinan sarana pelayanan kesehatan.[216]

Pada dasarnya, pemanfaatan rekam medis dapat dipakai untuk beberapa kepentingan, salah satunya adalah untuk keperluan pendidikan dan penelitian. Untuk keperluan pendidikan dan penelitian yang menyebutkan identitas pasien, harus mendapat persetujuan secara tertulis dari pasien atau ahli warisnya dan harus dijaga kerahasiaannya.

Namun demikian, sangat disayangkan Permenkes 269/2008 bisa dikatakan telah tidak relevan. Hal ini mengingat kerangka berpikir yang digunakan adalah rekam medis dalam bentuk konvensional, bukan elektronik. Sedangkan, saat ini telah sangat masif adanya praktik rekam medis dalam bentuk elektronik. Terlebih lagi, saat ini konsep yang dikenal tidak hanya rekam medis, melainkan juga rekam kesehatan. Rekam kesehatan ini misalnya, ketika terdapat seseorang yang mencatat kondisi kesehatannya secara sendiri, baik tindakan maupun penggunaan alatnya, yang bisa saja diserahkan juga pada fasilitas pelayanan kesehatan. Konsep rekam kesehatan ini yang belum dijangkau oleh peraturan perundang-undangan yang ada saat ini. Alasan-alasan inilah yang mendasari ketidak relevansian Permenkes 269/2008 dengan perkembangan yang ada.

10. Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran
Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran (Permenkes 36/2012) merupakan aturan implementatif dari UU 29/2004 yang memuat mengenai rahasia kedokteran. Peraturan ini secara umum mengatur lebih terperinci

[214] Pasal 10 ayat (1) Permenkes 269/2008.
[215] Pasal 10 ayat (2) Permenkes 269/2008.
[216] Pasal 10 ayat (3) Permenkes 269/2008.

mengenai cakupan rahasia kedokteran, penyimpanan dan pembukaan data yang dikelola oleh dokter, hingga pengawasannya.

Mengacu pada Permenkes 36/2012, rahasia kedokteran merupakan data dan informasi tentang kesehatan seseorang yang diperoleh tenaga kesehatan pada waktu menjalankan pekerjaan atau profesinya.[217]

Rahasia kedokteran mencakup data dan informasi mengenai: (1) identitas pasien; (2) kesehatan pasien meliputi hasil anamnesis, pemeriksaan fisik, pemeriksaan penunjang, penegakan diagnosis, pengobatan dan/atau tindakan kedokteran; dan (3) hal lain yang berkenaan dengan pasien.[218] Rahasia kedokteran ini wajib disimpan oleh semua pihak yang terlibat dalam pelayanan kedokteran dan/atau menggunakan data dan informasi tentang pasien, walaupun pasien telah meninggal dunia.[219]

Dalam konteks ini masih terdapat ruang untuk dibukanya rahasia kedokteran secara terbatas sesuai kebutuhan untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum[220] dalam rangka penegakan hukum, permintaan pasien sendiri[221], atau berdasarkan ketentuan peraturan perundang-undangan[222] oleh penanggung jawab pelayanan pasien.[223]

Meskipun demikian, penanggung jawab pelayanan pasien atau pimpinan fasilitas pelayanan kesehatan dapat menolak membuka rahasia kedokteran apabila permintaan tersebut bertentangan dengan ketentuan peraturan perundang-undangan.[224] Pasien atau keluarga terdekat pasien yang telah meninggal dunia yang menuntut tenaga kesehatan dan/atau fasilitas pelayanan kesehatan serta menginformasikannya melalui media massa, dianggap telah melepaskan hak rahasia kedokterannya kepada umum.[225] Penginformasian melalui media massa memberikan kewenangan kepada tenaga kesehatan dan/atau fasilitas pelayanan kesehatan untuk membuka atau mengungkap rahasia kedokteran yang bersangkutan sebagai hak jawab.[226] Dalam hal pihak pasien

[217] Pasal 1 angka 1 Permenkes 36/2012.
[218] Pasal 3 ayat (1) Permenkes 36/2012.
[219] Pasal 4 ayat (1) dan (3) Permenkes 36/2012.
[220] Pembukaan rahasia kedokteran untuk memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum dapat dilakukan pada proses penyelidikan, penyidikan, penuntutan, dan sidang pengadilan. Lihat: Pasal 7 ayat (1) Permenkes 36/2012.
[221] Pembukaan rahasia kedokteran atas dasar permintaan pasien sendiri dapat dilakukan dengan pemberian data dan informasi kepada pasien baik secara lisan maupun tertulis. Lihat: Pasal 8 ayat (1) Permenkes 36/2012.
[222] Pembukaan rahasia kedokteran berdasarkan ketentuan peraturan perundang-undangan dilakukan tanpa persetujuan pasien dalam rangka kepentingan penegakan etik atau disiplin, serta kepentingan umum. Lihat: Pasal 9 ayat (1) Permenkes 36/2012.
[223] Lihat: Pasal 5 ayat (1) dan (2) Pasal 10 Permenkes 36/2012.
[224] Pasal 11 Permenkes 36/2012.
[225] Pasal 13 ayat (1) Permenkes 36/2012.
[226] Pasal 13 ayat (2) Permenkes 36/2012.

menggugat tenaga kesehatan dan/atau fasilitas pelayanan kesehatan maka tenaga kesehatan dan/atau fasilitas pelayanan kesehatan yang digugat berhak membuka rahasia kedokteran dalam rangka pembelaannya di dalam sidang pengadilan.[227] Ketentuan mengenai penolakan dan penuntutan oleh pihak pasien ini pada dasarnya sama dengan apa yang diatur dalam UU 44/2009.

11. Peraturan Menteri Kesehatan Nomor 69 Tahun 2014 tentang Kewajiban Rumah Sakit dan Kewajiban Pasien
    Dalam Peraturan Menteri Kesehatan Nomor 69 Tahun 2014 tentang Kewajiban Rumah Sakit dan Kewajiban Pasien (Permenkes 69/2014) hanya terdapat Pasal 24 yang mengatur mengenai pelindungan data pribadi. Pasal 24 ayat (2) Permenkes 69/2014 menyebutkan hak-hak pasien, dimana diantaranya:

    a. Mendapatkan perlindungan atas rahasia kedokteran termasuk kerahasiaan rekam medik; dan
    b. Mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya.

12. Peraturan Menteri Kesehatan Nomor 75 Tahun 2014 tentang Pusat Kesehatan Masyarakat
    Menurut Peraturan Menteri Kesehatan Nomor 75 Tahun 2014 tentang Pusat Kesehatan Masyarakat (Permenkes 75/2014) Pusat Kesehatan Masyarakat (Puskesmas) sebagai salah satu fasilitas kesehatan tentu juga melaksanakan pencatatan rekam medis, termasuk melaksanakan pencatatan, pelaporan,dan evaluasi terhadap mutu dan akses pelayanan kesehatan.[228] Dalam Pasal 17 disebutkan bahwa:

    > Tenaga kesehatan di Puskesmas harus bekerja sesuai dengan standar profesi, standar pelayanan, standar prosedur operasional, etika profesi, menghormati hak pasien, serta mengutamakan kepentingan dan keselamatan pasien dengan memperhatikan keselamatan dan kesehatan dirinya dalam bekerja. Pasal ini dapat diartikan sebagai hak pasien untuk dilindungi privasi terkait dengan kerahasiaan rekam medis dan data-data kesehatan lainnya.

    Dalam pengelolaannya, setiap puskesmas wajib melakukan kegiatan sistem informasi puskesmas baik secara elektronik atau nonelektronik. Adapun sistem informasi mencakup: (1) pencatatan dan pelaporan kegiatan Puskesmas dan jaringannya; (2)

[227] Pasal 14 Permenkes 36/2012.
[228] Pasal 7 huruf f dan g Permenkes 75/2014.

survey lapangan; (3) laporan lintas sektor terkait; dan (4) laporan jejaring fasilitas pelayanan kesehatan di wilayah kerjanya.[229]

Sistem tersebut merupakan bagian dari sistem informasi kesehatan kabupaten/kota. Laporan kegiatan Puskesmas kemudian diolah menjadi sumber data kesehatan prioritas yang akan diselenggarakan melalui komunikasi data.[230] Berkaitan dengan kewenangan Puskesmas, Pasal 23 ayat (2) menyebutkan bahwa Puskesmas kawasan pedesaan dalam pelayanannya dapat melibatkan partisipasi masyarakat.

13. Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan
    Peraturan Menteri Kesehatan Nomor 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan (Permenkes 20/2019) mendefinisikan *telemedicine* sebagai pemberian pelayanan kesehatan jarak jauh oleh profesional kesehatan dengan menggunakan teknologi informasi dan komunikasi untuk kepentingan peningkatan kesehatan individu dan masyarakat.[231]

    Pelayanan kesehatan ini meliputi pertukaran informasi diagnosis, pengobatan, pencegahan penyakit dan cedera, penelitian dan evaluasi, dan pendidikan berkelanjutan penyedia layanan kesehatan.[232] Dalam rangka pelayanan *telemedicine*, fasilitas pelayanan kesehatan pemberi konsultasi dan peminta konsultasi memiliki kewajiban untuk menjaga kerahasiaan data pasien.[233]

B. Tata Kelola Data Kesehatan Penyakit Tertentu

Beberapa peraturan perundang-undangan dalam konteks tata kelola data kesehatan mengenai penyakit tertentu yang dapat dimaknai mengatur pentingnya pelindungan data, sebagai berikut:

1. Peraturan Menteri Kesehatan Nomor 21 Tahun 2013 tentang Penanggulangan HIV dan AIDS.
   Secara khusus kementerian kesehatan membentuk kebijakan guna menyinergikan penanggulangan HIV dan AIDS di Indonesia melalui penetapan Peraturan Menteri Kesehatan Nomor 21 Tahun 2013 tentang Penanggulangan HIV dan AIDS (Permenkes 21/2013). Dalam Permenkes ditegaskan bahwa pemeriksaan diagnosis HIV dilakukan berdasarkan prinsip konfidensialitas, persetujuan, konseling, pencatatan, pelaporan

[229] Pasal 43 Permenkes 75/2014.
[230] Pasal 44 Permenkes 75/2014.
[231] Lihat: Pasal 1 angka 1 Permenkes 20/2019.
[232] *Ibid*.
[233] Lihat: Pasal 17 ayat (2) dan Pasal 18 ayat (2) Permenkes 20/2019.

dan rujukan. Adapun prinsip konfidensialitas juga berarti hasil pemeriksaannya harus dirahasiakan dan dapat dibuka secara terbatas kepada pihak yang bersangkutan, tenaga kesehatan yang menangani, keluarga terdekat dalam hal yang bersangkutan tidak cakap, pasangan seksual, dan pihak lain sesuai dengan ketentuan peraturan perundangan.[234]

Dalam proses pengobatan dan perawatan, orang yang terinfeksi HIV wajib mendapatkan konseling pasca pemeriksaan diagnosis HIV yang kemudian diregistrasi secara nasional untuk mendapatkan pengobatan. Registrasi tersebut meliputi pencatatan yang memuat nomor kode fasilitas pelayanan kesehatan, nomor urut ditemukan di fasilitas pelayanan kesehatan dan stadium klinis saat pertama kali ditegakkan diagnosisnya. Registrasi tersebut harus dijaga kerahasiaannya.

Salah satu poin penting dalam penanggulangan HIV/AIDS yang dituliskan dalam peraturan ini adalah penyelenggaraan sistem pencatatan, pelaporan dan evaluasi dengan memanfaatkan sistem informasi. Semua kegiatan penanggulangan HIV dan AIDS harus dilakukan pencatatan dan pelaporan sesuai dengan pedoman. Termasuk pelayanan kesehatan yang melakukan perawatan, tindak lanjut perawatan dan pemberian ARV serta mendokumentasikannya dalam rekam medik.
Dalam penanggulangan HIV/AIDS dimungkinkan dilakukan surveilans sebagai bentuk pemantauan dan pengambilan keputusan dalam penanggulangan HIV/AIDS. Kegiatan surveilans tersebut dilakukan mulai dari pelaporan kasus, sero surveilans sentinel HIV dan sifilis, surveilans IMS, surveilans HIV berbasis layanan Konseling dan Tes HIV, surveilans terpadu biologis dan perilaku, survei cepat perilaku, dan kegiatan pemantauan resistensi ARV. Pelaporan kasus tersebut bertujuan untuk menentukan tingkat epidemi dan mencegah penularan lebih lanjut. Secara khusus dilakukan pemantauan resistensi ARV untuk melihat ambang batas tingkat resistensi obat baik bagi orang yang baru terkena HIV, telah melaksanakan pengobatan dan untuk mengoptimalisasi fungsi program ART dan mencegah resistensi ARV.

2. Peraturan Menteri Kesehatan Nomor 51 Tahun 2013 tentang Pedoman Pencegahan Penularan HIV dari Ibu ke Anak.
   Secara khusus kementerian kesehatan memberikan pedoman pencegahan penularan HIV dari ibu ke anak melalui Peraturan Menteri Kesehatan Nomor 51 Tahun 2013 tentang Pedoman Pencegahan Penularan HIV dari Ibu ke Anak (Permenkes 51/2013). Penetapan regulasi ini tidak terlepas dari adanya kondisi peningkatan kasus HIV dan dapat menjadi ancaman potensial terhadap kesehatan masyarakat di Indonesia yang dapat berdampak luas dan negatif bagi ketahanan bangsa.[235]

[234] Pasal 21 ayat (2) dan (3) Permenkes 21/2013.
[235] Konsideran huruf a Permenkes 51/2013.

Regulasi ini ditujukan agar upaya penanggulangan HIV AIDS akan terintegrasi dengan pelayanan kesehatan ibu dan anak pada fasilitas pelayanan kesehatan. Dalam pedoman ini ditegaskan bahwa faktor kerahasiaan status HIV ibu sangat penting untuk dijaga serta ditunjang untuk memberikan dukungan kepada anak dan keluarganya. Aspek kerahasiaan ini harus dijamin kepada ibu hamil ketika mengikuti proses konseling sebelum dan sesudah tes pada setiap jenjang pelayanan kesehatan.[236]

3. Peraturan Menteri Kesehatan Nomor 45 Tahun 2014 tentang Penyelenggaraan Surveilans Kesehatan.
   Menurut Peraturan Menteri Kesehatan Nomor 45 Tahun 2014 tentang Penyelenggaraan Surveilans Kesehatan (Permenkes 45/2014), surveilans kesehatan merupakan: [237]

   > Kegiatan pengamatan sistematis dan terus-menerus terhadap data dan informasi tentang kejadian penyakit atau masalah kesehatan dan kondisi yang mempengaruhi terjadinya peningkatan dan penularan penyakit atau masalah kesehatan untuk memperoleh dan memberikan informasi guna mengarahkan tindakan pengendalian dan penanggulangan secara efektif dan efisien.

   Penyelenggaraan ini merupakan salah satu prasyarat program kesehatan dan bertujuan untuk memastikan ketersediaan informasi tentang situasi, kecenderungan penyakit, faktor risiko dan faktor yang mempengaruhinya dengan tujuan sebagai bahan pengambilan keputusan.[238]

   Secara khusus, surveilans penyakit HIV/AIDS dapat dilakukan sebagai kategori surveilans penyakit menular.[239] Pelaksanaan surveilans kesehatan dimulai dari pengumpulan data, pengolahan data, analisis data, dan diseminasi sebagai satu kesatuan yang tidak terpisahkan untuk menghasilkan informasi yang objektif sebagai bahan pengambilan keputusan. Bentuk surveilans dapat dilakukan melalui basis indikator dan kejadian. Dalam surveilans berbasis indikator, artinya dilakukan untuk memperoleh gambaran penyakit, faktor risiko dan masalah kesehatan atau yang berdampak terhadap kesehatan menjadi indikator program dengan menggunakan sumber data yang terstruktur. Sedangkan basis kejadian, dilakukan untuk menangkap

[236] Lihat: Lampiran Permenkes 51/2013.
[237] Pasal 1 angka 1 Permenkes 45/2014.
[238] Pasal 2 Permenkes 45/2014.
[239] Pasal 4 Permenkes 45/2014.

dan memberikan informasi secara cepat tentang suatu penyakit, faktor risiko, dan masalah kesehatan dengan menggunakan sumber data selain yang terstruktur.

Proses pengumpulan data dapat dilakukan secara aktif dan dari pasien. Secara aktif misalnya dilakukan dengan cara mendapatkan data secara langsung dari fasilitas pelayanan kesehatan, masyarakat atau sumber data lainnya melalui kegiatan penyelidikan epidemiologi, surveilans aktif puskesmas/rumah sakit, survei khusus dan kegiatan lainnya. Sedangkan secara pasif artinya dilakukan dengan cara menerima data dari fasilitas pelayanan kesehatan, masyarakat atau sumber data lainnya, dalam bentuk rekam medis, buku register pasien, laporan data kesakitan/kematian, laporan kegiatan, laporan masyarakat dan bentuk lainnya.[240]

Pengolahan data dilakukan dengan cara perekaman data, validasi, pengkodean, laih bentuk, pengelompokan berdasarkan tempat, waktu dan orang.[241] Selanjutnya analisis data dilakukan dengan metode epidemiologi deskriptif dan/atau analitik untuk menghasilkan informasi yang sesuai dengan tujuan surveilans yang ditetapkan.[242] Adapun model diseminasi dapat dilakukan dengan cara beragam, mulai dari menyampaikan informasi kepada unit yang membutuhkan untuk dilaksanakan tindak lanjut, disampaikan kepada pengelola program sebagai sumber data/laporan, dan memberikan umpan balik kepada sumber data dalam rangka perbaikan kualitas data.[243]

Dalam pelaksanaannya, penyelenggaraan surveilans kesehatan harus sesuai dengan indikator kinerja surveilans yakni memperhatikan kelengkapan laporan, ketepatan laporan, dan indikator kinerja yang ditetapkan pada masing-masing program. Dalam penyelenggaraan surveilans kesehatan, masyarakat dapat berperan serta guna meningkatkan kualitas data dan informasi, mulai dari penyampaian data, pemberian bantuan sarana, tenaga ahli, dan pendanaan, pengembangan teknologi, serta sumbangan pemikiran dan pertimbangan.[244]

Dalam konteks pengolahan data pribadi khususnya rekam medis, tindakan surveilans merupakan salah satu bentuk pengungkapan (*disclosure)* terhadap data pribadi (rekam medis) dengan tujuan tertentu. Sebagaimana disebutkan bahwa Penyakit HIV/AIDS

[240] Pasal 9 Permenkes 45/2014.
[241] Pasal 10 Permenkes 45/2014.
[242] Pasal 11 Permenkes 45/2014.
[243] Pasal 11 Permenkes 45/2014.
[244] Pasal 22 Permenkes 45/2014.

merupakan salah satu penyakit yang dapat dilakukan surveilans untuk pengembangan kebijakan.

4. Peraturan Menteri Kesehatan Nomor 74 Tahun 2014 tentang Pedoman Pelaksanaan Konseling dan Tes HIV.
   Peraturan Peraturan Menteri Kesehatan Nomor 74 Tahun 2014 tentang Pedoman Pelaksanaan Konseling dan Tes HIV (Permenkes 74/2014) dibentuk untuk melaksanakan salah satu ketentuan dalam Peraturan Menteri Kesehatan mengenai Penanggulangan HIV dan AIDS sehingga membentuk pedoman pelaksanaan konseling dan tes HIV. Secara spesifik peraturan ini menjelaskan bahwa prinsip utama dalam pelaksanaan konsel dan tes HIV adalah aspek kerahasiaan. Aspek kerahasiaan ini bahwan menjadi landasan untuk meyakinkan pasien yang baru menerima hasil laboratorium yang menunjukan reaktif HIV untuk menerima penanggulangan HIV selanjutnya. Misalnya konseling HIV pada Ibu Hamil, jika hasil tes HIV positif maka layanan kesehatan yang harus dilakukan secara tatap muka individual, pertama kali, harus diberikan penjelasan mengenai aspek kerahasiaan status positifnya.[245]
   Aspek kerahasiaan ini juga harus dijelaskan dan ditekankan apabila tenaga kesehatan mendapatkan pasien yang menolak untuk mengetahui hasilnya (tidak ingin atau belum membuka hasilnya), tidak ingin mengungkapkan status HIV, termasuk dalam memberikan edukasi dan konseling mengenai Infeksi Menular Seksual dan untuk memberikan dukungan membuka diri kepada tenaga kesehatan.

   Dalam peraturan kementerian ini ditemukan rekomendasi penjelasan prosedur yang dapat digunakan petugas layanan kesehatan untuk memastikan kepada pasien bahwa konfidensialitasnya terjamin. Misalnya dalam contoh komunikasi di poin (5) disebutkan bahwa: [246]

   > Hasil tes HIV ini bersifat rahasia dan hanya anda (pasien-red) dan tim medis yang akan memberikan perawatan kepada anda yang tahu. Artinya, petugas kami tidak diizinkan untuk memberitahukan hasil tes anda kepada orang lain tanpa seizin anda. Untuk memberitahukannya kepada orang lain sepenuhnya menjadi hak anda.

   Selain itu pula, klausul jaminan kerahasiaan juga ditemukan dalam salah satu bentuk formulir 2 yang memuat *informed consen*' dari klien dalam melakukan tes HIV. Secara garis besar klausul dalam surat persetujuan ini diberikan klien yang hendak melakukan tes HIV/AIDS untuk menjalani pemeriksaan darah dengan ketentuan bahwa hasil tes akan tetap rahasia dan terbuka hanya untuk klien atau pasien yang bersangkutan dan

[245] Lihat: Lampiran Permenkes 74/2014.
[246] *Ibid.*

untuk tim perawatan dan pengobatan. Selanjutnya klausul juga menjelaskan bahwa klien menyetujui pengambilan darah untuk pemeriksaan HIV dan mendiskusikan Kembali hasil tes dan cara-cara untuk meningkatkan kualitas hidup terkait HIV/AIDS.[247]

5. Peraturan Menteri Kesehatan Nomor 82 Tahun 2014 tentang Penanggulangan Penyakit Menular.
   Berdasarkan Peraturan Menteri Kesehatan Nomor 82 Tahun 2014 tentang Penanggulangan Penyakit Menular (Permenkes 82/2014) pejabat kesehatan masyarakat[248] pada satuan kerja pemerintah pusat dan daerah dalam rangka menyelenggarakan program penanggulangan penyakit menular memiliki berbagai tugas. Salah satu tugasnya adalah memperoleh informasi dan data status kesehatan masyarakat dari fasilitas pelayanan kesehatan yang melakukan penanggulangan penyakit menular.[249]

   Selain itu, guna memutus mata rantai penularan dan/atau pengobatan penderita dalam rangka penanganan kasus, pejabat kesehatan masyarakat berhak mengambil dan mengumpulkan data dan informasi kesehatan dari kegiatan penanganan kasus.[250] Tidak hanya pejabat kesehatan masyarakat, terdapat Tim Gerak Cepat yang juga berhak mendapatkan akses untuk memperoleh data dan informasi. Tim Gerak Cepat di tingkat pusat, provinsi, dan kabupaten/kota dibentuk sebagai respon penyelenggaraan penanggulangan penyakit menular. Adapun, tugas dan fungsi tim tersebut adalah:

   a. Melakukan deteksi dini Kejadian Luar Biasa (KLB) atau wabah;
   b. Melakukan respon KLB atau wabah; dan
   c. Melaporkan dan membuat rekomendasi penanggulangan.

   Dalam melaksanakan tugas dan fungsi tersebut, Tim Gerak Cepat berhak mendapatkan akses untuk memperoleh data dan informasi secara cepat dan tepat dari fasilitas pelayanan kesehatan dan masyarakat.[251] Dengan melekatnya fungsi pengumpulan/perolehan dan/atau akses, sayangnya pejabat kesehatan masyarakat dan

---

[247] *Ibid.*
[248] Pejabat kesehatan masyarakat adalah Pegawai Negeri Sipil (PNS) di lingkungan kesehatan yang mempunyai tugas dan wewenang di bidang penanggulangan penyakit menular. Lihat: Pasal 1 angka 3 Permenkes 82/2014.
[249] Lihat: Pasal 29 ayat (1) Permenkes 82/2014.
[250] Lihat: Pasal 19 ayat (3) dan (4) Permenkes 82/2014.
[251] Pasal 24 ayat (3) Permenkes 82/2014.

Tim Gerak Cepat tidak memiliki kewajiban untuk melakukan pelindungan terhadap data yang dikumpulkan.

6. Peraturan Menteri Kesehatan Nomor 15 Tahun 2015 tentang Pelayanan Laboratorium Pemeriksa HIV dan Infeksi Oportunistik.
   Latar belakang dibentuknya Peraturan Menteri Kesehatan Nomor 15 Tahun 2015 tentang Pelayanan Laboratorium Pemeriksa HIV dan Infeksi Oportunistik (Permenkes 15/2015) untuk mengatur tata laksana penanggulangan HIV dan AIDS khususnya dalam pelayanan laboratorium yang berkualitas sebagai jejaring laboratorium HIV.

   Salah satu prinsip dalam layanan laboratorium HIV adalah menjaga privasi atau merahasiakan hasil rekam medis pasien HIV AIDS. Misalnya dalam pelayanan rujukan Konseling dan Tes (KT) HIV yang menggunakan sarana kesehatan di luar rumah sakit. Hasil pemeriksaan laboratorium dikembalikan ke layanan KT HIV unit peminta dalam amplop tertutup dengan menjamin kerahasiaan.[252]

   Prinsip kerahasiaan juga berlaku pada surat permintaan konfirmasi hasil pemeriksaan laboratorium. Secara khusus disebutkan bahwa surat tersebut bersifat rahasia, dan tata kelola seperti memberikan sampel dan tanggal penerimaan juga harus dijelaskan oleh siapa dan diterima oleh pihak siapa.[253] Laporan yang dirahasiakan hasilnya juga merupakan laporan hasil tes individu tujuan diagnosis yang dikirim kembali kepada dokter yang meminta di dalam amplop tertutup.[254]

7. Peraturan Menteri Kesehatan Nomor 67 Tahun 2016 tentang Penanggulangan Tuberkulosis (Permenkes 67/2016).
   Tuberkulosis (TB) adalah penyakit menular yang disebabkan oleh *Mycobacterium tuberculosis*, yang dapat menyerang paru dan organ lainnya.[255] Guna menangani penyakit tersebut, dilakukan segala upaya kesehatan yang mengutamakan aspek promotif dan preventif, tanpa mengabaikan aspek kuratif dan rehabilitatif yang ditujukan untuk melindungi kesehatan masyarakat, menurunkan angka kesakitan, kecacatan atau kematian, memutuskan penularan, mencegah resistensi obat dan mengurangi dampak negatif yang ditimbulkan akibat TB.[256]

---

[252] Peraturan Menteri Kesehatan Nomor 15 Tahun 2015 tentang Pelayanan Laboratorium Pemeriksa HIV dan Infeksi Oportunistik, bab IV, halaman 72
[253] *Ibid*, halaman 74
[254] Ibid, halaman 121
[255] Pasal 1 angka 1 Permenkes 67/2016.
[256] Lihat: Pasal 1 angka 2 Permenkes 67/2016.

Berdasarkan situasi tersebut ditetapkan Peraturan Menteri Kesehatan Nomor 67 Tahun 2016 tentang Penanggulangan Tuberkulosis (Permenkes 67/2016). Regulasi ini mengatur mengenai surveilans tuberkulosis (TB) dan sistem informasi terkait penanggulangan TB. Surveilans TB merupakan pemantauan dan analisis sistematis terus menerus terhadap data dan informasi tentang kejadian penyakit TB atau masalah kesehatan dan kondisi yang mempengaruhinya untuk mengarahkan tindakan penanggulangan yang efektif dan efisien.[257] Dalam penyelenggaraan surveilans TB tersebut, dilakukan pengumpulan data secara aktif (langsung dari masyarakat atau sumber data lainnya) dan pasif (dari fasilitas pelayanan kesehatan) baik secara manual ataupun elektronik.[258]

Mengenai sistem informasi, sistem ini merupakan pengelola data dan informasi dari hasil surveilans, yang selanjutnya digunakan untuk mendukung penyelenggaraan program penanggulangan TB.[259] Sistem ini berangkat dari pencatatan dan pelaporan yang ada di tingkat bawah (klinik dan dokter perorangan) sampai ke Menteri Kesehatan.[260] Adapun, pelaporan yang dilakukan di tingkat bawah dan pelaporan oleh dinas kesehatan provinsi dilakukan setiap 3 (tiga) bulan sekali. Meski begitu, sayangnya belum terdapat pelindungan atas data-data yang dikumpulkan tersebut.

8. Keputusan Menteri Kesehatan Nomor 1479 Tahun 2003 tentang Pedoman Penyelenggaraan Sistem Surveilans Epidemiologi Penyakit Menular dan Penyakit Tidak Menular Terpadu.
   Dalam latar belakang Keputusan Menteri Kesehatan Nomor 1479 Tahun 2003 tentang Pedoman Penyelenggaraan Sistem Surveilans Epidemiologi Penyakit Menular dan Penyakit Tidak Menular Terpadu (Kepmenkes 1479/2003) mengutip WHO yang menjabarkan surveilans sebagai:

   > Proses pengumpulan, pengolahan, analisis dan interpretasi data secara sistematik dan terus menerus serta penyebaran informasi kepada unit yang membutuhkan untuk mengambil tindakan.

   Pengembangan surveilans epidemiologi merupakan bentuk kegiatan analisis secara sistematis dan terus menerus terhadap penyakit atau masalah-masalah kesehatan dan kondisi yang mempengaruhi terjadinya peningkatan dan penularan penyakit, agar dapat melakukan tindakan penanggulangan secara efektif dan efisien melalui proses pengumpulan data, pengolahan dan penyebaran informasi epidemiologi kepada

[257] Pasal 8 ayat (1) Permenkes 67/2016.
[258] Lihat: Pasal 9 ayat Permenkes 67/2016.
[259] Pasal 22 ayat (1) Permenkes 67/2016.
[260] Lihat: Pasal 23 Permenkes 67/2016.

penyelenggara program kesehatan. Penyelidikan Epidemiologi adalah serangkaian kegiatan yang dilakukan untuk mengenal penyebab, sifat-sifat penyebab, sumber dan cara penularan/penyebaran serta faktor yang dapat mempengaruhi timbulnya penyakit atau masalah kesehatan yang dilakukan untuk memastikan adanya Kejadian Luar Biasa (KLB) atau setelah terjadi KLB/Wabah. Kategori KLB diartikan sebagai kejadian kesakitan dan/atau kematian yang bermakna secara epidemiologi pada satu daerah dalam kurun waktu tertentu, dan merupakan keadaan yang dapat menjurus pada terjadinya wabah. Sedangkan definisi wabah adalah kejadian berjangkitnya suatu penyakit menular dalam masyarakat yang jumlah penderitanya meningkat secara nyata melebihi dari pada keadaan yang lazim pada waktu dan daerah tertentu serta dapat menimbulkan malapetaka dan ditetapkan oleh Menteri.[261]

Sistem surveilans epidemiologi merupakan tatanan prosedur penyelenggaraan surveilans epidemiologi yang terintegrasi antara unit-unit penyelenggara surveilans dengan laboratorium, sumber-sumber data, pusat penelitian, pusat kajian dan penyelenggara program kesehatan, meliputi tata hubungan surveilans epidemiologi antar wilayah kabupaten/kota, provinsi dan pemerintah pusat.
Salah satu ruang lingkup sistem surveilans epidemiologi kesehatan adalah penyakit HIV/AIDS sebagai bagian dari surveilans penyakit menular. Setiap sistem penyelenggaran surveilans epidemiologi penyakit memiliki komponen yakni mulai dari: tujuan yang jelas dan dapat diukur, unit surveilans epidemiologi yang terjadi dari kelompok kerja surveilans, konsep surveilans epidemiologi hingga kejelasan sumber dan cara-cara memperoleh, mengolah, analisis, dan mekanisme kerja lainnya, dukungan advokasi, peraturan perundangan dan sarana serta anggaran, pelaksanaan mekanisme kerja, jejaring surveilans epidemiologi di setiap prosesnya, serta indikator kinerja.

Setiap layanan kesehatan baik di tingkat nasional, provinsi, hingga kabupaten/kota memiliki unit penyelenggaraan surveilans, mulai dari badan penelitian, pusat data dan informasi, rumah sakit, laboratorium kesehatan, unit surveilans, dan puskesmas, hingga mitra. Dalam ketentuan ini disebutkan sumber daya manusia meliputi tenaga ahli epidemiologi, tenaga pelaksana surveilans epidemiologi, manajer unit kesehatan, jabatan fungsional epidemiologi, entomologi, sanitarian, statistisi, sumber daya manusia laboratorium, sumber daya manusia lainnya yang terkait.

9. Keputusan Menteri Kesehatan Nomor 451 Tahun 2012 tentang Rumah Sakit Rujukan Bagi Orang Dengan HIV dan AIDS.
   Keputusan Menteri Kesehatan Nomor 451 Tahun 2012 tentang Rumah Sakit Rujukan Bagi Orang Dengan HIV dan AIDS (Kepmenkes 451/2012) berisikan daftar sejumlah

[261] Pasal 1 angka 3 Permenkes 45/2014.

rumah sakit rujukan bagi orang dengan HIV dan AIDS atau bagi ODHA dengan dibebankan sejumlah tugas dan kewenangan. Adapun tugas-tugas dari rumah sakit rujukan ODHA adalah dengan menyusun standar prosedur operasional, ketersediaan obat Antiretroviral, menyiapkan sarana, prasarana, dan fasilitas, menyiapkan tenaga kesehatan, membentuk tim kelompok kerja/pokja khusus HIV dan AIDS, serta melaporkan pelaksanaan bagi ODHA.

Rumah sakit rujukan ODHA juga wajib melakukan pemantauan dan evaluasi terhadap pelayanan kesehatan bagi ODHA. Meskipun tidak secara spesifik mengatur mengenai sejumlah prinsip pelindungan data dan kerahasiaan rekam medis ODHA, tetapi dapat diartikan bahwa setiap rumah sakit yang menjadi rujukan harus memiliki standar prosedur operasional, yang salah satu aspek dan prinsipnya adalah menjaga kerahasiaan rekam medis dan status HIV/AIDS.

10. Surat Edaran Direktur Jenderal Pengendalian Penyakit dan Penyehatan Lingkungan Kementerian Kesehatan Nomor HK.03.03/III/0992/2014 Tahun 2014 tentang Penyelenggaraan Pelayanan Orang dengan HIV-AIDS di Rumah Sakit.
    Surat Edaran Direktur Jenderal Pengendalian Penyakit dan Penyehatan Lingkungan Kementerian Kesehatan Nomor HK.03.03/III/0992/2014 Tahun 2014 tentang Penyelenggaraan Pelayanan Orang dengan HIV-AIDS di Rumah Sakit (SE Dirjen Pengendalian Penyakit dan Penyehatan Lingkungan Kemenkes HK.03.03/III/0992/2014) berisikan bahwa setiap rumah sakit harus memastikan penyelenggaraan pelayanan orang dengan HIV/AIDS di rumah sakit. Sekurang-kurangnya rumah sakit kelas C, wajib mampu mendiagnosis, melakukan pengobatan dan perawatan ODHA sesuai dengan ketentuan dalam sistem rujukan. Termasuk Fasilitas pelayanan kesehatan primer dan rumah sakit kelas D.
    Surat Edaran ini juga menegaskan bahwa rumah sakit tidak diperkenankan menolak dalam memberikan pelayanan kesehatan ODHA. Meskipun tidak secara spesifik menjelaskan mengenai kerahasiaan pasien, tetapi pelaksanaan pengobatan dan perawatan ODHA sesuai dalam sistem rujukan dapat diartikan termasuk jaminan kerahasiaan status dan rekam medis ODHA.

11. Keputusan Menteri Kominfo Nomor 159 Tahun 2020 tentang Upaya Penanganan Corona Virus Disease (COVID-19) Melalui Dukungan Sektor Pos dan Informatika.
    Keputusan Menteri Kominfo Nomor 159 Tahun 2020 tentang Upaya Penanganan Corona Virus Disease (COVID-19) Melalui Dukungan Sektor Pos dan Informatika (Kepmenkominfo 159/2020) merupakan peraturan perundang-undangan pertama yang menjadi landasan digunakannya sebuah aplikasi untuk surveilans COVID-19. Dalam

menangani COVID-19, surveilans kesehatan merupakan salah satu upaya yang dilakukan.[262]

Kepmenkominfo 159/2020 menjabarkan surveilans kesehatan meliputi penelusuran (*tracing*), pelacakan (*tracking*), dan pemberian peringatan.[263] Selain surveilans kesehatan, terdapat berbagai upaya yang juga dilakukan, yakni akses layanan telekomunikasi dan internet, diseminasi informasi, sosialisasi, dan upaya-upaya lain yang ditetapkan pemerintah.[264]

Dalam rangka menyelenggarakan upaya-upaya tersebut, penyelenggara telekomunikasi berkontribusi, memfasilitasi, dan melakukan langkah-langkah yang diperlukan sesuai permintaan pemerintah/kementerian/lembaga/Gugus Tugas Percepatan Penanganan COVID-19 yang meliputi, namun tidak terbatas pada: [265]

a. Pemberian informasi dan data;
b. Penyediaan aplikasi;
c. Pemanfaatan *Mobile Subscriber Integrated Services Digital Network Number* (MSISDN);
d. Pemanfaatan alat dan perangkat telekomunikasi;
e. Pemanfaatan jaringan dan/atau jasa telekomunikasi;
f. Penyediaan layanan telekomunikasi dan internet dengan kapasitas dan kualitas layanan yang baik;
g. Penyediaan produk dan solusi yang mendukung kebijakan presiden untuk bekerja dari rumah, belajar dari rumah, dan ibadah di rumah sesuai dengan kapasitas masing-masing Penyelenggara Telekomunikasi;
h. *Short Message Services* ke banyak tujuan (SMS *blast*);
i. Fasilitas teknologi;
j. Optimasi, operasional, dan pemeliharaan/perbaikan (*operation and maintenance*) jaringan telekomunikasi, dengan tetap mematuhi kebijakan pemerintah untuk menjaga jarak aman (*physical distancing*); dan
k. Tindakan lain yang diperlukan yang ditetapkan pemerintah.

Mengenai penyediaan aplikasi, Kemenkominfo dapat menunjuk salah satu penyelenggara telekomunikasi untuk menyediakan aplikasi, dimana operasionalisasinya akan ditetapkan lebih lanjut oleh pemerintah.[266] Proses kerjasama

[262] Lihat: Kepmenkominfo 159/2020.
[263] *Ibid*.
[264] *Ibid*.
[265] *Ibid*.
[266] *Ibid*.

dengan penyelenggara telekomunikasi ini perlu menjadi fokus bahasan, mengingat akan berimplikasi juga pada bagaimana nantinya data-data dikumpulkan dan diproses.[267]

Menelaah berbagai ketentuan yang ada dalam Kepmenkominfo 159/2020, pada dasarnya di dalamnya hanya bersifat memberikan arahan kepada para pemangku kepentingan untuk membantu upaya penanganan COVID-19. Hal tersebut dapat dipahami karena bentuknya yang merupakan 'keputusan'.

12. Keputusan Menteri Kominfo Nomor 171 Tahun 2020 tentang Penetapan Aplikasi PeduliLindungi dalam Rangka Pelaksanaan Surveilans Kesehatan Penanganan Corona Virus Disease 2019 (COVID-19).
Keputusan Menteri Kominfo Nomor 171 Tahun 2020 tentang Penetapan Aplikasi PeduliLindungi dalam Rangka Pelaksanaan Surveilans Kesehatan Penanganan Corona Virus Disease 2019 (COVID-19) (Kepmenkominfo 171/2020) merupakan *beschikking* yang menjadi landasan digunakannya aplikasi PeduliLindungi sebagai aplikasi surveilans kesehatan oleh pemerintah dalam menangani penyebaran COVID-19. Surveilans yang dimaksud dalam peraturan ini meliputi penelusuran (*tracing*), pelacakan (*tracking*), dan pemberian peringatan. Hal ini sebagaimana senada dengan surveilans kesehatan yang dimaksud dalam Kepmenkominfo 159/2020.

Aplikasi PeduliLindungi dikembangkan oleh P.T. Telekomunikasi Indonesia, Tbk. dan hak ciptanya dilisensikan secara eksklusif kepada Pemerintah Republik Indonesia cq. Kementerian Komunikasi dan Informatika dan Kementerian Badan Usaha Milik Negara sesuai dengan ketentuan peraturan perundang-undangan.[268] Pelaksanaan teknis aplikasi PeduliLindungi melibatkan operator telekomunikasi dengan tetap menjaga perlindungan data pribadi sesuai peraturan perundang-undangan.[269]

Mengacu pada Kepmenkominfo 171/2020, PeduliLindungi hanya digunakan pada masa darurat COVID-19. Komitmen ini perlu untuk lebih diperjelas, karena hanya penggunaan PeduliLindungi yang hanya digunakan pada saat COVID-19, tidak terdapat kepastian terhadap data-data yang dikumpulkan. Praktiknya, TraceTogather di Singapura menggunakan data-data yang dikumpulkan untuk kepentingan-kepentingan lain. Meski mulanya TraceTogather berkomitmen untuk melindungi privasi dan hanya akan menggunakan data untuk tujuan pelacakan kontak. Perkembangannya, data yang dikumpulkan untuk pelacakan kontak COVID-19 dapat

[267] *Ibid*.
[268] Lihat: Kepmenkominfo 171/2020.
[269] *Ibid*.

> diserahkan ke polisi untuk penyelidikan kriminal.[270] Petugas Polisi yang berwenang dapat meminta kewenangan *Criminal Procedure Code* (CPC) untuk meminta pengguna mengunggah data TraceTogether mereka untuk penyelidikan kriminal. Kepolisian Singapura diberi wewenang di bawah CPC untuk mendapatkan data apapun, termasuk data TraceTogether, untuk penyelidikan kriminal.

Berangkat dari berbagai peraturan perundang-undangan di atas, baik yang terkait tata kelola data kesehatan secara umum maupun penyakit tertentu, dapat diketahui bahwa prinsip kerahasiaan cukup diatur dengan baik. Hampir setiap peraturan perundang-undangan yang mengatur kesehatan, mengintegrasikan prinsip kerahasiaan. Bahkan, terdapat juga prinsip retensi data, yakni sampai kapan sebuah data akan disimpan.

Namun demikian, masih terdapat catatan terkait ketidakselarasan pemaknaan rekam medis, data kesehatan, informasi kesehatan, dan sejenisnya. Juga terkait dengan konsepsi "pemilik" yang dianut, menjadikan tidak selaras dengan adanya konsep "subjek data" dalam pelindungan data pribadi. Selain itu, masih belum terlihat keteraturan aktor dalam tata kelola data kesehatan. Mengenai aktor, bahkan belum mampu memetakan aktor-aktor yang saat ini juga terlibat, seperti pengembang aplikasi kesehatan.

Berdasarkan catatan tersebut, tabel berikut ini merupakan pemetaan yang dapat dilakukan terkait pelindungan data dalam konteks tata kelola data kesehatan:

[270] Laurel Wamsley, "Singapore Says COVID-19 Contact-Tracing Data Can Be Requested By Police", NPR, 5 Januari 2021, https://www.npr.org/sections/coronavirus-live-updates/2021/01/05/953604553/singapore-says-covid-19-contact-tracing-data-can-be-requested-by-police diakses pada 15 Januari 2021.

Tabel Tata Kelola Data Kesehatan Secara Umum

Peraturan Perundang-Undangan	Pemaknaan Rekam Medis, Data Kesehatan, atau Sejenisnya	Aktor Pengendali dan/atau Pemroses Data Kesehatan
UU 29/2004	Rekam medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Selanjutnya, disampaikan bahwa dokumen rekam medis merupakan milik dokter, dokter gigi, atau sarana pelayanan kesehatan, sedangkan isi rekam medis merupakan milik pasien.	Dokter atau dokter gigi, pimpinan sarana pelayanan kesehatan.
UU 36/2009	Terdapat penyebutan data kesehatan. Meski begitu, tidak ditemukan pendefinisiannya.	Penyelenggara kesehatan.
UU 44/2009	Ruang lingkup data pasien adalah pelaksanaan kegiatan rekam medis yang dilakukan oleh rumah sakit.	Rumah sakit.
UU 36/2014	Meski terdapat penggunaan frasa rekam medis, namun tidak terdapat pendefinisiannya. Disebutkan bahwa mengenai rekam medis akan diatur dengan Peraturan Menteri. Dalam konteks saat ini, maka satu-satunya Peraturan Menteri Kesehatan tentang Rekam Medis adalah Permenkes 269/2008.	Tenaga kesehatan.
UU 38/2014	Menggunakan frasa informasi kesehatan, yakni informasi-informasi yang terkait dengan	Perawat.

	masalah kesehatan.	
PP 46/2014	Data kesehatan diartikan sebagai angka dan kejadian berupa keterangan dan tanda-tanda yang secara relatif belum bermakna bagi pembangunan kesehatan. Sedangkan, informasi kesehatan adalah data kesehatan yang telah diolah atau diproses menjadi bentuk yang mengandung nilai dan makna yang berguna untuk meningkatkan pengetahuan dalam mendukung pembangunan kesehatan.	Fasilitas pelayanan kesehatan dan pengelola sistem informasi kesehatan.
Perpres 72/2012	Terdapat penggunaan istilah informasi kesehatan, meskipun tidak terdapat pendefinisiannya.	Pemerintah pusat dan daerah.
Permenkes 269/2008	Rekam medis diartikan sebagai berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien. Paling tidak, data yang direkam adalah identitas pasien; hasil anamnesis, mencakup sekurang-kurangnya keluhan dan riwayat penyakit; hasil pemeriksaan fisik dan penunjang medik; diagnosis; dan pengobatan dan/atau tindakan.	Pimpinan sarana pelayanan kesehatan, petugas yang ditunjuk oleh pimpinan sarana pelayanan kesehatan, petugas pengelola dan sarana pelayanan kesehatan, dokter, dokter gigi, tenaga kesehatan tertentu, dan sarana pelayanan kesehatan non rumah sakit.
Permenkes 36/2012	Rekam medis diartikan sebagai berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang diberikan kepada pasien, termasuk dalam bentuk	Semua pihak yang terlibat dalam pelayanan kedokteran dan/atau menggunakan data dan informasi

	elektronik.	tentang pasien wajib menyimpan rahasia kedokteran. Secara lebih detail, disebutkan bahwa pihak yang terlibat meliputi: a. dokter dan dokter gigi serta tenaga kesehatan lain yang memiliki akses terhadap data dan informasi kesehatan pasien; b. pimpinan fasilitas pelayanan kesehatan; c. tenaga yang berkaitan dengan pembiayaan pelayanan kesehatan; d. tenaga lainnya yang memiliki akses terhadap data dan informasi kesehatan pasien di fasilitas

		pelayanan kesehatan; e. badan hukum/korporasi dan/atau fasilitas pelayanan kesehatan; dan f. mahasiswa/siswa yang bertugas dalam pemeriksaan, pengobatan, perawatan, dan/atau manajemen informasi di fasilitas pelayanan kesehatan.
Permenkes 69/2014	Terdapat penggunaan istilah rekam medik.	Rumah sakit, dokter dan dokter gigi, serta tenaga kesehatan.
Permenkes 75/2014	Terdapat penggunaan frasa data kesehatan, meski tidak terdapat definisi.	Fasilitas pelayanan kesehatan dan tenaga kesehatan.

Permenkes 20/2019	Digunakan istilah data pasien.	Pelayanan *telemedicine*, fasilitas pelayanan kesehatan, fasilitas pelayanan kesehatan pemberi konsultasi, dan fasilitas pelayanan kesehatan peminta konsultasi.

Tabel Tata Kelola Data Kesehatan Penyakit Tertentu

Peraturan Perundang-Undangan	Pemaknaan Rekam Medis, Data Kesehatan, atau Sejenisnya	Aktor
Permenkes 21/2013	Terdapat penggunaan istilah rekam medik (bukan medis). Hal ini tentu perlu dikaji, apa yang membedakan penggunaan kata medis dengan medik.	Fasilitas pelayanan kesehatan, tenaga kesehatan.
Permenkes 51/2013	Terdapat penggunaan istilah data individu pasien. Dimana data tersebut disimpan di unit layanan dan menjadi milik unit layanan.	Fasilitas pelayanan kesehatan, tenaga kesehatan, dinas kesehatan di daerah, Kementerian Kesehatan.

Permenkes 45/2014	Data dan informasi yang dimaksud merupakan data dan informasi yang terhadapnya dilakukan surveilans.	Unit pelayanan kesehatan pada fasilitas pelayanan kesehatan (termasuk puskesmas dan rumah sakit).
Permenkes 74/2014	Terdapat pengkategorian hasil tes HIV dikategorikan sebagai data yang bersifat rahasia.	Petugas layanan kesehatan (khususnya tim medis yang memberikan perawatan).
Permenkes 82/2014	Terdapat penggunaan istilah data kesehatan dan data status kesehatan. Namun, tidak ada lebih lanjut apa yang membedakan diantara keduanya.	Fasilitas pelayanan kesehatan yang melakukan penanggulangan penyakit menular, pejabat kesehatan masyarakat pada satuan kerja pemerintah pusat dan daerah, serta Tim Gerak Cepat pada tingkat pusat, provinsi, dan kabupaten/kota.
Permenkes 15/2015	Terkandung berbagai jenis data, namun tidak didefinisikan.	Sumber daya manusia pada laboratorium, jejaring laboratorium pada fasilitas pelayanan tingkat pertama-ketiga dan

		nasional.
Permenkes 67/2016	Data yang dimaksud merupakan data yang terhadapnya dilakukan surveilans.	Klinik, dokter perorangan, dinas kesehatan di daerah, Kementerian Kesehatan.
Kepmenkes 1479/2003	Data yang dimaksud merupakan data yang terhadapnya dilakukan surveilans.	Setiap layanan kesehatan baik di tingkat nasional, provinsi, hingga kabupaten/kota memiliki unit penyelenggaraan surveilans, mulai dari badan penelitian, pusat data dan informasi, rumah sakit, laboratorium kesehatan, unit surveilans, dan puskesmas, hingga mitra.
Kepmenkes 451/2012	Tidak menyebutkan.	Rumah sakit.

SE Dirjen Pengendalian Penyakit dan Penyehatan Lingkungan Kemenkes HK.03.03/III/0992/2014	Tidak menyebutkan.	Rumah sakit.
Kepmenkominfo 159/2020	Tidak menyebutkan.	Kominfo, penyelenggara telekomunikasi (dapat sebagai penyedia aplikasi).
Kepmenkominfo 171/2020	Tidak menyebutkan.	Kominfo, PT Telekomunikasi Indonesia, Tbk., operator telekomunikasi.

Berdasarkan uraian di atas, terdapat 2 (dua) kategori kebijakan yang dapat dipetakan yang memiliki relevansi dengan tata kelola pelindungan data pribadi dalam sektor kesehatan, seperti terlihat melalui diagram di bawah ini.



C. Pertanggung Jawaban Pelindungan Privasi Data Kesehatan: Pemetaan Aktor

Secara umum pengelolaan sistem informasi kesehatan nasional setidaknya memiliki sejumlah tujuan berikut:

1. Menjamin ketersediaan, kualitas, dan akses terhadap Informasi Kesehatan yang bernilai pengetahuan serta dapat dipertanggungjawabkan;
2. Memberdayakan peran serta masyarakat, termasuk organisasi profesi dalam penyelenggaraan Sistem Informasi Kesehatan; dan

3. Mewujudkan penyelenggaraan Sistem Informasi Kesehatan dalam ruang lingkup sistem kesehatan nasional yang berdaya guna dan berhasil guna terutama melalui penguatan kerja sama, koordinasi, integrasi, dan sinkronisasi dalam mendukung penyelenggaraan pembangunan kesehatan yang berkesinambungan.

Pengembangan sistem informasi kesehatan nasional tersebut memiliki mekanisme yang mengatur siklus pengelolaan data dan informasi kesehatan dengan sumber informasi yang diperoleh dari penyelenggara layanan kesehatan dan kewenangannya, seperti:

1. Pelayanan kesehatan rutin atau berkala oleh tenaga kesehatan yang berwenang;
2. Penyelenggaraan rekam medik, meliputi rekam medik elektronik dan rekam medik non elektronik;
3. Surveilans kesehatan;
4. Sensus dan survei dengan menggunakan metode dan instrumentasi yang dapat dipertanggungjawabkan secara ilmiah;
5. Penelitian dan pengembangan kesehatan;
6. Pemanfaatan teknologi dan sumber lain yang sesuai perkembangan ilmu pengetahuan dan teknologi serta dapat dipertanggungjawabkan; dan
7. Cara lain sesuai dengan ketentuan peraturan perundang-undangan.

Dalam pengelolaannya sistem informasi kesehatan menerapkan model sentralisasi dan desentralisasi sekaligus sehingga aktor pemangku yang terlibat dalam pengelolaan sistem informasi kesehatan sangat beragam termasuk pemerintah pusat, pemerintah daerah, bahkan di tingkat penyedia fasilitas pelayanan kesehatan. Tidak terbatas pada itu, ada pula instansi lain seperti Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan), Badan Penyelenggara Jaminan Sosial Ketenagakerjaan (BPJS Ketenagakerjaan, dan kementerian sektor lain yang juga mengelola data kesehatan warga untuk programnya seperti Kementerian Agama untuk program haji, Kementerian Pendidikan terkait data kesehatan siswa, dan sebagainya. Hal ini juga termasuk dengan sektor swasta.

Lebih lanjut peraturan perundang-undangan memberikan kewajiban bagi:

1. Pemerintah pusat untuk melakukan pengelolaan satu Sistem Informasi Kesehatan skala nasional dalam ruang lingkup Sistem Kesehatan Nasional;
2. Pemerintah provinsi, untuk melakukan pengelolaan satu Sistem Informasi Kesehatan skala provinsi;
3. Pemerintah kabupaten/kota, untuk melakukan pengelolaan satu Sistem Informasi Kesehatan skala kabupaten/kota; dan

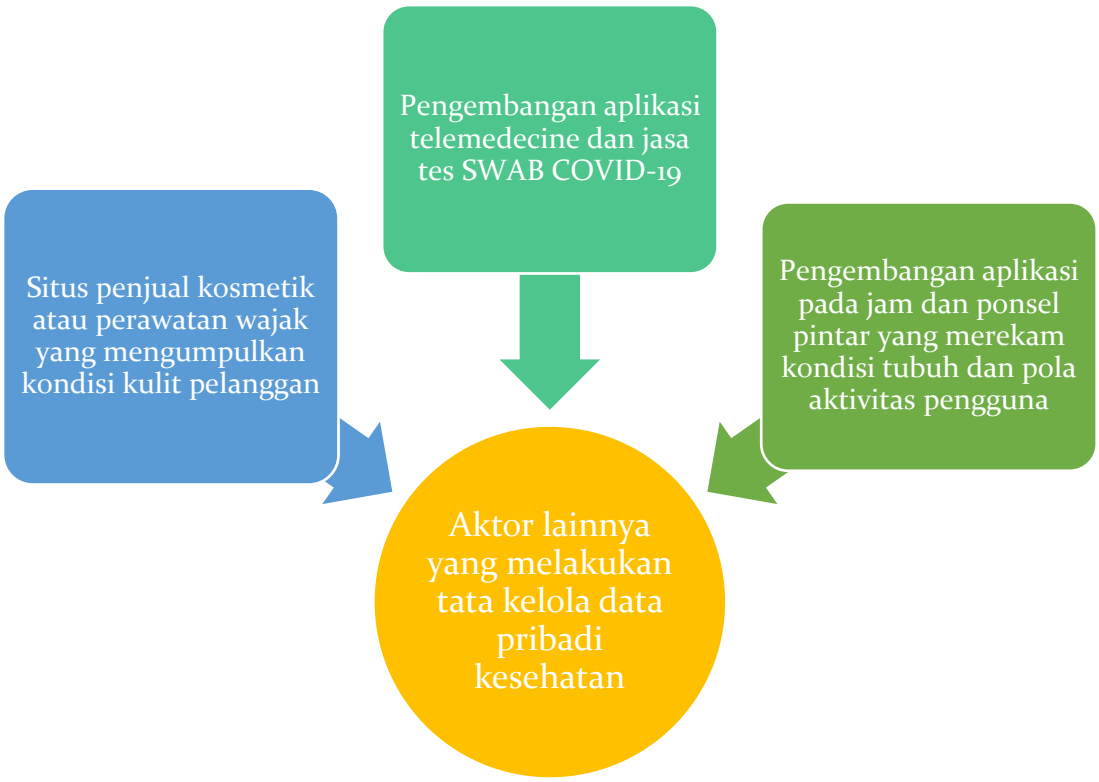
4. Fasilitas pelayanan kesehatan, untuk melakukan pengelolaan Sistem Informasi Kesehatan skala Fasilitas Pelayanan Kesehatan.

Meskipun demikian, pengaturan instansi di luar sektor kesehatan seperti BPJS dan kementerian lainnya belum diatur lebih jelas mengenai tanggung jawab pelindungan data pribadi atas data kesehatan yang dimanfaatkan.

Berdasarkan peraturan perundang-undangan tersebut identifikasi aktor dan peran yang dimainkan aktor tersebit dapat dilihat melalui diagram di bawah ini.



Selain aktor yang telah teridentifikasi, masih terdapat aktor lainnya yang masuk dalam skala sistem kesehatan dan alur data yang melibatkan pihak swasta, seperti pihak perbankan yang kerap kali memiliki produk asuransi kesehatan, situs-situs penjual kosmetik atau perawatan wajah dan kulit yang mengharuskan pengumpulan data tubuh calon konsumen dan berkaitan dengan perkembangan penggunaan aplikasi yang dibuat oleh swasta yang menyediakan jasa telemedicine atau bahkan tawaran penggunaan jasa tes COVID-19. Diagram di bawah ini menggambarkan pelibatan aktor lain dalam tata kelola data kesehatan.


Pengembangan aplikasi telemedecine dan jasa tes SWAB COVID-19
Situs penjual kosmetik atau perawatan wajak yang mengumpulkan kondisi kulit pelanggan
Pengembangan aplikasi pada jam dan ponsel pintar yang merekam kondisi tubuh dan pola aktivitas pengguna
Aktor lainnya yang melakukan tata kelola data pribadi kesehatan

VII. Permasalahan Pelindungan Data Pribadi Dalam Sektor Kesehatan di Indonesia.

A. Konsep dan Ruang Lingkup Data Kesehatan Belum Menyangkut Data Digital

Jika mengacu dari regulasi yang telah dijabarkan di atas, rekam medis dalam hukum positif di Indonesia masih mengacu pada rekam medis yang dikelola oleh penyedia layanan kesehatan seperti rumah sakit. Belum termasuk data kesehatan yang dikelola dalam sistem digital dan informasi lainnya berkaitan dengan tubuh manusia seperti aktivitas dan perilaku yang dimasukan ke dalam sistem aplikasi pintar secara sukarela oleh penggunanya. Dalam Peraturan Menteri Kesehatan yang menjadi dasar kebijakan mengenai tata kelola rekam medis diartikan sebagai catatan atau dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien. Data seperti hasil amnesis dan riwayat penyakit, hasil pemeriksaan fisik, diagnosis dan pengobatan. Selain itu, Permenkes Rekam Medis juga belum mengakomodir tata kelola rekam medis yang diproses dalam sistem informasi elektronik.

Pada perkembangannya pemanfaatan data kesehatan tidak hanya terbatas pada rekam medis, melainkan juga informasi pribadi untuk kepentingan administrasi dan data terkait tubuh lainnya seperti aktivitas dan kebiasaan. Selain itu sistem pengelolaan data kesehatan dalam berbagai layanan kesehatan telah menggunakan sistem informasi elektronik atau dalam bentuk digital. Konsep dan ruang lingkup data kesehatan yang masih terbatas pada informasi yang dikelola oleh penyedia layanan kesehatan berbasis kertas (non-digital) akan berdampak pada minimnya pelindungan data pribadi kepada pasien. Misalnya dalam hal pemanfaatan yang seharusnya terbatas bagi pihak-pihak tertentu sesuai dengan kapasitas dan kewenangannya di lingkungan medis atau untuk kepentingan yang telah ditentukan peraturan perundangan berpotensi diabaikan apabila dilakukan dalam bentuk digital, sehingga kontrol terhadap pemanfaatan data pribadi kesehatan pasien tidak terbatas dan dilakukan tanpa pengawasan. Sebagaimana diketahui, data kesehatan dan rekam medis kerap kali menjadi basis untuk melakukan penilaian atau *credit scoring* dalam proses rekrutmen pekerjaan atau untuk mendapatkan asuransi atau menentukan besaran premi asuransi. Meskipun terdapat sejumlah aturan untuk tidak mendiskriminasi penyakit tertentu, namun perspektif mengelola data kesehatan pekerja sebelum rekrutmen telah menjadi praktik lazim bagi para penerima kerja. Dalam konteks inilah prinsip-prinsip pelindungan data pribadi terhadap pemanfaat data kesehatan non-layanan medis tidak memiliki pengaturan khusus sebab tidak tunduk pada undang-undang dan aturan terkait sektor kesehatan.

Sedangkan dalam konteks data kesehatan yang bukan ditentukan oleh petugas atau laya nan medis, seperti data kebiasaan dan pantauan aktivitas pengguna aplikasi seperti data kalori

yang dikonsumsi, denyut jantung, jumlah langkah harian, siklus menstruasi, dan pencatatan suasana hati (*journaling)* untuk kesehatan mental merupakan komoditas baru dalam ekonomi digital yang sangat rentan dieksploitasi. Data-data tersebut meskipun tidak berkaitan erat dengan rekam medis, kerap kali mampu mengidentifikasikan individu dan sangat dimanfaatkan untuk kepentingan pemasaran produk dan layanan kesehatan. Padahal data terkait dengan tubuh dan kesehatan merupakan bagian dari data sensitif yang berpotensi menimbulkan diskriminasi dan erat kaitannya dengan kehidupan dan keamanan pribadi pengguna atau individu yang bersangkutan.

Selain itu, pandemi COVID-19 memaksa penanggulangannya memaksimalkan pemanfaataan teknologi. Misalnya dalam rangka melakukan surveilans, terdapat pemantauan gerak dari Orang Dalam Pemantauan (ODP) dan melakukan pelacakan termasuk pemberian peringatan melalui teknologi. Salah satunya melalui aplikasi PeduliLindungi. Tanpa ada pembaharuan konsep dan ruang lingkup data kesehatan dalam bentuk digital, potensi penyalahgunaan menjadi semakin besar dan kesulitan dalam penanggulangannya.

B. Kebutuhan Sinkronisasi Perspektif Data Kesehatan dalam Kacamata Pelindungan Data Pribadi

Sebagaimana telah disebutkan berdasarkan tinjauan regulasi pada bab sebelumnya, menurut Undang-Undang tentang Praktik Kedokteran, di Indonesia dokumen rekam medis merupakan milik sarana layanan kesehatan termasuk rumah sakit dan pekerja medis yakni dokter dan dokter gigi. Sedangkan isi rekam medis adalah milik pasien. Konsep ini cukup membingungkan apabila dilihat dengan perspektif pelindungan data pribadi, sebab dapat berimplikasi pada kontrol pasien atas datanya. Kepemilikan dokumen rekam medis dapat berimplikasi pada minimalnya kontrol pasien atas data kesehatan tentang dirinya.

Dalam konteks pelindungan data pribadi, pasien adalah subjek data sebab data kesehatan termasuk rekam medis merupakan informasi tentang dirinya dan melekat atasnya. Dengan demikian, individu memiliki kontrol terhadap pengumpulan dan informasi kesehatan pribadi yang saat ini dikelola dan dianggap sebagai aset oleh institusi kesehatan, pemerintah, dan vendor-vendor penyedia teknologi untuk kesehatan. Meskipun dalam Undang-Undang Praktik Kedokteran disebutkan bahwa isi dari rekam medis adalah bagian dari hak pasien untuk diketahui secara pribadi, tetapi hal tersebut belum memberikan kontrol sepenuhnya kepada pasien atas data pribadi dan rekam medisnya termasuk dalam hal pemanfaatan yang dilakukan dengan melibatkan pihak lain.

Kepemilikan data pada dasarnya mengacu pada penguasaan atas data yang tidak secara khusus mengidentifikasi individu tertentu. Dalam hal ini layanan kesehatan melakukan

penguasaan termasuk pemrosesan data kesehatan sehingga perlu mengidentifikasikan peran dan tanggung jawab sebagai pengendali dan pemroses data yang harus tunduk pada prinsip-prinsip pelindungan data pribadi. Beberapa prinsip seperti kerahasiaan dan retensi data memang telah diakui dalam peraturan perundang-undangan sektoral kesehatan. Meskipun demikian, diperlukan adanya aturan lebih rigid dan terbatas untuk membatasi wewenang pemanfaatan data sesuai dengan dasar hukum atau *legal ground* dengan pertimbangan analisis risiko terhadap pasien sebagai subjek data sebab akan berimplikasi pada hidupnya.

Dalam Permenkes tentang Rekam Medis memang disebutkan sejumlah alasan yang memungkinkan adanya pengungkapan informasi kesehatan atau rekam medis seperti untuk:

1. Kepentingan kesehatan pasien;
2. Pemenuhan permintaan aparatur penegak hukum dalam rangka penegakan hukum atas perintah pengadilan;
3. Permintaan dan/atau persetujuan pasien sendiri;
4. Permintaan institusi/lembaga berdasarkan ketentuan peraturan perundang-undangan; dan
5. Untuk kepentingan penelitian, pendidikan, dan audit medis, sepanjang tidak menyebutkan identitas pasien.

Namun dalam implementasinya diperlukan kaidah-kaidah sesuai pelindungan data pribadi. Misalnya dalam hal kepentingan kesehatan pasien, diperlukan informasi rinci kepada pasien maupun keluarga pasien dengan memberikan informasi lebih lanjut kepada pihak-pihak yang mungkin terkait dalam pengungkapan data pribadi dan retensinya. Begitu pula dalam hal kebutuhan pengungkapan data kesehatan untuk penegakan hukum, diperlukan aturan teknis implementatif berkaitan dengan jangka waktu dan derajat informasi yang bisa diungkapkan serta relevansinya pada kasus hukum terkait sehingga tidak menyebabkan diskriminasi lebih lanjut.

Dalam hal keterlibatan lembaga lain atau untuk kebutuhan penelitian, perlu ada penegasan mengenai kewajiban dan tanggung jawab dari pihak-pihak tersebut sebagai pemroses data. Kebutuhan untuk menilai apakah ada kemampuan yang memadai atau memenuhi syarat dalam tata kelola data kesehatan juga penting sebelum me mberikan akses terhadap pemanfaatan data. Hal-hal kunci di atas tentu tidak menegasikan posisi pasien sebagai subjek data yang memiliki kontrol atas datanya sehingga penting untuk mendapatkan persetujuan dengan informasi memadai.

C. Belum Adanya Peta Besar Alur Pemrosesan Data Pribadi Kesehatan dalam Sistem Kesehatan Nasional

Sebagaimana telah disebutkan dalam bab sebelumnya, dalam pengelolaan sistem informasi kesehatan telah dilaksanakan model sentralisasi dan desentralisasi sekaligus yang melibatkan berbagai pihak lintas sektor kesehatan termasuk instansi swasta. Mulai dari pemerintah pusat, pemerintah daerah, bahkan di tingkat penyedia fasilitas pelayanan kesehatan. Tidak terbatas pada itu, ada pula instansi lain seperti Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan), Badan Penyelenggara Jaminan Sosial Ketenagakerjaan (BPJS Ketenagakerjaan, dan kementerian sektor lain yang juga mengelola data kesehatan warga untuk programnya seperti Kementerian Agama, dan Kementerian Pendidikan, dan aplikasi pemantauan COVID-19. Sedangkan terkait sektor swasta, tidak hanya penyedia layanan kesehatan perusahaan umumnya menyimpan data kesehatan pasien serta layanan perbankan yang mempunyai produk asuransi juga memproses data pribadi kesehatan.

Dari aktor-aktor tersebut, Indonesia belum memiliki peta besar berkaitan dengan alur pemrosesan data pribadi.

Dampak dari kekosongan peta tersebut adalah tidak adanya identifikasi aktor-aktor terlibat yang melakukan pemrosesan dan pengelolaan data kesehatan, sehingga kewajiban dan tanggung jawab untuk menjaga data kesehatan termasuk data pribadi yang terkait dengan layanan kesehatan masih tersebar dengan aturan kewenangan terkait. Kondisi ini sebenarnya dapat berimplikasi pada minimalnya kontrol terhadap tata kelola dan pelindungan data pribadi, serta proteksi kepada subjek data. Di Amerika, tersebarnya data kesehatan yang melibatkan berbagai aktor bahkan dieksploitasi untuk kepentingan investasi dan penanaman modal. Situasi riil sekarang juga menyebabkan tidak adanya harmonisasi dan sinkronisasi standar operasional dalam tata kelola data pribadi, sehingga kerentanan eksploitasi semakin besar.

D. Kebocoran Data Kesehatan di Berbagai Wilayah di Indonesia

Kebocoran data kesehatan sebenarnya memiliki dampak kerugian yang paling besar jika dibandingkan data yang lain. Pertama, karena fakta isi rekam medis tidak dapat dihapus mengingat berisikan kondisi kesehatan seseorang. Kedua, data kesehatan terdiri dari data pribadi yang mengidentifikasi seseorang dengan informasi kesehatan yang bersifat sangat sensitif yang jika disebarkan kepada pihak yang tidak memiliki kewenangan berpotensi menjadi bahan diskriminasi. Di Indonesia tercatat telah terjadi sejumlah kebocoran data kesehatan dan penyebaran informasi kesehatan tanpa izin dari pasien atau orang yang bersangkutan. Terutama pada pandemi COVID-19, kerap kali pengungkapan identitas pasien

COVID-19 tidak mempertimbangkan pelindungan data pribadi pasien dan keluarganya dengan menyebutkan nama lengkap, NIK, dan alamat rumah yang bersangkutan. Meskipun pengungkapan identitas diperlukan untuk proses penelusuran dan pelacakan, tetapi diperlukan metode lebih rinci sesuai dengan prinsip pelindungan data dan kerahasiaan dalam dunia medis.

Dalam skala besar, pada bulan Juni 2020 lalu, salah satu akun dalam forum Hacker mengklaim memiliki lebih dari 200.000 data pribadi pasien COVID-19 Indonesia. Elemen data yang dimiliki adalah nama, nomor telepon, alamat, hasil tes PCR, dan lokasi tempat pasien dirawat.[271] Meskipun dalam beberapa saat instansi pemerintah melalui Badan Siber Sandi Negara (BSSN) membantah adanya kebocoran data sebab tidak ditemukan upaya paksa akses ke dalam jaringan sistem elektronik data pasien COVID-19 di Indonesia, tetapi data pasien COVID-19 beserta data pribadinya terungkap ke publik terutama dalam situs pasar gelap. Hal ini menunjukan bahwa perlu ada standar manajemen dalam tata kelola data pribadi yang lebih memperhatikan pelindungan privasi, termasuk cara pengungkapan data dan pengamanan informasi lainnya seperti NIK, alamat dan nomor telepon yang penyalahgunaannya sangat rentan terhadap warga.

E. Kebutuhan Menyeimbangkan Transparansi Data untuk Kesehatan Publik dalam Koridor Pelindungan Privasi

Kebutuhan untuk penelitian, pendidikan dan pengembangan ilmu pengetahuan dan melindungi kepentingan kesehatan publik secara umum merupakan alasan fundamental yang memungkinkan adanya pemanfaatan akses data kesehatan. Meskipun demikian, alasan-alasan tersebut tidak menegasikan adanya kewajiban untuk tunduk pada prinsip pelindungan data pribadi serta kepatuhan terhadap sejumlah kewajiban bagi pengend ali dan pemroses data pribadi khususnya data kesehatan. Sehingga diperlukan adanya kerangka data pribadi yang menentukan pemanfaatan data kesehatan yang sesuai dengan kaidah pelindungan data pribadi.

Transparansi data kesehatan, secara khususnya jumlah kasus pada penyakit tertentu sangat dibutuhkan dalam pengendalian penyakit dan program kesehatan lainnya. Dalam penanganan pandemi COVID-19 jumlah orang positif COVID-19 di satu wilayah sangat menentukan penanggulangan dan memastikan strategi di layanan kesehatan dan pengambilan keputusan. Dalam konteks penanggulangan HIV/AIDS, partisipasi masyarakat diakui untuk peningkatan layanan kesehatan. Partisipasi masyarakat melalui komunitas sebagai sayap layanan kesehatan dilakukan di berbagai kegiatan, mulai dari penjangkauan

[271] https://www.kompas.com/tren/read/2020/06/20/180500065/data-pasien-covid-19-diduga-bocor-mengapa-hal-ini-bisa-terjadi?page=all

kelompok kunci, melakukan pendampingan hingga memastikan rujukan ke layanan kesehatan untuk melakukan tes HIV, pendaftaran akses pengobatan ARV, hingga tes viral load. Kegiatan-kegiatan ini kemudian dievaluasi dan hasilnya menunjukan adanya kebutuhan untuk melakukan penelusuran bagi ODHA yang putus layanan ARV atau disebut *loss to follow-up*. Atau dalam program vaksinasi, dibutuhkan daftar jumlah penerima akses vaksin yang membutuhkan data nama dan alamat untuj proses verifikasi dan validasi. Juga berkaitan dengan data BPJS Kesehatan yang memungkinkan adanya pemrosesan data lanjutan untuk pengembangan *data analytics* atau penelitian dari data sampel basis data kepesertaan dan kaminan pelayanan kesehatan.

Dalam situasi-situasi di atas, akses data pribadi bukan tidak dimungkinkan, hanya saja diperlukan adanya standar operasional yang jelas dalam manajemen data-data tersebut khususnya yang menyangkut data pribadi. Misalnya, untuk beberapa situasi data yang dibutuhkan bukan data pribadi melainkan data agregat yang tidak mengungkapkan idnividu tertentu. Lebih lanjut, jika dibutuhkan adanya pengungkapan data pribadi, perlu diadakannya uji publik terhadap *legal basis,* penilaian risiko yang mempertimbangkan kebutuhan pengungkapan data tersebut untuk kepentingan publik dan risiko yang dialami pasien atau individu. Selain itu kewajiban untuk tunduk pada prinsip dan komitmen menjaga kerahasiaan dan integritas dari sistem informasi data kesehatan, memastikan adanya retensi berapa lama data disimpan dengan prinsip minimalisasi, dan aktor-aktor terlibat yang memiliki akses dan mengelola data pribadi tunduk pada kewajiban pemroses dan pengendali salah satunya *non-disclosure agreement*.

Selain data pasien COVID-19, data jaminan kesehatan juga memiliki risiko tinggi jika terjadi kebocoran. Terutama pasca pemanfaatan data BPJS Kesehatan melibatkan sejumlah pemrosesan data lanjutan, seperti pengembangan *data analytics* dan fasilitas *payment gateway* untuk pembayaran iuran,[272] dan penerbitan data sampel basis data kepesertaan dan jaminan pelayanan kesehatan yang digunakan untuk penelitian dan pengambilan kebijakan berbasis bukti. Data jaminan kesehatan ini menjadi urgen dan memiliki risiko tinggi, mengingat data kepesertaan juga terasosiasi dengan rekam medis peserta BPJS, termasuk status kesehatan seperti HIV dan penyakit lainnya.[273]

F. Potensi Diskriminasi terhadap Kelompok Rentan dan Kondisi serta Penyakit tertentu

[272] https://swa.co.id/TelecommunicationUpdate/telecommunicationupdate/telkom-update/telkomgroup-dan-bpjs-kesehatan-sepakati-kemitraan-strategis-optimalisasi-penyelenggaraan-program-jkn-kis

[273] https://www.cnbcindonesia.com/tech/20190225142730-37-57456/sri-mulyani-wanti-wanti-agar-data-bpjs-tak-bocor-ada-apa

Data kesehatan sangat penting terhadap identitas individu dan kondisi lainnya tentang diri mereka. Banyak pihak yang tidak ingin diketahui publik bahwa dirinya memiliki sedang dalam kondisi sakit atau terluka. Kerap kali informasi mengenai disabilitas, penyakit, atau kondisi kesehatan tertentu berdampak pada sudut pandang orang terhadap pihak tersebut sehingga perlu dirahasiakan atau tidak diungkapkan. Lebih dari itu, pelindungan data kesehatan juga penting secara instrumental, untuk meminimalkan adanya tindakan diskriminasi terhadap kondisi kesehatan atau ketubuhan. Sebagaimana telah disebutkan rekam medis dan kondisi kesehatan kerap kali menentukan layanan atau kehidupan manusia lainnya seperti pekerjaan atau akses layanan dan besaran iuran asuransi. Belum lagi realita stigmatisasi terhadap penyakit tertentu yang masih kental di Indonesia dan diskriminasi pada kondisi kesehatan terhadap komunitas atau identitas gender tertentu sehingga membutuhkan pelindungan dan tata kelola khusus mengenai data kesehatan untuk meminimalisir hal ini.

Di Indonesia, orang dan anak dengan HIV/AIDS (ODHA dan ADHA) masih mengalami diskriminasi tinggi, baik dalam lingkungan pekerjaan, pendidikan, maupun masyarakat secara umum dan ketika berhadapan dengan aparat penegak hukum. Diskriminasi kepada pekerja atas status HIV baik di sektor swasta maupun pemerintahan masih sering terjadi hingga berdampak pada pemutusan hubungan kerja. Meskipun ada regulasi khusus yang menyebutkan bahwa ODHA tidak bisa dikeluarkan karena statusnya, namun hal ini belum sepenuhnya diindahkan. Termasuk kasus adanya ADHA yang dikeluarkan dari sekolah dan kesulitan mengakses layanan pendidikan. Belum lagi realita adanya pengungkapan hasil tes HIV seorang terdakwa atau tersangka kejahatan yang dilakukan aparat pe negak hukum kepada publik hingga peliputan media massa, padahal tidak relevan dengan kejahatan tertentu yang meningkatkan stigmatisasi di masyarakat. Stigmatisasi ini muncul karena beberapa hal, mulai dari minimnya pengetahuan publik termasuk aparat mengenai cara penularan HIV/AIDS dan minimnya perspektif kerahasiaan atas pengelolaan data kesehatan termasuk a status HIV/AIDS. Kondisi miris ini kemudian juga terjadi meningkat dalam konteks pandemi COVID-19, menyebabkan beberapa orang yang positif COVID-19 merasakan diskriminasi, mulai dari tenaga medis yang diusir dari tempat tinggal,[274] kehilangan pekerjaan, hingga pelecehan dan ujaran kebencian karena dianggap sebagai sumber penyakit. Padahal, stigmatisasi sosial atas status COVID-19 dapat memperburuk penanggulangan pandemi.

Selain status penyakit tertentu, beberapa kondisi kesehatan juga berpotensi pada diskriminasi tertentu. Misalnya status kehamilan dialami anak perempuan atau perempuan dewasa di luar pernikahan. Di Indonesia, anak sekolah yang hamil kerap kali mendapatkan stigma negatif di

[274] https://republika.co.id/berita/q7n17y409/cerita-duka-tenaga-medis-meninggal-hingga-diusir-dari-emkosanem

masyarakat, bahkan mengalami diskriminasi hingga dikeluarkan paksa dari sekolah.[275] Belum lagi perempuan usia dewasa yang diketahui hamil di luar nikah juga kerap kali mendapat stigma negatif, meskipun dalam beberapa kasus adalah korban dari pemerkosaan. Lebih lanjut, orientasi seksual dan aktivitas seksual yang merupakan bagian dari data kesehatan yang lebih luas juga menjadi data sensitif dan rentan mengalami diskriminasi di Indonesia.[276]

Keenam permasalahan pelindungan data pribadi dalam sektor kesehatan tersebut dapat digambarkan melalui diagram di bawah ini.



[275] https://www.merdeka.com/peristiwa/hamil-siswi-smk-dikeluarkan-dari-sekolah.html
[276] https://www.bbc.com/indonesia/berita_indonesia/2014/08/140814_lgbt_indonesia

VIII. Kesimpulan dan Rekomendasi

A. Kesimpulan

Seiring dengan upaya berbagai belahan dunia dalam menanggulangi pandemi COVID-19 untuk menciptakan kesehatan publik, isu data kesehatan dan mekanisme pelindungannya menjadi penting. Pasalnya, data pribadi kesehatan yang tergolong sebagai data sensitif dan rentan menimbulkan diskriminasi, sangat relevan dengan pengambilan kebijakan kesehatan publik. Pengelolaan dan pemanfaatan data pribadi kesehatan bahkan dapat mempengaruhi akses masyarakat terhadap akses pelayanan kesehatan itu sendiri atau layanan publik lainnya seperti asuransi dan layanan perbankan.

Istilah pelindungan data pribadi dalam sektor kesehatan kerap kali diasosiasikan dengan kerahasiaan dalam kerangka kode etik kesehatan. Hal ini ditemukan dalam sejumlah kerangka legislasi sektor kesehatan yang menginternalisasikan 'kerahasiaan' dalam kode etik profesi dan rangkaian pengaturan tata kelola data kesehatan khususnya rekam medis, seperti ketentuan retensi data yang membatasi sampai kapan sebuah data akan disimpan. Meskipun demikian, prinsip kerahasiaan tersebut sebenarnya menjadi penting untuk dielaborasi lebih lanjut untuk mengidentifikasi kebutuhan di langkah teknis. Pasalnya, jika mengacu pada konsepnya, kerahasiaan atau *'confidentiality'* umumnya mengacu pada strategi prinsip keamanan sistem informasi.

Efektifitas menciptakan ekosistem yang aman dan menjalankan prinsip kerahasiaan ini juga wajib didukung dengan tata kelola yang berpusat pada pelindungan data pribadi. Hal ini akan berimplikasi pula pada perkembangan konsep 'kepemilikan' data oleh instansi penyedia layanan kesehatan yang cenderung memiliki konotasi eksploitatif, sehingga perlu untuk menempatkan pandangan perlindungan hak, yakni menyebutkan pasien sebagai subjek data dalam konteks tata kelola datanya.

Selain itu, terdapat sejumlah hal konseptual yang perlu dikembangkan sebagai bentuk produksi pengetahuan baru yang harus disepakati yang berimplikasi pada kebijakan kesehatan publik. Hal ini juga akan membantu menjawab kemungkinan tantangan dan persoalan yang berkaitan dengan perkembangan teknologi. Salah satunya mengenai ruang lingkup data kesehatan yang tidak terbatas pada rekam medis, namun berbagai informasi mengenai kesehatan. Hingga kini memang masih sangat nampak ketidakselarasan pemaknaan rekam medis, data kesehatan, informasi kesehatan. Lebih lanjut, pemaknaan

tersebut belum mampu mengikuti perkembangan teknologi, seperti halnya keberadaan rekam medis elektronik dan aplikasi-aplikasi pencatatan aktivitas gaya hidup yang berimplikasi pada profil kesehatan seseorang. Dengan pembaharuan konsep ini, identifikasi aktor yang terlibat tata kelola data kesehatan juga semakin nampak sehingga penting untuk mendistribusikan kewajiban di tiap-tiap sektor terlibat. Salah satunya misalnya pengembang aplikasi kesehatan yang mengelola data yang tergolong data sensitif namun tidak memiliki beban tanggung jawab sebagaimana tenaga medis.

B. Rekomendasi

Dalam rangka memastikan pelindungan privasi dalam tata kelola data kesehatan, berikut rekomendasi yang seharusnya diadopsi oleh para pemangku kepentingan:

1. Pengambil kebijakan untuk sektor kesehatan publik perlu mengkaji lebih lanjut terkait dengan perkembangan konsep data kesehatan di era teknologi yang tidak terbatas pada rekam medis fisik melainkan dalam bentuk digital. Serta data-data kesehatan non-rekam medis yang hanya ditentukan oleh tenaga medis, melainkan segala informasi tentang tubuh seseorang yang berimplikasi pada profil kesehatan seorang individu seperti pencatat detak jantung, siklus menstruasi, dan sebagainya;
2. Mengingat data kesehatan tergolong sebagai data sensitif yang berpotensi menyebabkan diskriminasi, maka penting untuk mengintegrasikan prinsip-prinsip hak asasi manusia dalam tata kelola datanya. Sektor kesehatan dan pengambil kebijakan yang terkait perlu untuk memperbarui dan mereformasi mekanisme pelindungan dan tata kelola sistem data kesehatan di Indonesia yang lebih mengedepankan pelindungan pasien sebagai subjek data;
3. Melakukan revisi, harmonisasi, dan akselerasi proses lahirnya peraturan perundang-undangan terkait kesehatan yang responsif. Kebijakan spesifik mengenai langkah teknis pelindungan data pribadi dalam data kesehatan seperti standar operasional yang dapat diimplementasikan oleh layanan kesehatan dan tenaga medis;
4. Melakukan identifikasi aktor-aktor baik privat maupun publik, di tingkat pusat dan daerah. Dari identifikasi tersebut akan membantu untuk mendistribusikan kewajiban dan kewenangan sebagai pengendali dan pemroses data pribadi di sektor kesehatan yang sesuai dengan prinsip pelindungan data pribadi dan mengikuti perkembangan teknologi yang diimplementasikan ke tingkat kebijakan maupun regulasi;
5. Melakukan akselerasi pembahasan RUU Pelindungan Data Pribadi. Dengan disahkannya RUU tersebut akan menjadi rujukan utama dalam rangka harmonisasi peraturan perundang-undangan terkait kesehatan dengan prinsip-prinsip pelindungan data pribadi.

Profil ELSAM

Lembaga Studi dan Advokasi Masyarakat (ELSAM) menggabungkan metode kerja organisasi think tank dan advokasi hak asasi manusia (HAM), dalam operasionalnya. Karakter inilah yang membuat ELSAM unik dibandingkan dengan organisasi HAM sejenis di Indonesia. ELSAM berupaya untuk terus mendorong hadirnya kebijakan berbasis bukti untuk memperkuat perlindungan HAM.

Saat ini ELSAM setidaknya memiliki empat kegiatan utama, yang terdiri atas: (1) studi dan produksi pengetahuan HAM untuk mendukung advokasi kebijakan;(2) pengarusutamaan HAM dalam pembentukan kebijakan;(3) advokasi hukum untuk mendorong perubahan kebijakan dan pembelaan hak korban; dan (4) penyelenggaraan berbagai pendidikan HAM.

- Dalam penyelenggaraan studi dan produksi pengetahuan HAM, ELSAM memfokuskan diri pada topik-topik khususnya: (i) bisnis dan HAM; (ii) teknologi dan HAM, terutama terkait tata kelola internet, kebijakan konten, perlindungan data pribadi, keamanan siber, dan respons terhadap perkembangan terbaru teknologi; (iii) lingkungan dan HAM, dengan mendorong adopsi pendekatan berbasis hak dalam upaya-upaya keberlanjutan.

- Dalam pengarusutamaan HAM pada proses pembentukan kebijakan, fokus ELSAM terutama pada topik: bisnis dan HAM, teknologi dan HAM, penyelesaian pelanggaran HAM di masa lalu, dan perlindungan kebebasan sipil, khususnya dalam konteks kebebasan berekspresi, kebebasan beragama, juga kebebasan berkumpul dan berorganisasi.

- Dalam melakukan advokasi hukum, ELSAM menerapkan pendekatan litigasi strategis sebagai upaya untuk sekaligus melakukan perubahan kebijakan, dan adanya pemulihan hak-hak korban. Selain melakukan pembelaan hukum di

pengadilan, terutama pengujian berbagai peraturan perundang-undangan dan kebija kan, ELSAM juga secara berkala mengirimkan amicus brief untuk kasus-kasus tertentu.

- Dalam upaya promosi dan penguatan kapasitas pemangku kepentingan, ELSAM secara terus-menerus menyelenggarakan berbagai pendidikan HAM. Pendidikan ini ditujukan bagi seluruh aktor, tidak hanya para pembela HAM, tetapi juga pengambil kebijakan di tingkat pusat dan daerah, aparat penegak hukum, juga korporasi swasta. Materinya juga mencakup topik-topik khusus, seperti: bisnis dan HAM, perlindungan data pribadi, keamanan digital, dan pendekatan berbasis hak dalam pengambilan kebijakan.

Selama lebih dari dua dekade ELSAM telah memberikan sejumlah kontribusi dalam mendorong adopsi dan implementasi HAM, mulai dari pengesahan berbagai konvensi internasional HAM, hingga pembentukan sejumlah undang-undang. Berbagai undang-undang yang lahir pasca-reformasi, seperti UU Komisi Kebenaran dan Rekonsiliasi dan UU Perlindungan Saksi dan Korban, ELSAM secara khusus terlibat dalam proses pembentukannya. Selanjutnya, dalam perkembangannya saat ini, ELSAM mendorong lahirnya berbagai legislasi untuk merespons kecepatan inovasi digital, seperti perlindungan data pribadi dan keamanan siber. ELSAM juga terlibat aktif dalam penguatan kelembagaan HAM, seperti Komisi Nasional HAM, Lembaga Perlindungan Saksi dan Korban, serta upaya memastikan konsistensi pelaksanaan HAM melalui dukungan dalam optimalisasi kebijakan Rencana Aksi Nasional (RAN) HAM.