IMPLIKASI PENERAPAN PROGRAM *E-HEALTH* DIHUBUNGKAN DENGAN PERLINDUNGAN DATA PRIBADI

Sinta Dewi Rosadi

Universitas Padjajaran
Jl Dipati Ukur No. 35 Bandung
Email: sintadewirosadi@yahoo.com

Diterima: 28 Nopember 2016 | **Direview**: 29 Desember 2016 | **Disetujui**: 11 Januari 2017

Abstract

The ICT advancement to connect health centers and hospitals to use electronic health applications (e-health) has become a global issue. E-health which is one of the Action Plan of the World Summit on the Information Society (WSIS) Geneva 2003 is an ICT-based application for the health care industry. The use of e-health application is to improve access, efficiency, effectiveness, and quality of medical process involving the organization of medical services in hospitals, clinics, health centers, medical practitioners both doctors and therapists, laboratories, pharmacies, insurers also involves the patient as a consumer. But in the service process will collect some sensitive personal data of consumers and cause new legal problems, to what extent of the health providers can protect the personal data of patients that their personal data can be accessed, disseminated easier through advances in ICTs. This research aims to examine in depth about how far patient's personal data will be protected in e-health program and how far the existing law has provided protection. The method used is normative juridical approach with descriptive analytical specifications. The process of data collection is done through literature and field research. The results of the research to date e-health program has been carried out in several provinces in Indonesia but until now the existing regulations do not provide maximum protection of personal data of patients. The approach of existing law is still sectoral and very general therefore has not yet provide maximum protection

***Key words**: E-Health program, protection, personal data*

Abstrak

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) untuk menghubungkan pusat kesehatan maupun rumah sakit dengan menggunakan aplikasi *electronic health* (*e-health*) telah menjadi isu global. *E-health* yang merupakan salah satu Rencana Aksi *World Summit on the Information Society* (WSIS) Geneva 2003 tersebut merupakan aplikasi berbasis TIK untuk industri pelayanan kesehatan. Penggunaan aplikasi e-health bertujuan untuk meningkatkan akses, efisiensi, efektivitas, serta kualitas proses medis yang melibatkan organisasi pelayanan medis di rumah sakit, klinik, puskesmas, praktisi medis baik dokter maupun terapis, laboratorium, apotek, asuransi juga melibatkan pasien sebagai konsumen. Akan tetapi dalam proses pelayanan dengan menggunakan program *E-health* akan mengumpulkan sejumlah data pribadi konsumen yang merupakan data pribadi sensitif dan menimbulkan permasalahan hukum yang baru yaitu sejauhmana pihak penyelenggara jasa kesehatan dapat melindungi data pribadi pasien dapat diakses, disebarluaskan secara lebih mudah melalui kemajuan TIK. Penelitian ini bertujuan untuk menelaah secara mendalam tentang bagaimana perlindungan data pribadi pasien dalam program *e-health* dan bagaimana hukum yang ada (*existing law*) dalam memberikan perlindungan. Metode penelitian yang digunakan adalah menggunakan

 DOI: http://dx.doi.org/10.21776/ub.arenahukum.2016.00903.6

pendekatan yuridis normatif dengan spesifikasi bersifat deskriptif analitis. Proses pengumpulan data dilakukan melalui penelitian kepustakaan dan penelitian lapangan. Hasil penelitian hingga saat ini program e-health telah dilakukan dibeberapa Propinsi di Indonesia akan tetapi hingga saat ini peraturan yang ada (*exisiting law*) belum memberikan perlindungan yang maksimal atas data pribadi pasien karena pengaturannya masih bersifat sektoral dan tersebar dalam beberapa Peraturan Perundang-undangan.

Kata kunci: program *E-Health*, perlindungan, data pribadi

Latar Belakang

Salah satu pilar globalisasi adalah penggunaan komunikasi yang merupakan pilar utama hubungan internasional dengan menggunakan kemajuan teknologi informasi. Dalam perkembangannya, kemajuan teknologi informasi telah mendorong negara-negara untuk meliberalisasi sektor komunikasi sehingga mendorong kompetisi dan globalisasi komunikasi dan pada akhirnya telah menstimulasi kemajuan ekonomi.[1]

Kini, dunia sedang berada dalam abad informasi yang keberadaan suatu informasi mempunyai peranan yang sangat penting di dalam kehidupan manusia.[2] Melalui kemajuan informasi, komunikasi, dan teknologi (selanjutnya akan disebut dengan TIK) merupakan salah satu faktor utama yang mendorong perkembangan dan pertumbuhan ekonomi dunia.[3] Saat ini, informasi merupakan komoditi yang mempunyai nilai ekonomi tinggi karena tidak semua pihak mampu untuk memproses dari suatu data yang mentah menjadi suatu informasi yang sesuai dengan kebutuhannya.[4] TIK memainkan peran penting dalam mendukung kehidupan sehari-hari, termasuk didalamnya pada bidang kesehatan.

Pemanfaatan TIK untuk kesehatan (*e-Health*) telah menjadi isu global dan merupakan salah satu Rencana Aksi WSIS (*World Summit on the Information Society*) Geneva 2003 untuk menghubungkan pusat kesehatan dan rumah sakit menggunakan teknologi informasi dan komunikasi . *E-Health* merupakan aplikasi berbasis TIK yang berkaitan dengan industri pelayanan kesehatan serta bertujuan untuk meningkatkan akses, efisiensi, efektivitas, serta kualitas proses medis. Karena proses medis ini selain melibatkan organisasi pelayanan medis di rumah sakit, klinik, puskesmas, praktisi medis baik dokter maupun terapis, laboratorium, apotek, asuransi juga melibatkan pasien

1 John Baylis & Steve Smith, *The Globalization of World Politics, An Introduction to International Relations*, (New York: Oxford University Press, 2001), pp. 540-541.

2 *Ibid*.

3 Kofi A. Anan dalam *UNCTAD E-commerce and Development*, (New York: UNCTAD Report, 2004), p. 4.

4 Edmon Makarim, *Kompilasi Hukum Telematika*, (Jakarta: RajaGrafindo Perkasa, 2003), hlm. 3. Lihat juga M. Arsyad Sanusi, *Teknologi Informasi & Hukum E-commerce*, (Jakarta: Dian Ariesta, 2004), hlm. 9. Menurut Branscomb, *Information is the Lifeblood that sustain political, social and business decision*, dalam Anne W. Branscomb, "Global Governance of Global Networks: "A survey of Transborder Data Flows in Transition", *Vanderbilt Law Review Vol. 36*, (1983): 985.

sebagai konsumen. Indonesia merupakan suatu negara berkembang dengan sejumlah banyak masalah dan tantangan (*challenges*) dalam bidang kesehatan masyarakat. Pengembangan dan penggunaan Telemedika dan *e-health* (serta bidang-bidang terkait lainnya) mempunyai banyak peluang guna membantu pemecahan masalah dan tantangan dalam bidang tersebut.Berbagai jenis aplikasi yang dapat dimanfaatkan antara lain, pencatatan dan pelaporan, pengelolaan wabah, resep elektronik, pengelolaan pasien TBC, sistem telemedika bergerak, *e-psychology*, *mobile e-health*, berbagai jenis sistem *e-health* dengan pengolahan citra, serta sistem *open*-EHR (*Electronic health record*).[5]

Melalui program *e-health* diperkirakan 98.000 kematian tiap tahun akibat kesalahan yang dapat dihindari, 70% komplikasi akibat pelayanan medis dapat dicegah, Proses pelayanan kesehatan dipahami dari segi sistem bukan individu. Dalam hal ini, Teknologi informasi berperan penting sebagai agen perubahan.[6] Sementara itu, dari bidang teknologi informasi juga mampu memberikan dukungan pengambilan keputusan dalam manajemen obat dan pengobatan. Penggunaan media TIK diharapkan kesalahan dan ketidak akuratan dalam pemberian obat, bisa diminimalisir.[7] Untuk mendukung program e-health beberapa provider TIK seperti PT Telkom Tbk tetap mengembangkan *'Project Business e-Health'* yang difokuskan untuk membangun layanan informasi terintegrasi berbasis elektronik bagi ekosistem kesehatan.[8] Potensi bisnis dari program e-health ini direspon oleh Bank Mandiri dengan meluncurkan program elektronik klaim Jaminan Kesehatan Semesta (Jamkesta) Mandiri *'Coordinating of Benefit"* (COB) di RSUD Wonosari, Kabupaten Gunung Kidul, Daerah Istimewa Yogyakarta, Senin, ia mengatakan proyek tersebut berjalan di atas *platform Helalth Information Exchange* (HIE) yang merupakan sistem yang memfasilitasi pertukaran data kesehatan secara elektronik dan data yang bisa dipertukarkan adalah data hasil pemeriksaan dokter, pemberian obat , pemberian resep obat, pemeriksaan laboratorium, penetapan harga layanan kesehatan oleh rumah sakit.[9]

Akan tetapi penerapan program *e-health* pada waktu yang sama akan menimbulkan sejumlah permasalahan hukum baru yang seringkali luput untuk dibicarakan: (1) berkaitan dengan bagaimana perlindungan hukum atas privasi atas data pribadi pasien; (2) bagaimana ketentuan hukum yang ada dapat memberikan perlindungan hukum bagi pasien . Dalam perkembangan ekonomi yang

5 Putra Setia Utama, "E-Health di Indonesia", http://ehealthindonesia.com/content/telemedika-e-health-aplikasinya-di-indonesia-butuh-kerjasama-multidisipliner, diakses 10 Maret 2014.

6 *Ibid*.

7 *Ibid*.

8 Telkom, "Proyek E Helath Telkom Jalan Terus", http://ehealthindonesia.com/content/proyek-ehealth-telkom-jalan-terus, diakses 12 Maret 2014.

9 *Ibid*.

modern seperti sekarang ini maka informasi termasuk data pribadi merupakan aset yang sangat berharga yang mempunyai nilai ekonomi tinggi sehingga banyak dimanfaatkan oleh kalangan bisnis sehingga diperlukan perlindungan. Selanjutnya keinginan menjaga privasi atas data pribadi tersebut berkaitan erat dengan tingkat kepercayaan pengguna. Pengguna dalam hal ini pengguna layanan jasa kesehatan terutama yang berbasis elektronik akan merasa nyaman melakukan transaksi melalui internet kalau merasa yakin adanya perlindungan data pribadinya sehingga tidak akan disebarluaskan kepada pihak lain tanpa seizinnya.[10]

Artikel ini sebagai hasil dari penelitian yang telah dilakukan pada tahun 2015 dengan judul Penerapan Program *E-health* Dihubungkan dengan Perlindungan Data Privasi di Indonesia atas dana penelitian UNPAD.

Pada tahun 2016 Moody Rizky Syailendra, Mahasiswa Program S1, Fakultas Hukum Unpad menulis tentang Perlindungan Data Pribadi Terkait Program *E-health* di Indonesia. Penelitian saudara Moody lebih menitik beratkan pada program *E-Health* Nasional sedangkan tulisan ini memaparkan pengaruh instrumen internasional dalam melindungi data pribadi dan bagaimana implikasi program *E-health* terhadap perlindungan data pribadi. Metode penelitian yang digunakan adalah Metode yang digunakan dalam penelitian ini berupa pendekatan juridis normatif dengan spesifikasi bersifat deskriptif analitis. Proses pengumpulan data dilakukan melalui penelitian kepustakaan dan penelitian lapangan dan tahap penelitian kepustakaan dilakukan untuk mencari data sekunder dengan menggunakan bahan hukum primer, sekunder, dan tertier. Dalam tahap ini juga dilakukan tinjauan kepustakaan terhadap sejumlah instrumen internasional yang mengatur perlindungan privasi atas data pribadi yang telah merupakan *international global standards* sehingga diadopsi oleh banyak negara-negara dalam menyusun undang-undang perlindungan data pribadi.

Pembahasan

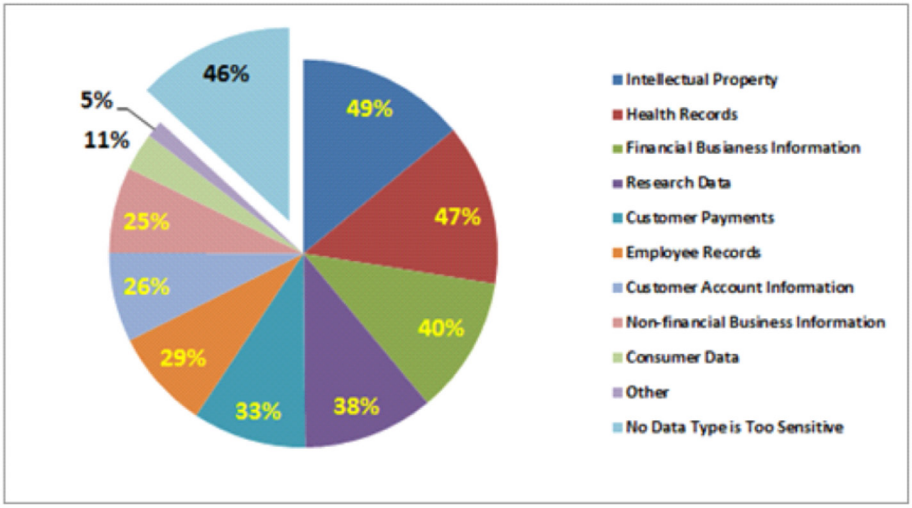
Perkembangan praktik di negara lain telah menunjukkan bahwa telah terjadi banyak kasus pelanggaran data pribadi pasien sehingga telah merugikan pasien karena privasinya telah dilanggar, sebagai berikut:

Data statistik pada Gambar 1. telah menujukan tingkat pelanggaran yang sangat tinggi atas data kesehatan masyarakat yang dapat diakses dan disalahgunakan oleh pihak lain.

Data statistik pada Gambar 2. telah menujukan tingkat pelanggaran yang sangat tinggi atas data kesehatan masyarakat yang dapat diakses dan disalahgunakan oleh pihak lain. Di Indonesia, permasalahan hukum akan timbul mengingat belum ada belum

10 Kementrian Pendayagunaan Aparatur Negara, *Harmonisasi dan Sinkronisasi Konsepsi Hukum Perlindungan Data dan Data Pribadi*, (Jakarta: November, 2007), hlm. 2-5.

Gambar 1. Data Statistik tentang Pelanggaran Privasi yang Terjadi dalam Berbagai Sektor

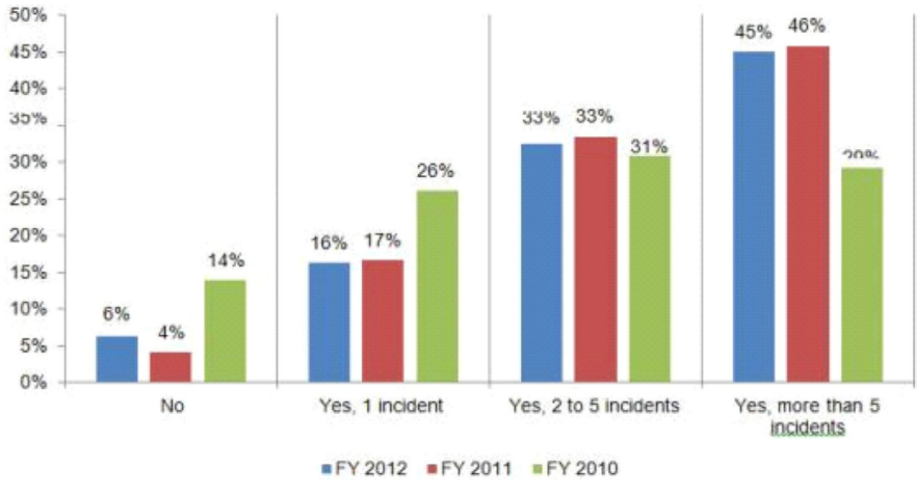


Sumber: entreprisefeature.com

ada regulasi yang memadai yang mengatur perlindungan privasi atas data pribadi pasien yang merupakan data pribadi senditif karena dikhawatirkan data pribadi pasien akan dikompilasi, diakses dan disebarluaskan kepada pihak lain tanpa sepengetahuan dan persetujuan pasien sendiri. Contohnya dapat dimanfaatkan secara ekonomi oleh indutri penyedia jasa lainnya seperti industri obat-obatan, industri asuransi sehingga akan terjadi yang disebut dengan *direct selling*. Pemasaran langsung merupakan salah satu cara pemasaran dengan melakukan promosi langsung atau dikenal dengan *targeted advertisement.*

Konsep perlindungan data sering dipersepsikan sebagai bagian dari perlindungan privasi. Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Allan Westin yang untuk pertamakalinya mendefinisikan privasi sebagai hak individu, grup atau lembaga untuk menentukan

Gambar 2. Tingkat Pelanggaran Privasi dalam Informasi Jasa Kesehatan



Sumber: entreprisefeature.com

apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan *information privacy* karena menyangkut informasi pribadi.[11]

Pengaturan data pribadi muncul sebagai suatu hak individu untuk menentukan apakah mereka akan membagi atau bertukar data pribadu mereka atau tidak. Selain itu individu juga memiliki hak untuk menentukan syarat-syarat pelaksanaan pemindahan data pribadi tersebut. Salah satu prinsip pengaturan data pribadi di negara-negara Eropa adalah pengaturan arus keluar masuk arus data pribadi antar negara dan melarang data pribadi keluar negara-negara Eropa apabila negara ketiga belum memiliki undang-undang yang setara (*adequacy*) dengan negara-negara Eropa sehingga dikhawatirkan akan menghambat perdagangan dan bisnis internasional yang sudah mengglobal. Untuk menghindari hal tersebut maka OECD ((*The Organization for Economic and Cooperation Development)* mengeluarkan suatu *Guidelines* yang dikenal dengan *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[12]

A. OECD Guidelines 1980

Tujuan utama *Guidelines* 1980 menyatakan bahwa "negara-negara anggota dianggap perlu untuk mengembangkan suatu pedoman yang akan membantu untuk menyelaraskan undang-undang perlindungan data pribadi negara anggota OECD dengan tetap menjunjung tinggi hak asasi manusia, yang secara bersamaan juga mencegah terjadinya hambatan perdagangan internasional dalam hal ini keluar dan masuknya data pribadi secara lintas batas.[13] Guidelines menghasilkan prinsip-prinsip dasar perlindungan data sehingga dapat membantu pemerintah, pengusaha, dan perwakilan konsumen dalam upaya untuk melindungi privasi atas data pribadi dan menghindarkan hambatan perdagangan yang tidak perlu untuk aliran data pribadi lintas-batas baik online maupun offline. prinsip-prinsip perlindungan tersebut yaitu[14]

1. **Prinsip pengumpulan batasan (*collection limitation principle*)**

Harus ada batas untuk mengumpulkan data pribadi dan data tersebut harus diperoleh dengan cara yang sah serta adil dan, bila perlu, dengan sepengetahuan atau persetujuan dari subyek data.

2. **Prinsip kualitas data (*data quality principle*)**

Data pribadi harus sesuai dengan tujuan penggunaannya dan, untuk tujuan yang diperlukan, data harus akurat, lengkap, dan terus diperbaharui.

---

11 Menurut Alan Westin, *Privacy is the claim of individuals, group or institution to determine for themselves when, how, and to what extent information about them is communicated to others* dalam, Allan Westin, Alan F. Westin, *Privacy and Freedom*, (New York: Atheneum, 1970), p. 7.

12 Ian J. Llyod, *Information Technology Law*, (United Kingdom: Oxford University Pers, 2014), p. 31.

13 Abu Bakar Munir, Siti Hajar Mohd Yasin dan Md. Ershadul Karim, *Data Protection Law in Asia*, (Hong Kong, Thompson Reuters Limited), pp. 34-35.

14 Lihat OECD Guidelines 1980.

3. Prinsip tujuan khusus (*purpose specification principle*)

Tujuan untuk mana data pribadi tersebut dikumpulkan harus ditentukan selambat-lambatnya pada saat pengumpulan data dan penggunaan selanjutnya terbatas pada pemenuhan tujuan tersebut atau yang lainnya tidak bertentangan dengan tujuan-tujuan dan sebagaimana ditentukan pada setiap kesempatan adanya perubahan tujuan.

4. Prinsip batasan pengunaan (*use limitation principle*)

Data pribadi tidak boleh diungkapkan, disediakan, atau digunakan untuk tujuan selain yang ditentukan kecuali:

1. Dengan persetujuan subjek data
2. Berdasarkan hukum

5. Prinsip perlindungan keamanan (*security safeguard principle*)

Data pribadi harus dilindungi dengan perlindungan dan keamanan yang wajar terhadap risiko seperti kehilangan data atau akses yang tidak sah, perusakan, penggunaan, modifikasi, atau pengungkapan data.

6. Prinsip keterbukaan (*openness principle*)

Harus ada kebijakan umum tentang keterbukaan terhadap pengembangan, praktik, dan kebijakan yang berkenaan dengan data pribadi. Artinya harus dibangun eksistensi dan sifat alami data pribadi, dan tujuan utama penggunaannya, serta identitas dan tempat tinggal pengontrol data.

g. Prinsip Partisipasi Individu (*Individual Participation Principle*)

Setiap individu harus memiliki hak:

a. untuk memperoleh data dari pengendali data, atau sebaliknya,
b. mengkonfirmasi apakah pengendali data memiliki data yang berkaitan dengannya;
c. untuk disampaikan kepadanya, data yang berkaitan dengannya dalam waktu yang wajar, tidak berlebihan, dengan cara yang wajar, dan dalam bentuk yang mudah dimengerti.
d. untuk memperoleh alasan jika terdapat permintaan berdasarkan sub-paragraf (a) dan (b) ditolak, dan hak untuk dapat mengajukan keberatan atas penolakan tersebut.
e. untuk menentang data yang berkaitan dengannya dan, jika keberatan tersebut berhasil, untuk memiliki data yang terhapus, diperbaiki, selesai, atau diubah.
f. Prinsip Akuntabilitas (*Accountability Principle*)

Pengendali data harus bertanggung jawab untuk mematuhi semua tindakan yang akan memberikan efek terhadap prinsip-prinsip tersebut di atas.

B. APEC *Privacy Framework*

Kawasan Asia Pasifik bekerja sama pada isu-isu privasi dengan *Asia Pacific Economic Cooperation Privasi (APEC) Framework* tahun 2004. Pentingnya melindungi informasi pribadi dan data dapat ditemukan dalam pembukaan dari *Framework Privacy APEC 2004* yang menyebutkan bahwa potensi perdagangan elektronik tidak dapat diwujudkan tanpa kerjasama antara pemerintah dan pelaku bisnis. Sebagai

lembaga kerjasama internasional, APEC telah membutuhkan perlindungan sejak awal untuk mengatasi masalah privasi dan perlindungan data karena berhubungan dengan masalah ekonomi. Untuk mengatasi masalah ini, APEC telah mengembangkan prinsip pendekatan yang bertujuan untuk menyelaraskan hukum sebanyak mungkin dengan prinsip yang sudah dikembangkan secara internasional. Dengan demikian, *Framework Privacy APEC* dapat berfungsi sebagai titik badan penegakan privasi independen (atau badan antar-agensi) sebagai titik kontak untuk perekonomian lain dan memberikan badan penegak hukum kemampuan untuk bekerja sama dengan badan penegakan badan di negara lain.

Peran Kerangka Privasi APEC 2004 adalah untuk menyeimbangkan informasi dan mempromosikan perlindungan privasi yang efektif dan arus informasi yang bebas. Kerangka privasi APEC berisi sembilan prinsip:[15]

a. Mencegah dampak buruk: Suatu prinsip yang dirancang untuk mencegah penyalahgunaan informasi.
b. Pemberitahuan: Dimaksudkan untuk memastikan bahwa individu dapat mengetahui informasi apa yang dikumpulkan tentang mereka dan untuk tujuan apa.
c. Batas Pengumpulan: Pengumpulan informasi pribadi yang relevan dengan tujuan pengumpulan.
d. Penggunaan Informasi Pribadi: Informasi pribadi harus digunakan hanya untuk memenuhi tujuan pengumpulan dan tujuan lain yang terkait.
e. Pilihan: Prinsip ini adalah untuk memastikan bahwa individu diberi pilihan dalam kaitannya dengan pengumpulan, penggunaan, transfer, dan pengungkapan informasi pribadi mereka.
f. Integritas Informasi Pribadi: Informasi pribadi harus akurat, lengkap, dan selalu diperbaharui sejauh yang diperlukan.
g. Perlindungan keamanan: Prinsip ini mengakui bahwa orang yang mempercayakan informasi mereka kepada pihak lain berhak untuk mengharapkan bahwa informasi mereka dilindungi dengan keamanan yang wajar.
h. Akses dan Koreksi: Individu memiliki kemampuan untuk mengakses dan memperbaiki informasi pribadi mereka.
i. Akses dan Koreksi: Individu memiliki kemampuan untuk mengakses dan memperbaiki informasi pribadi mereka.

Anggota APEC tidak diwajibkan untuk melaksanakan Kerangka privasi APEC di dalam negeri dengan cara tertentu. Karena, ada situasi dan kondisi yang berbeda yang berlaku dalam menangani perlindungan privasi dan data di antara anggota APEC. Tidak ada peraturan yang harus diselaraskan antara anggota APEC.

15 Apec Privacy Framework, lihat juga Graham Greenleaf, *Asian Data Privacy Laws, Trade and Human Rights Perspectives,* (United Kingdom: Oxford University Press, 2014), pp. 33.

C. Program E-health dan Potensi Pelanggaran Data Pribadi Pasien

Program e-health merupakan salah satu bentuk pengembangan e-government yang telah diamanatkan oleh pemerintah melalui instruksi Presiden No.3 Tahun 2003 tentang kebijakan dan Strategi Nasional yang merupakan upaya pemerintah dalam meningkatkan kualitas layanan publik secara efektif dan efisien.[16] Salah satu contoh program e-health yaitu:[17]

a. *Individual electronic health information* yaitu penyedia jasa akan memberikan pelayanan penyimpanan dan pengelolaan informasi kesehatan seseorang contohnya program Personal health record (PHR), electronic health record (EHR), Electronic medical record (EMR);
b. *Healthcare service delivery tools* yaitu penyedia jasa kesehatan memberikan pelayanan diagnosis dan memberikan pelayanan kesehatan kepada seseorang melalui elektronik contohnya *realtime clinical data access* and *analysis, clinical decision support*;
c. *Healthcare management and administration* yaitu penyedia jasa memberikan pelayanan jasa kesehatan secara komprehensif dari mulai informasi kesehatan, pengobatan, pengawasan dan tindakan.

Dalam program e-health, rekam kesehatan elektronik (RKE) atau *Electronic Health Record* (EHR) merupakan media yang utama dalam sistem informasi rumah sakit untuk memberikan pengobatan yang leih cepat dan efektif bagi pasien. RKE memuat data kondisi kesehatan pasien yang sangat bersifat pribadi yang tersimpan dalam sistem komputer dan memungkinkan antar dokter dan penyedia layanan kesehatan untuk dapat mengakses dan saling bertukar infomasi dengan menggunakan aplikasi berbasis web dalam memberikan pelayanan terhadap pasien. Data yang terdapat dalam RKE meliputi data demografi, riwayat medis, pengobatan, hasil uji Data tersebut meliputi data demografi, riwayat medis, pengobatan, hasil uji laboratorium dan radiologi, proses keperawatan, discharge planning dan bahkan informasi penagihan. Data pasien dapat diakses langsung, pasien dapat dilacak dengan mudah dan memberikan perlindungan yang dapat membantu mencegah kesalahan medis.[18] Adapun jenis data rekam medis elektronik dapat berupa teks baik yang terstruktur maupun naratif, gambar digital, suara, video maupun berupa bisignal seperti rekaman EKG.[19]

---

16 Nur Mas Ammah dan Eva Hany Fanida, Penerapan Layanan *Electronic Health (E-health)* di Puskesmas Kecamatan Genteng Kota Surabaya, 2014, hlm. 1-2.

17 Anis Fuad, "Perkembangan *e-health* Global: Bagaimana di Indonesia", http://www.scribd.com/doc/178823999/Perkembangan-e-health-global-bagaimana-di-Indonesia#scribd, diakses 10 Agustus 2016.

18 Sunardi, "Sistem Electronic Medical record dalam Pelayanan Kesehatan di Rumah Sakit", http://www.kompasiana.com/sunardinadhif/sistem-electronik-medical-record-dalam-pelayanan-kesehatan-di-rumah-sakit, 2015, hlm. 1-2, diakses 10 Oktober 2016.

19 *Ibid*.

Ada beberapa persoalan hukum yang muncul antara lain:

Pertama, konsumen kurang memahami dinamika pengumpulan informasi pribadi. Mereka memiliki rasa mengganggu samar-samar bahwa informasi adalah "di luar sana" tentang mereka - tetapi tidak harus bagaimana sampai di sana dan apa yang bisa dilakukan dengan itu. Mereka tahu, misalnya, teknologi yang berperan dalam mengumpulkan, menyimpan dan menyebarkan informasi pribadi, tapi tidak khusus.

Kedua, konsumen frustrasi oleh kurangnya kontrol mereka memiliki lebih dari penggunaan informasi pribadi mereka. "Junk mail" adalah antara lima topik teratas tahun keluhan demi tahun.

Ketiga: Ada banyak kesalahpahaman tentang hukum dan peraturan perlindungan privasi yang ada. Kebanyakan konsumen berpikir ada undang-undang privasi jauh lebih dan peraturan daripada benar-benar ada.

Keempat: Banyak kasus terburuk dari kekerasan privasi kami telah mendengar tentang hotline adalah hasil dari kesalahan, kecerobohan dan penilaian buruk oleh orang-orang yang menangani informasi pribadi. Dan beberapa hasil keamanan yang tidak memadai dalam penanganan informasi pribadi.

1. Aspek privasi atas data pribadi dalam program *e-health*

Dalam memberikan pelayanan maka pihak penyedia layanan kesehatan akan mengumpulkan, menyimpan, mengirimkan dan menggunakan informasi medis pasien yang merupakan data pribadi pasien meliputi dokumen, catatan, spesimen patologi dan diagnostik tanpa sepengetahuan pasien. Penggunaan TIK dengan memungkinkan data pribadi pasien diakses dan diolah dalam jumlah yang besar dan dalam waktu yang sangat cepat sehingga bila tidak diikuti oleh pengaturan yang khusus akan melanggar privasi atas data pribadi pasien yang merupakan data yang bersifat sensitif sehingga memerlukan perlindungan hukum yang khusus. Alasan mengapa informasi medis sangat penting untuk dilindungi adalah seringkali data pribadi pasien diperjual belikan atau diungkap untuk keperluan asuransi, kesempatan kerja, mendapatkan program bantuan pemerintah tanpa sepengetahuan pasien.

2. Pengertian data pribadi

Beberapa instrumen internasional seperti OECD *Guidelines* maupun *Data Protection Convention* dari Dewan Eropa data pribadi diartikan semua informasi yang berhubungan dengan orang-perorangan yang teridentifikasi dan dapat diindetifikasi (*"information relating to an identified or identifiable natural person*").[20] Definisi data pribadi tersebut di atas sangat luas mengingat pesatnta perkembangan TIK dikhawatirkan apabila dirinci secara limitatif tidak bisa mengikuti perkembangan jaman akibatnya masih banyak terjadi perdebatan mengingat masing masing

20 OECD Guidelines, 1980.

negara berbeda dalam mengkategorikan data pribadi.

Di negara-negara yang telah memiliki undang-undang Perlindungan Data Pribadi menyerahkan kepada Lembaga perlindungan data untuk memberikan penafsiran tentang kategori data pribadi yang akan diatur oleh undang-undangnya.[21]

Sebagai contoh beberapa undang-undang nasional mencoba mengkategorikan data pribadi antara lain: nama, alamat, alamat email, nomor telefon, no identitas penduduk yang kemudian dikombinasikan dengan informasi yang ada di register publik sehingga dapat mengidentikasikan seseorang.[22] Dalam program *E-health* biasanya data pribadi yang dilidungi adalah yang disebut dengan *unique identifier* seperti nama lengkap, *account number,* penyedia jasa karena dapat menindentifikasi seorang pasien, data demografi seperti alamat, nomor telepon, alamat email yang biasanya digabung dengan usia, jenis kelamin. Selain itu data pribadi yang harus dilindungi karena dapat mengidentifikasi seseorang adalah kondisi medis seseorang seperti tingkat alergi, kebiasaan merokok/minum beralkohol termasuk data kunjungan baik ke rumah sakit maupun dokter termasuk hasil diagnostik, pengobatan yang telah dilakukan, obat-obatan yang digunakan. Kemudian informasi tentang pembayaran pasien serta asuransi yang digunakan juga dapat merujuk pada identifikasi seseorang. Termasuk yang yang dilindungi adalah data pribadi pasien yang dikirimkan baik menggunakan media biasa maupun media elektronik contohnya di Amerika Serikat dalam HIPAA (*The Health Insurance Portability and Accountability Act*) data pembicaraan antara pasien dan dokter harus dilindungi seperti hanya data dalam bentuk kertas.[23]

Salah satu perdebatan tentang alamat IP (IP *Adresses)* apakah dapat dikategorikan sebagai data pribadi atau bukan. Google beranggapan bahwa masalah ini tidak pernah pasti, karena terkadang alamat IP bisa dianggap sebagai data pribadi dan terkadang tidak. Sementara pihak lain, termasuk para ahli perlindungan data berpendapat bahwa alamat IP harus dianggap sebagai data pribadi. Di Bulan November 2011, *European Court of Justice* juga menyatakan bahwa alamat IP adalah data pribadi.[24]

Alamat IP dapat membantu mengindentifikasikan pengguna di internet (atau setidaknya komputer mereka) dan memungkinkan data untuk diterima oleh

21 Mark F. Kightlinger, E. Jason Albert, and Daniel P. Cooper, *International Privacy*, Chapter 10, (United Kingdom: Privacy International, 2002), p. 121.

22 Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981. Pasal 2.

23 Lihat HIPAA (The Health Insurance Portability and Accountability Act), 2003, Pasal 1.

24 Van Bael & Bellis, European Union: ECJ Confirms That IP Address Are Peronal Data, http://www.mondaq.com/x/162538/Copyright/ECJ+Confirms+That+IP+Addresses+Are+Personal+Data, hlm. 1, diakses 10 September 2016.

mereka sehingga dengan demikian alamat IP dapat dianggap sebagai data pribadi. Namun demikian, alamat IP juga dapat berganti sangat cepat dikarenakan ISPs seringkali memiliki alamat IP yang lebih sedikit dari pelanggan dan selalu mewajibkan pelanggan untuk selalu mendaftar ketika akan menyalakan atau mematikan koneksi. Beberapa perusahaan internet telah berusaha untuk mengurangi resiko dimungkinkannya pengguna teridentifikasi dengan menggunakan alamat IP tanpa nama. Namun demikian, penggunaan media sosial seperti blog, twitter, dan jasa web lainnya semakin meningkatkan kemungkinan teridentifikasinya data-data yang tanpa nama tersebut [25]

3. Data pribadi sensitif

Dalam hukum perlindungan data pribadi ada yang membedakan antara data pribadi yang umum (*general*) dan sensitif (*sensitive*) berdasarkan sejauhmana pengungkapannya akan membahayakan pemilik data apabila pengolahan data tersebut tanpa persetujuan. Data 'sensitif' biasanya mendapatkan perlindungan hukum yang lebih besar[26]. Di Uni Eopa yang diatur dalam *European Data Protection Directive* melarang pengolahan data sensitif kecuali jika telah mendapatkan persetujuan yang jelas dari pemilik data. *Directive* menentukan data pribadi yang sensitif dalam daftar yang rigid yang terdiri dari: Data data yang menyangkut etnisitas, pendapat politik, agama dan kepercayaan, keanggotaan dari organisasi perdagangan termasuk juga data yang berhubungan dengan kesehatan fisik dan mental seseorang serta kehidupan seks seseorang.[27] Mengingat data kesehatan pasien dikategorikan dalam data yang sensitif sehingga dalam penerpan program *E-health* perlindungan privasi atas data pribadi pasien harus benar-benar diperhatikan, contohnya seperti yang terjadi di Kanada yang menerapkan persyaratan yang ketat mengenai pengolahan data yang sensitif, namun tidak seperti *Directive*, hukum ini tidak memiliki daftar kategori yang rigid.[28] Pendekatan yang diambil di Kanada yang menentukan bahwa organisasi perdagangan sebelum mengakses atau mengolah data pribadi yang sensitif harus mendapatkan persetujuan yang nyata (*opt-in*) dari pemilik data. Sifat dari pengamanan yang diperlukan sangat tergantung dari sensifitas informasi yang telah dikumpulkan tersebut, jumlah distribusi dan format serta penyimpanan dari informasi tersebut. Semakin sensitif suatu informasi, maka penjagaannya harus dilakukan dengan perlindungan tingkat tinggi.[29]

---

25 Ian. J. Lloyd, *op.cit*., pp. 44-45.

26 Mark F. Kightlinger, E. Jason Albert, and Daniel P. Cooper, *op.cit*., pp. 130.

27 *Ibid*.

28 Ian J. Lyod, *op.cit*., p. 42.

29 James Waldo, Herbert S. Lin, Lynette, *Enganging Privacy And Information Technology in Digital Age*, (Washington D.C: National Academies Press, 2007), p. 210.

4. Pihak-pihak yang dapat memanfaatkan data pribadi kesehatan

Banyak pihak yang dapat mengakses data pribadi untuk kepentingan bisnis antara lain: Pihak Asuransi merupakan pihak yang banyak memanfaatkan data medis pasien untuk kepentingan bisnisnya biasanya pada awal penerimaan konsumen baru mereka meminta data medis pasien untuk mengikuti program asuransi baru; Apotik memiliki data medis pasien terutama obat-obat yang dipakai dalam data base mereka dan apabila diungkap kepada pihak lain dapat mengindetifasi seseorang; Instansi pemerintah terutama di negara-negara yang telah maju seringkali meminta catatan medis seseorang biasanya untuk menverifikasi klaim medis, jaminan sosial dan menerima kompensasi pekerja; lembaga pendidikan juga seringkali memiliki catatan kesehatan murid-muridnya seperti riwayat vaksin murid, informasi tentang pemeriksaan fisik dan mental ketika masuk suatu lembaga pendidikan, konseling yang telah dilakukan yang akan memuat informasi tentang perilaku seseorang termasuk kesehatan mental seseorang.

5. Kewajiban penyelenggara jasa kesehatan

Sistem pengamanan data pribadi pasien harus menerapkan suatu risk assesment yang biasanya memberikan informasi kepada pasien:

a. seberapa jauh informasi data pribadi pasien dilindungi dan adakah kemungkinan data pribadi pasien di identifikasi ulang atau *reindefication*;

b. mengetahui rang yang tidak sah yang menggunakan informasi kesehatan dilindungi atau kepada siapa pengungkapan itu dibuat;

c. Apakah informasi kesehatan yang dilindungi telah diperoleh atau dilihat oleh orang lain;

d. sejauh mana resiko yang telah dilindungi dialihkan/mitigasi.

Apabila terbukti telah terjadi kebocoran data pribadi pasien maka penyedia layanan kesehatan khususnya dalam program e-health harus menempuh beberapa langkah yaitu:[30]

a. harus memberitahukan secara tertulis kepada pasien menyusul penemuan pelanggaran informasi atas data pribadi pasien kesehatan dilindungi;

b. mekanisme lainnya yaitu melalui media cetak dan elektronik sehingga masyarakat mengetahui khususnya bila terjadi kebocoran yang masif.[31]

c. pihak penyedia layanan kesehatan harus memberi tahu kepada institusi yang langsung menangani kesehatan misalnya Kementerian Kesehatan atau badan lain yang

30 US Department of Health and Human Services, "Breach Notification Notices", http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, p. 1, diakses 20 Oktober 2016. Pada tahun 2009, Kementerian Kesehatan Amerika Serikat telah mengeluarkan pengumumam bahwa telah terjadi bebocoran 500 data pasien dari sistem e-health, tindakan ini adalah menerapkan prinsip data breach notification seperti yang dikutip dalam "Beraches Affecting 500 or more Individuals", https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, hlm. 1-2, diakses 21 Oktober 2016.

31 *Ibid*.

mengawasi penerapan privasi atas data pribadi contohnya Data *Privacy Agency*/DPA.

d. Pihak penyedia jasa kesehatan wajib memberitahu asosiasi bisnis sehingga dapat mengambil tindakan pengamanan sehingga dapat memperbaiki sistem yang ada.

6. Prinsip-prinsip perlindungan privasi atas data pribadi dalam program *E-health*

Dalam melindungi privasi atas data pribadi pasien yang diatur secara khusus adalah bagaimana data medis pasien dikumpulkan dan diproses dalam suatu data base sehingga tidak dapat diungkapkan atau disebar luaskan tanpa sepengetahuan pasien. Melihat praktek negara-negara yang telah sebaiknya diatur dalam suatu undang-undang yang khusus yang memuat prinsip-prinsip perlindungan khususnya ada syarat yaitu data medis pasien tidak dapat dikumpulkan tanpa persetujuan pasien dan pengumpulan serta pemrosesan data harus sesuai tujuan awal. Contohnya apabila data medis dikumpulkan dan diproses untuk kepentingan pengobatan di rumah sakit maka setelah pengobatan selesai tidak boleh digunakan oleh perusahaan asuransi atau pabrik obat. prinsip lainnya pasien harus mengetahui tujuan pengumpulan data pribadi. Prinsip selanjutnya adalah jaminan dari penyedia jasa kesehatan untuk menjamin keamanan sistemnya sehingga tidak ada kehilangan, kebocoran data, pencurian data, serta akses illegal atas data medis yang disimpannya.

Prinsip-Prinsip perlindungan privasi atas data pribadi dalam program e-health yang paling utama antara lain:

a. Prinsip Kesepakatan pasien sebagai pemilik data kesehatan kecuali:

1) adanya izin secara tertulis dari pasien sebagai pemilik data;

2) adanya perintah dari undang-undang

3) untuk kepentingan pasien sendiri;

b. Prinsip Tujuan yang spesifik: tujuan mengapa ta itu dikumpulkan dan setiap panggunaan selanjutnya harus terbatas sesuai dengan spesifikasi tujuan tersebut;

c. Prinsip Keamanan: pengguna data diharuskan mengambil langkah-langkah yang perlu guna menjaga keamanan data tersebut. Pihak penyimpan data wajib melindungi dengan metode apapun dari gangguan pihak lain;

d. Prinsip Retensi, rinsip ini mengatur mengenai jangka waktu suatu data dapat dimusnahkan. Jika data tersebut sudah digunakan sesuai dengan tujuannya, data tersebut harus segera dimusnahkan.

7. Prinsip keamanan data pribadi pasien

Selain harus melindungi privasi atas data pribadi pasien, penyelenggaran juga harus menerapkan standar keamanan data pribadi dalam sistemnya antara lain:

a. harus menyediakan mekanisme akses kontrol seperti password dan nomor PIN, untuk membantu membatasi akses pada data pribadi pasien sehingga pasien memiliki kontral atas informasi data pribadinya;

b. menggunakan enkripsi untuk menyimpan data pribadi pasien sehingga

informasi atas data pribadi pasien tidak dapat diakses oleh pihak lain.

c. menerapkan sebuah audit yang dapat mencatat siapa siapa saja yang mengakses informasi data kesehatan.[32]

8. Privasi dan perlindungan data pribadi pasien dia Indonesia

Terkait perlindungan data pribadi, Indonesia telah mengatur dalam Undang-undang Nomor 11 Tahun 2008 yaitu Undang-undang Informasi dan Transaksi Elektronik dalam Pasal 26 ayat (1) UU ITE telah mengatur bahwa:

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap infromasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan

Terhadap pihak yang dirugikan atas dilanggarnya ketentuan tersebut, dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan ketentuan ayat (2) pasal tersebut.[33]

Kemudian dalam Peraturan Pemerintah No 82 Tahun 2002 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, data pribadi diatur dalam Pasal 15 yang mengatur tanggung jawab penyelenggara sistem elektronik yang wajib menjaga rahasia, keutuhan dan ketersediaan data pribadi yang dikelolanya dan wajib menjamin bahwa perolehan, penggunaan dan pemanfaatan data pribadi harus berdasarkan persetujuan pemilik data pribadi serta penggunaan data pribadi tersebut harus sesuai dengan tujuan pengumpulan data. Juga terjadi kegagalan dalam perlindungan data pribadi maka pemilik data pribadi dapat memberitahukan kepada penyelenggara sistem elekronik.Terkait dengan perlindungan rekam medis data pribadi pasien telah undang-undang Nomor 29 tahun 2004 tentang praktik kedokteran telah mengatur secara sekilas mengenai perlindungan rekam medis milik pasien. Pasal 47 ayat (2) undang-undang ini mengatakan:

> "Rekam medis sebagaimana dimaksud pada ayat (1) harus disimpan dan dijaga kerahasiannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan."

Dokter atau dokter gigi memiliki kewajiban untuk menyimpan, menjaga, dan melindungi segala informasi yang diketahuinya mengenai pasiennya. Hal ini seperti yang telah diatur di dalam Pasal 57 Huruf (c) undang-undang praktik kedokteran, yang berbunyi:

> ….merahasiakan segala sesuatu yang diketahuinya tentang pasien, bahkan juga setelah pasien itu meninggal dunia."

Masalah bocornya data pasien diatu Pasal 79 butir (c) Undang-undang Praktik Kedokteran yang berbunyi:

> "Dipidana dengan pidana kurungan paling lama 1 (satu) tahun atau denda

32 *Ibid*.

33 Pasal 26 ayat (2) UU ITE: (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini.

> paling banyak Rp. 50.000.000,00 (lima puluh juta rupiah), setiap dokter atau dokter gigi yang:
>
> …. dengan sengaja tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 51 huruf a, huruf b, huruf c, huruf d, atau huruf e."

Undang-undang Nomor 36 Tahun 2009 tentang Kesehatan juga mengatur tentang kerahasiaan kondisi kesehatan yaitu dalam 57:

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

Simpulan

Program *e-health* sangat diperlukan di Indonesia mengingat belum meratanya pemberian layanan kesehatan baik oleh pemerintah maupun swasta dikarenakan kendala wilayah Indonesia yang tersebar di berbagai propinsi sehingga program *e-health* dapat menyediakan jasa pelayanan yang lebih efisien karena melalui TIK dapat menjangkau daerah terpencil dan masyarakat dapat menikmati pelayanan kesehatan secara efisien dan efektif. Tetapi dalam konteks perlindungan privasi atas data pribadi pasien belum sepenuhnya terjamin karena belum pahamnya masyarakat Indonesia akan hak nya dan belum merata pemahaman baik pihak pemerintah akan pentingnya perlindungan data pribadi pasien sehingga diperlukan pengaturan yang khusus tentang perlindungan data pribadi pasien dalam program *e-health* walaupun telah diatur di dalam beberapa undang-undang, Peraturan Pemerintah maupun Peraturan Menteri seperti dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran, Undang-undang Nomor 36 Tahun 2009 tentang Kesehatan, Peraturan Menteri Kesehatan Nomor 269/ Menkes/Per/III/2008, Peraturan Pemerintah No 82 Tahun 2002 tentang Penyelenggaraan Sistem dan Transaksi Elektronik namun pengaturannya sangat umum dan belum menerapkan prinsip-prinsip perlindungan data pribadi yang spesifik sehingga belum dapat memberikan perlindungan yang maksimal dan akibatnya masih adanya data pribadi atau rekam medis milik pasien yang dapat dengan mudah diakses oleh pihak lain tanpa adanya persetujuan dengan pemilik data yang bersangkutan.

DAFTAR PUSTAKA

Buku

Baylish, John & Steve Smith. *The Globalization of World Politics, An Introduction to International Relations*. New York: Oxford University Press, 2001.

Llyod, J. Ian. *Information Technology Law.* United Kingdom: Oxford University Press, 2014.

Makarim, Edmon. Kompilasi Hukum Telematika. Jakarta: RajaGrafindo Perkasa, 2003.

Murray, Andrew. *Information Technology Law, The Law and Society.* New York: Oxford University Press, 2010.

Munir, Abu Bakar, dkk. *Thompson Reuters Hong Kong Limited*. Hong Kong: Sweet & Maxwell, 2014.

Sanusi, M. Arsyah. *Teknologi Informasi & Hukum E-commerce*. Jakarta: Dian Ariesta, 2004.

Waldo, James dkk. *Enganging Privacy And Information Technology in Digital Age.* Washington D.C: National Academies Press, 2007.

Westin, F, Alan. *Privacy and Freedom*. New York: Atheneum, 1970.

Jurnal

Branscomb, Anne W. "Global Governance of Global Networks: "A survey of Transborder Data Flows in Transition". *Vanderbilt Law Review*, *Vol. 36*, (1983): 985.

Laporan

Kofi A. Anan. Dalam *UNCTAD E-commerce and Development Report*. New York: UNCTAD, 2004.

Kightlinger, Mark F. dkk. *International Privacy.* Chapter 10. United Kingdom: Privacy International, 2002.

Paper

Kementrian Pendayagunaan Aparatur Negara. "Harmonisasi dan Sinkronisasi Konsepsi Hukum Perlindungan Data dan Data pribadi". Jakarta: (November 2007): 2-5.

Ammah, Nur Mas dan Eva Hany Fanida. *Penerapan Layanan Electronic Health (E-health) di Puskesmas Kecamatan Genteng Kota Surabaya*. (2014): 1-2.

Peraturan Perundang-undangan

OECD Guideline, 1980.

Konvensi Eropa tentang Convention for the Protection of Individuals with regard to the processing of Personal Data 1981.

HIPAA (The Health Insurance Portability and Accountability Act), 2003.

Naskah Internet

Fuad, Anis. "Perkembangan e-health Global: Bagaimana di Indonesia". http://www.scribd.com/doc/178823999/Perkembangan-e-health-global-bagaimana-di-Indonesia#scribd. Diakses 10 Agustus 2016.

Utama, Putra Setia. http://ehealthindonesia.com/content/telemedika-e-health-aplikasinya-di-indonesia-butuh-kerjasama-multidisipliner. Diakses 10 Maret 2014.

Telkom. "Peran Teknologi Informasi ICT dalam Bidang Kesehatan dan Pengobatan". http://ehealthindonesia.com/content/peran-teknologi-informasi-ict-dalam-bidang-kesehatan-dan-pengobatan. Diakses 10 Maret 2014.

_____. "Proyek E Health Telkom Jalan Terus". http://ehealthindonesia.com/content/proyek-ehealth-telkom-jalan-terus. Diakses12 Maret 2014.

Sunardi. "Sistem Electronic Medical record dalam Pelayanan Kesehatan di Rumah Sakit". http://www.kompasiana.com/sunardinadhif/sistem-electronik-medical-record-dalam-pelayanan-kesehatan-di-rumah-sakit. Diakses 10 Oktober 2016.

Bael, Van & Bellis. "European Union: ECJ Confirms That IP Address Are Peronal Data". http://www.mondaq.com/x/162538/Copyright/ECJ+Confirm+That+IP+Are+Personal. Diakses 10 September 2016.

Privacy Right Clearing House. "Protecting Health Information: The HIPAA Security and Breach Notification Rules". https://www.privacyrights.org/printpdf/67499. Diakses 2016.

US Department of Health and Human Services/ Breach Notification Notices. http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Diakses 21 Oktober 2016.