LITERATUR *REVIEW* PERMASALAHAN PRIVASI PADA REKAM MEDIS ELEKTRONIK

Annisa Maulida Ningtyas[1], Ismil Khairi Lubis[2]
[1,2] Rekam Medis dan Informasi Kesehatan/Departemen Layanan dan Informasi Kesehatan,
Sekolah Vokasi, Universitas Gadjah Mada,
Gedung SV UGM, Sekip Unit 1, Blimbing Sari, Caturtunggal, Kec. Depok, Kabupaten Sleman,
Daerah Istimewa Yogyakarta 55281 (0274) 541020

[1]annisamaulidaningtyas@ugm.ac.id
[2]ismil.khari@ugm.ac.id

Abstrak: Rekam Medis Elektronik (RME) merupakan salah satu terobosan dari pemanfaatan teknologi informasi dalam bidang kesehatan bertujuan untuk mempermudah pelayanan kesehatan. Dengan semakin banyaknya penyedia layanan kesehatan yang memanfaatkan RME ini, yang harus diperhatikan bukan hanya masalah migrasi data dari konvensional menjadi digital, namun juga mengenai cara pengamanan data pada RME yang memiliki sifat sensitif dan rahasia yang selama ini permasalahan privasi belum diatur dan ditangani secara memadai pada proses pembuatan RME ini. Untuk menyelesaikan masalah tersebut, peneliti membuat sebuah literatur *review* mengenai teknik pengamanan data pada 20 artikel prosiding dan jurnal. Teknik pengamanan data yang seringkali digunakan sebagai usaha pengamanan data adalah kriptografi, *firewall*, dan kontrol akses.
Kata Kunci: rekam medis elektronik, keamanan data, kriptografi, *cyber-security*

Abstract: Electronic Medical Record (EMR) is one of the breakthroughs of the use of information technology in healthcare aims to facilitate health services. The number of healthcare providers utilizing EMR, which must be considered not only the problem of data migration from conventional to digital but also how to secure data on EMRs that privacy issues have not been adequately addressed and handled making the process of this EMR. To solve the problem, the researcher made a literature review of data security techniques in 20 articles proceedings and journals. Data security techniques that are often used as an effort to secure data is cryptography, firewall, and access control.
Keywords: electronic medical record, data security, cryptography, cyber-security

I. PENDAHULUAN

Pada saat ini, sektor pelayanan kesehatan menunjukan perkembangan yang sangat signifikan dalam pemanfaatan Teknologi Informasi Kesehatan dalam melaksanakan pelayanan kesehatan [1]. Di Indonesia pemanfaatan teknologi informasi di bidang kesehatan yang sudah diterapkan adalah Sistem Informasi Kesehatan (SIK), sekarang mulai berkembang ke arah pembuatan Rekam Medis Elektronik (RME).

Penerapan SIK dan pengembangan RME ini memberikan perubahan yang luar biasa pagi pasien, dokter, dan pelayanan kesehatan lainnya serta institusi kesehatan baik di Indonesia ataupun di luar negeri. Implementasi Rekam Medis Elektronik ini dimaksudkan untuk mempermudah pelayanan kesehatan dan diharapkan memiliki efek yang positif pada perawatan dan tindakan yang diberikan kepada pasien [2].

Rekam medis eletronik didefinisikan oleh *Center of Medicare and Medicaid Services* (CMS) sebagai catatan medis elektronik pasien, yang dikelola oleh penyedia layanan kesehatan dari waktu ke waktu, dan mencakup data klinis yang relevan dengan perawatan seorang pasien dibawah instansi pelayanan kesehatan tertentu, termasuk

demografi, catatan kemajuan, permasalahan, pengobatan, tanda vital, riwayat pengobatan sebelumnya, imunisasi, hasil laboratorium dan laporan radiologi [3]. Disebutkan dalam penelitian [4] bahwa 70% orang mengkhawatirkan jika informasi kesehatan mengenai mereka mengalami kebocoran.

Hal ini sudah dibuktikan dengan adanya penjualan data pasien pada Rumah Sakit Rumah Sakit Universitas Chicago dan Rumah Sakit Wilcox Memorial, Kauai, Hawaii (sebanyak 130.000 data pasien). Telah disebutkan sebelumnya, bahwa RME merupakan salah satu terobosan dari pemanfaatan teknologi informasi dalam bidang kesehatan yang saat ini gencar dikembangkan di Indonesia, hal ini berasosiasi dengan pemahaman para pengguna yang terlibat dalam pelayanan kesehatan mengenai *cyber-security*.

Pemahaman mengenai *cyber-security* ini sangat dibutuhkan dalam pemanfaatan teknologi informasi dalam bidang kesehatan khususnya dalam pengembangan RME ini. Hal ini dikarenakan sifat sensitif dari informasi yang disimpan dalam RME, dan selama ini permasalahan privasi belum diatur dan ditangani secara memadai pada proses pembuatan RME ini.

Di Indonesia Undang-undang yang mengatur mengenai keamanan privasi di dalam payung hukum adalah Undang-Undang Informasi dan Transaksi Elektronik (ITE) dalam pasal 5 dan 6, serta Permenkes Nomor 269 Tahun 2008 tentang Rekam Medis pasal 2. Namun dari Undang-undang yang ada ini masih sebatas mengenai aspek legalitas hukum dari RME dan belum mengatur mengenai permasalahan privasi dari data RME ini, sehingga pengembangan RME saat ini masih sebatas menggantikan RME dari kertas ke dalam bentuk digital. Dalam transformasinya, pemahaman mengenai permasalahan yang muncul dari proses migrasi ini akan dibahas lebih lanjut mengenai teknik keamanan data sebagai salah satu solusi dari masalah privasi pada RME berdasarkan literatur *review* penelitian-penelitian sebelumnya.

II. METODE

Jenis penelitian ini adalah studi literatur mengenai permasalahan privasi dalam RME. Studi literatur yang dilakukan pada penelitian ini terbatas pada teknik-teknik yang diterapkan untuk menjaga keamanan data yang berkolerasi dengan permasalahan privasi pada RME. Literatur yang digunakan dalam makalah ini adalah prosiding dan jurnal yang berasal dari PubMed, IEEE, dan ScienceDirect.

Prosiding dan jurnal yang digunakan menggunakan kata kunci "*Security in Electronic Medical Record*", "*Access Control in Electronic Medical Record*", "*Privacy Issues in Electronic Health Record* ", "*Firewall in EMR*". Dari hasil pencarian ditemukan 20 artikel yang sesuai dengan kata kunci.

III. HASIL

Standar mengenai pertukaran, integrasi, berbagi dan pengambilan informasi kesehatan elektronik yang mendukung praktik klinis dan manajemen dan evaluasi pelayanan kesehatan diatur oleh sebuah badan non-profit yaitu Health Level Seven International (HL7).

HL7 berfokus pada bagaimana data ditransimisikan dari satu layanan ke layanan lainnya. Selain aturan HL7, kerahasiaan dan keamanan informasi kesehatan yang dilindungi, termasuk di dalamnya adalah RME di negara Amerika dibahas dalam *Health Insurance Portability and Accountability Act* (HIPAA) [5]. Namun, pada kenyataannya persyaratan keamanan

end-to-end lebih kompleks dari yang tertuang dalam HL7 [6], [7]. Hal ini diperumit dengan sensitifitas dari data rekam medis yang merupakan data yang rahasia dan tidak dapat disebarluaskan secara bebas [3], [8]–[10].

Dengan pemanfaatan teknologi informasi, salah satunya adalah penggunaan media internet sebagai salah satu pemanfaatan teknologi dalam mempermudah pengaksesan data memudahkan data-data rekam medis pasien diretas oleh pihak yang tidak bertanggung jawab. Pada Mei 2017, *malware WannaCry* menginfeksi ratusan sistem informasi rumah sakit diseluruh Eropa, untuk menyimpan data-data rekam medis seluruh pasien, untuk kemudian meminta tebusan jika data tersebut ingin dikembalikan [11].

Disebutkan dalam penelitian [4] bahwa 70% orang mengkhawatirkan jika informasi kesehatan mengenai mereka mengalami kebocoran. Hal ini sudah dibuktikan dengan adanya penjualan data pasien pada Rumah Sakit. Rumah Sakit Universitas Chicago dan Rumah Sakit Wilcox Memorial, Kauai, Hawaii (sebanyak 130.000 data pasien). Dari kejadian tersebut menunjukan bahwa meskipun RME merupakan solusi yang baik untuk penyajian dan pengolahan data secara *real-time*, namun masih memiliki permasalahan yang itu bagaimana data yang disimpan dan yang mengalir pada sistem dengan aman dan tetap terjaga kerahasiaannya. Untuk mengatasi permasalahan ini, beberapa penelitian melakukan berbagai teknik pengamanan data yang disajikan dalam Tabel 1.

IV. PEMBAHASAN

Berdasarkan 20 artikel jurnal dan prosiding yang didapatkan dengan pencarian berdasarkan kata kunci "keamanan dan permasalahan privasi pada rekam medis elektronik" dapat dilihat bahwa teknik keamanan data dan sistem informasi pada data RME dan jaringan kesehatan adalah dengan memanfaatkan teknik dari kriptografi.

Tabel 1. Teknik Pengamanan Data Yang Dilakukan Pada Data RME

Penulis	Teknik Keamanan
[7]	Menerapkan *Document Archiving and Communication System* untuk menjaga keamanan dan interoperabilitas dari RME dan dokumen klinis lainnya.
[6]	Memanfaatkan tiga level keamanan dalam XML, yaitu 1. XML *Key Management Services* (tanda tangan digital untuk mengautentifikasi pesan dari sumber data) 2. XML *Encryption* (untuk melindungi keamanan data yang dikirim) 3. XML *Key Management Services* (pendaftaran kunci publik dan validasi)
[12]	Penerapan *firewall* untuk pengamanan data
[13]	Enkripsi pada data RME, *password* dan *backup* sistem
[14]	Memberikan fitur *hide* (sembunyi) untuk mengatur mengenai data RME apa saja yang dapat ditampilkan atau disembunyikan dari pihak-pihak yang memiliki wewenang yang berbeda.
[15]	Enkripsi data, dan membuat data RME menjadi anonimus, jika data tersebut diambil untuk penelitian
[16]	*Firewall*, enkripsi dan dekripsi data RME, Audit Log, serta untuk menjaga keamanan data, data-data RME diawasi oleh seorang *Chief Information Security Officer*
[17]	Penerapan *role-based* dan autentifikasi personal dengan menggunakan enkripsi
[12][18]	*Password*, kontrol akses dan *firewall*
[8]	Kontrol akses, Penyimpanan data dengan menggunakan Enkripsi, Audit untuk mengetahui siapa saja yang mengakses data dan apa saja perubahan yang dilakukan
[19]	Kontrol akses, Fungsi Log Audit untuk mengetahui kegiatan apa saja yang dilakukan pada data RME, Fungsi Agregasi data
[20]	Keamanan dengan menggunakan *role-based*
[21]	*Role-Based Access Control* (RBAC)
[22]	Skema autentifikasi dengan penggunaan ID
[23]	Kriptografi (tanda tangan digital, algoritma enkripsi, sertifikasi digital)
[24]	*Mobile agents*
[25]	Protokol kriptografi matriks RBAC
[26]	Tanda tangan digital
[27]	*Cloud computing*
[28]	Kontrol akses untuk mencegah orang yang tidak bertanggung jawab mengakses data RME.

Enkripsi dan dekripsi merupakan bagian dari kriptografi yaitu informasi yang rahasia atau sensitif dapat diubah bentuknya dari bentuk yang dapat dimengerti ke dalam bentuk yang tidak dapat dimengerti [29]. Bentuk informasi yang dapat dimengerti disebut dengan *plaintext*, sedangkan

bentuk informasi yang sudah tidak dapat dimengerti disebut dengan *chipertext*. Proses perubahan bentuk informasi dari *plaintext* menjadi *chipertext* disebut dengan enkripsi, dan sebaliknya disebut dengan dekripsi dengan menggunakan sebuah kunci [8].

Teknik keamanan data dengan enkripsi meningkatkan keamanan ketika proses pertukaran data terjadi pada sistem informasi. Dengan adanya enkripsi ini, data RME yang diakses harus dibuka dengan cara mendekrip nya menggunakan sebuah kunci. Teknik dekripsi salah satunya adalah dengan menggunakan tanda tangan digital. Metode ini telah terbukti dapat menjaga data dari pelanggaran keamanan [16].

Selanjutnya enkripsi dan dekripsi juga merupakan metode yang berhasil mengamankan data pada *Personal Health Information* (PHI) dengan mengakses *mobile agent. Mobile agent* merupakan salah satu perangkat lunak yang dapat memindahkan data dari satu komputer ke komputer lainnya secara autonomus, dan fungsi ini dapat dijalankan meskipun pengguna sudah tidak terhubung dengan jaringan [30]. Dengan mengamankan *mobile agent* pada saat terjadi pertukaran data, RME tidak hanya menjadi lebih aman tetapi juga mudah diakses [24].

Teknik kriptografi lainnya adalah dengan menggunakan *username* dan *password*. Penggunaan *username* dan *password* dapat menghindari pelanggaran keamanan, namun pengguna disarankan untuk mengganti *password* secara berkala. *Password* yang digunakan tidak boleh memiliki makna bagi pengguna, misalnya tanggal lahir. Hal ini dilakukan untuk mencegah peretas menebak *password* dengan mudah.

Selain teknik-teknik yang telah disebutkan sebelumnya, teknik keamanan yang paling sering digunakan lainnya adalah dengan pemanfaatan *firewall* [12], [15], [16], [18]. Meskipun *firewall* dalam penerapannya membutuhkan biaya yang mahal dan bervariasi berdasarkan ukuran dan ruang lingkup organiasasi, namun *firewall* ini telah terbukti berhasil mengamankan jaringan dan dapat melindungi keamanan data RME [3].

Firewall dalam provider jaringan baik berupa perangkat keras atau perangkat lunak bertindak sebagai penyangga keamanan antara jaringan penyedia dan jaringan "*untrusted*", seperti internet. Ketika ditempatkan pada sebuah jaringan, *firewall* dapat membantu untuk memastikan bahwa hanya informasi dan personel yang tepat yang hanya diperbolehkan untuk mengakses ke jaringan penyedia, memblokir transmisi yang tidak diinginkan atau berbahaya dari pengguna yang tidak sah, dan dapat memfilter konten yang diizinkan untuk dilihat oleh pengguna. Dengan perilakunya ini, *firewall* sangat berfungsi untuk mengamankan data RME yang rahasia.

Selanjutnya, teknik keamanan yang dapat dilakukan adalah dengan memberikan fitur *hide* (sembunyi) untuk mengatur mengenai data RME apa saja yang dapat ditampilkan atau disembunyikan dari pihak-pihak yang memiliki wewenang yang berbeda. Kemudian, teknik keamanan data yang dilakukan adalah dengan menerapkan kontrol akses terhadap data RME.

Kontrol akses ini dapar berupa *password* dan nomor PIN yang dapat membatasi akses terhadap informasi. Kontrol akses berisi mengenai sejauh mana pengguna diijinkan untuk mengakses data RME. Misalnya, pengguna A diberikan akses untuk membaca, menulis dan mengeksekusi data, selanjutnya pengguna B hanya diberikan akses untuk membaca data [31].

Kontrol akses lainnya yang digunakan adalah dengan menerapkan *role-based access control* (RBAC). Metode RBAC ini mengizinkan pengguna mengakses data sesuai dengan perannya pada organisasi pelayanan kesehatan. Prosedur penentuan peran biasanya didasarkan pada evaluasi kebutuhan dan kebijakan keamanan. Contohnya, untuk RME peran pengguna yang terlibat adalah perawat, dokter, pasien dan pegawai administrasi [17]. Masing-masing peran ini memiliki akses yang berbeda-beda yang disesuaikan dengan perannya.

Dari studi literatur yang telah dilakukan, diharapkan dalam proses pengembangan RME yang sedang gencar dilakukan di bidang kesehatan baik pemerintah ataupun swasta tidak hanya mementingkan migrasi data dari kertas menjadi digital untuk mempermudah pekerjaan dari perekam medis dan mempertimbangkan bagaimana data dapat disajikan secara tepat sehingga penyadian informasi didapatkan secara *real time* saja, namun dibalik itu kemanan data dari pasien harus juga diperhatikan.

Sebagaimana kita ketahui bahwa data pada rekam medis merupakan data yang bersifat rahasia, sensitif dan privasi untuk setiap pasien yang perlu dijaga keamanannya. Hal ini perlu menjadi pertimbangan dikarenakan tidak menutup kemungkinan bahwa sistem informasi kesehatan khususnya RME yang telah diterapkan oleh penyedia layanan kesehatan saat ini akan terintegrasi dengan seluruh penyedia layanan kesehatan dimanapun tidak terbatas oleh wilayah.

Dalam hal ini pasien dapat berkunjung ke penyedia layanan jasa manapun dengan nomor rekam medis yang sama. Selain itu juga, sistem informasi kesehatan yang ada dapat terintegrasi dengan penyedia jasa lainnya, seperti bank atau perusahaan asuransi. Sehingga diperlukan pemahaman dan penerapan teknik kemanan data dari sisi teknologi informasipun harus dipertimbangkan dan diterapkan dalam sistem yang telah ada saat ini, serta perlu dibentuk sebuah dasar hukum yang jelas yang mengatur regulasi privasi pada RME.

V. KESIMPULAN

Rekam medis elektronik berisi informasi mengenai pasien dan hasil diagnosis dari tindakan kesehatan yang dilakukan, yang sebagian bear dianggap sebagai informasi kesehatan yang harus dilindungi keamanannya. Seperti yang telah dijelaskan, privasi dan keamanan merupakan hal yang penting dalam implementasi RME, maka diperlukan teknik-teknik keamanan data yang dapat melindungi data dan infromasi yang ada didalamnya.

Teknik pengamanan data yang dapat dilakukan adalah dengan memanfaatkan metode kriptografi, *firewall*, kontrol akses, dan teknik keamanan lainnya. Metode ini telah terbukti sebagai teknik sangat menjanjikan dan berhasil untuk menjaga privasi dan keamanan dari RME.

REFERENSI

[1] J. Walker, E. Pan, D. Johnston, J. Adler-Milstein, D. W. Bates, and B. Middleton, “The value of health care information exchange and interoperability.,” *Health Aff. (Millwood).*, vol. Suppl Web, pp. 10–18, 2005.

[2] D. Sittig, D. Gonzales, and H. Singh, “Contingency planning for electronic health record-based care continuity: a survey of recommended practices.,” *Int J Med Inf.*, vol. 83, pp. 797–804, 2014.

[3] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, “Security Techniques for the Electronic Health Records,” *J. Med. Syst.*, vol. 41, no. 8, 2017.

[4] M. C. Rash, “Privacy concerns hinder electronic medical records,” *Bus. J. Gt. Triad Area*, 2005.

[5] S. A. Spooner, “Pediatric Biomedical Informatics,” vol. 10, pp. 83–91, 2016.

[6] P. Ray and J. Wimalasiri, “The need for technical solutions for maintaining the privacy of EHR,” *Annual International Conference of the IEEE Engineering in Medicine and Biology - Proceedings*. pp. 4686–4689, 2006.

[7] J. Delgado, S. Llorente, M. Pàmies, and J. Vilalta, “Security and privacy in a DACS,” *Stud. Health Technol. Inform.*, vol. 228, pp. 122–126, 2017.

[8] HealthIT.gov, "Privacy, Security and Electronic Health Records," *Dep. Heal. Hum. Serv.*, pp. 1–2, 2014.

[9] K. Mireku, Z. FengLi, M. Dennis NiiAyeh, A. Khan, and I. Khan, "Secured cloud database health care mining analysis," *2016 3rd Int. Conf. Comput. Sustain. Glob. Dev.*, pp. 3740–3937, 2016.

[10] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology.," *Conf. Proc. IEEE Eng. Med. Biol. Soc.*, vol. 1, pp. 5453–5458, 2006.

[11] M. M. Mello, J. A. Milstein, K. L. Ding, and L. Savage, "Legal Barries to the Growth of Health Information Exchange - Boulders or Pebbles?," *Growth (Lakeland)*, vol. 93, no. June, pp. 1–5, 2010.

[12] M. A. Al-shaher, "Protect Healthcare System Based on Intelligent Techniques," pp. 421–426, 2017.

[13] K. Amer, "Informatics: Ethical Use of Genomic Information and Electronic Medical Records," *J. Am. Nurses Assoc*, vol. 20(2), 2015.

[14] L. C. Huang, H. C. Chu, C. Y. Lien, C. H. Hsiao, and T. Kao, "Embedding a hiding function in a portable electronic health record for privacy preservation," *J. Med. Syst.*, vol. 34, no. 3, pp. 313–320, 2010.

[15] R. Collier, "New tools to improve safety of electronic health records," *C. Can. Med. Assoc. J.*, vol. 186, no. 4, pp. 250–251, 2014.

[16] M. C. Jannetti, "In Focus: Safeguarding patient information in electronic health records," *AORN J.*, vol. 100, no. 3, pp. C7–C8, 2014.

[17] S. V. Senese, "A Study of Access Control for Electronic Health Records," 2015.

[18] E. S. Hunter, "Electronic Health Records in an Occupational Health Setting—Part I. A Global Overview," *Workplace Health Saf.*, vol. 61, no. 2, pp. 57–60, Feb. 2013.

[19] A. Omotosho and J. Emuoyibofarhe, "A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records," *Int. J. Appl. Inf. Syst.*, vol. 7, no. 8, pp. 11–18, 2014.

[20] M. A. de J. Carvalho and P. B. Paiva, "Health Information System (HIS) role-based access control current security trends and challenges," *Hindawi J. Healthc. Eng.*, vol. 2018, pp. 1–17, 2017.

[21] M. Ehsan Rana, M. Kubbo, and M. Jayabalan, "Privacy and Security Challenges Towards Cloud Based Access Control in Electronic Health Records," *Asian J. Inf. Technol.*, vol. 16, no. February 2017, pp. 2–5, 2017.

[22] A. Chaturvedi, D. Mishra, and S. Mukhopadhyay, "An enhanced dynamic ID-based authentication scheme for telecare medical information systems," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 29, no. 1, pp. 54–62, 2017.

[23] A. Tejero and I. De La Torre, "Advances and current state of the security and privacy in electronic health records: Survey from a social perspective," *J. Med. Syst.*, vol. 36, no. 5, pp. 3019–3027, 2012.

[24] M. Nikooghadam and A. Zakerolhosseini, "Secure communication of medical information using mobile agents," *J. Med. Syst.*, vol. 36, no. 6, pp. 3839–3850, 2012.

[25] H. C. Lee and S. H. Chang, "RBAC-matrix-based EMR right management system to improve HIPAA compliance," *J. Med. Syst.*, vol. 36, no. 5, pp. 2981–2992, 2012.

[26] N. Shank, E. Willborn, L. Pytlikzillig, and H. Noel, "Electronic health records: Eliciting behavioral health providers' beliefs," *Community Ment. Health J.*, vol. 48, no. 2, pp. 249–254, 2012.

[27] Y. Y. Chen, J. C. Lu, and J. K. Jan, "A secure EHR system based on hybrid clouds," *J. Med. Syst.*, vol. 36, no. 5, pp. 3375–3384, 2012.

[28] M. Sicuranza and M. Ciampi, "A semantic access control for easy management of the privacy for EHR systems," *Proc. - 2014 9th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. 3PGCIC 2014*, pp. 400–405, 2014.

[29] M. E. Smid and K. Dennis, "The Data Encryption Standard Past and Future," *Proc. IEEE*, vol. 76, no. 5, pp. 550–559, 1988.

[30] M. S. Greenberg, J. C. Byington, and D. G. Harper, "Mobile agents and security," *IEEE Commun. Mag.*, vol. 36, no. 7, pp. 76–85, 1998.

[31] B. S. Alhaqbani, "Privacy and Trust Management for Electronic Health Records," *A Diss. PHD*, no. June, 2010.