Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik *Medical Check-Up* MP

Diva Rizky Amanda Tiorentap[1], Hosizah[2]
[1,2]Program Studi Manajemen Informasi Kesehatan, Fakultas Ilmu-Ilmu Kesehatan, Universitas Esa Unggul, Jakarta, Indonesia
Jl. Arjuna Utara No.9, Kebon Jeruk Jakarta Barat
Korespondensi E-mail: divarizkya@gmail.com

Abstract

Electronic medical records are a form of evidence of advances in information technology in health services. In an effort to maintain the security and confidentiality of information on electronic medical records, ISO 27001 states that the ideal information system must cover have 3 aspects, namely these are confidentiality, integrity and availability. The purpose of this study was is to determine the aspects of information security in the application of electronic medical records in the MP Medical Check-Up clinic based on Gap Analysis: Status of ISO 27001 Implementation - Checklist. This study is a qualitative descriptive study using observation and interview methods. The results of the study shows that the percentage of information security achievement based on the checklist assessment is a) 60% privacy aspects, b) 31% integrity aspects, c) 48% authentication aspects, d) availability 25 %, e) Aspects of access control (access control) 56%, f) Aspects of non-repudiation (non repudiation) 33%. This is due to the absence of an ISO 27001 audit and no official internal audit. The findings (gaps) that occur are only discussed in a meeting and resolved on the spot. So then, the suggestions that can be proposed are to immediately carry out an internal and external audit of the MP clinical information system in accordance with ISO 27001, improve rules in flowcharts to reduce data crashes such as data duplication and so on, as well as affirmation and commitment to the importance of maintaining information system security to all users.

Keywords: *Electronic Medical Records, Information security, ISO 27001*

Abstrak

Rekam medis elektronik merupakan salah satu bentuk bukti kemajuan teknologi informasi dalam layanan kesehatan. Dalam upaya menjaga keamanan dan kerahasiaan informasi pada rekam medis elektronik, *ISO 27001* menyatakan bahwa sistem informasi yang ideal harus mencakup 3 aspek yakni *confidentiality*, *integrity* dan *availability*. Tujuan dari studi ini adalah untuk mengetahui aspek keamanan informasi dalam penerapan rekam medis elektronik di klinik *Medical Check-Up* MP berdasarkan *Gap Analysis : Status of ISO 27001 Implementation – Checklist*. Studi ini merupakan deskriptif kualitatif dengan menggunakan metode observasi dan wawancara. Hasil studi menunjukkan bahwa persentase pencapaiaan keamanan informasi berdasarkan penilaian *checklist* adalah a) Aspek kerahasiaan (*privacy*) 60%, b) Aspek integritas (*integrity*) 31%, c) Aspek autentikasi (*authentication*) 48%, d) Aspek ketersediaan (*availability*) 25%, e) Aspek kontrol akses (*access control*) 56%, f) Aspek nir-sangkal (*non repudiation*) 33%. Hal ini disebabkan oleh belum dilakukannya audit *ISO 27001* dan belum dilakukannya audit internal secara resmi, temuan (*gap*) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga. Maka, saran yang dapat diusulkan adalah segera dilakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sesuai dengan *ISO 27001*, perbaikan *rule* dalam *flowchart* untuk mengurangi *data crash* seperti duplikasi data dan sebagainya, serta penegasan dan komitmen akan pentingnya menjaga keamanan sistem informasi kepada seluruh *user*.

Kata Kunci: *Rekam Medis Elektronik, Keamanan informasi, ISO 27001*

Pendahuluan

Pesatnya perkembangan teknologi informasi di berbagai bidang menjadi fenomena yang lumrah pada era digital saat ini. Tak terkecuali pada bidang kesehatan, salah satu bentuknya adalah penggunaan sistem informasi dalam layanan kesehatan. Bukan menjadi rahasia bahwa penggunaan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang menguntungkan pemberi pelayanan (*provider*) yang dalam hal ini adalah rumah sakit, klinik, dan sebagainya. Beberapa contoh manfaat yang dapat diperoleh yakni meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan pembacaan ketersediaan fasilitas dan aksesibilitas informasi (1).

Salah satu bentuk pemanfaatan sistem informasi dalam layanan kesehatan adalah rekam medis elektronik. Menurut C. S. Kruse (2017) dalam Ningtyas dan Ismil (2018) Rekam medis eletronik merupakan catatan medis berbentuk elektronik, yang dikelola oleh penyedia layanan kesehatan dimana didalamnya berisi data demografi, catatan kemajuan, permasalahan, pengobatan, tanda vital, riwayat pengobatan sebelumnya, imunisasi, hasil laboratorium dan laporan radiologi (2).

Terlepas dari manfaat yang dapat diperoleh dari sistem informasi, terdapat ancaman yang juga harus menjadi perhatian khusus bagi pengguna. Menurut Roohparvar (2017) dalam Direktorat Proteksi Infrastruktur Informasi Kritis Nasional (IIKN) Badan Siber dan Sandi Negara (2019) alasan bahwa keamanan informasi pada sektor kesehatan harus menjadi prioritas diantaranya karena teknik pencurian data oleh hacker semakin bervariasi, teknik perlindungan data pasien semakin kompleks, Meningkatnya kasus penyanderaan data menggunakan *ransomware*, risiko dari pihak ketiga, kerawanan *e-mail* dan aplikasi bergerak (*mobile application*) (3).

Pada Februari 2017 terjadi kasus bocornya data dari *Cloudflare*, yakni sebuah perusahaan penyedia layanan *cloud*. Selain itu, terjadi juga kasus serangan *ransomware WannaCry* yang dinyatakan merupakan salah satu serangan *cyber* terbesar yang pernah terjadi di dunia. *WannaCry* memanfaatkan *tool* senjata *cyber* dinas intel Amerika Serikat, NSA, yang dicuri peretas dan dibocorkan di internet. Dalam kasus ini, tercatat 150 negara termasuk Indonesia menjadi korbannya. Kasus ini menyebabkan kelumpuhan sistem, salah satunya adalah sistem informasi RS Kanker Dharmais. Dimana terjadi kelambatan pada sistem informasi RS sehingga mengakibatkan penumpukan pasien (4).

Adapun ketentuan mengenai keamanan dan kerahasiaan informasi khususnya di bidang kesehatan diatur dalam *Health Insurance Portability and Accountability Act (HIPAA)* harus memenuhi hal sebagai berikut, a) Memastikan kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan yang dilindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan; b) Melindungi terhadap ancaman atau bahaya yang diantisipasi secara wajar; c) Melindungi dari penggunaan atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan peraturan privasi; d) Pastikan kepatuhan oleh tenaga kerjanya (5). Ketentuan tersebut dikelompokkan menjadi 3 (tiga) standar keamanan pokok yaitu *administrative safeguards* (perlindungan administratif), *physical safeguards* (perlindungan fisik) dan *technical safeguards* (perlindungan teknis) (6).

Disamping itu dalam *ISO/IEC 27001* menyatakan bahwa aspek keamanan informasi mencakup *confidentiality, integrity dan availability* (7). Senada dengan pernyataan Rahardjo (2017) bahwa prinsip-prinsip keamanan informasi terdiri dari *privacy, confidentiality, integrity, availability, non repudiation, authentication, dan authorization* (8).

Berdasarkan penelitiaan Nugrahaeni dan Nurhayati (2018) yang dilakukan di RSUD Dr. Moewardi diperoleh hasil sebagai berikut, a) aspek kerahasiaan (*privacy*) dapat dibuktikan dengan penjagaan informasi dari pihak yang tidak memiliki hak akses melalui *username* dan *password* bagi tiap pengguna; b) aspek integritas (*integrity*) dibuktikan dengan penghapusan data belum dapat terfasilitasi; c) Aspek autentikasi (*authentication*) dibuktikan dengan akses terhadap informasi menggunakan *Personal Identification Number (PIN)*; d) aspek ketersediaan (*availability*) dapat terfasilitasi namun belum maksimal; e) aspek kontrol akses *(access control)* terfasilitasi dengan adanya keterbatasan hak akses pengguna; f) aspek nir-sangkal *(non repudiation)* dibuktikan dengan identifikasi terhadap pihak yang melakukan pengisian dan perubahan informasi belum maksimal (9).

Alhaqbani (2017) dalam Lubis dan Annisa (2018) menyatakan bahwa aspek kontrol akses dapat diimplementasikan melalui penggunaan *password* serta *PIN* yang dapat membatasi akses terhadap informasi. Selanjutnya, menurut Al-Shaher (2010) dalam Lubis dan Annisa (2018) penggunaan *firewall* juga 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 (2).

Berdasarkan hasil observasi di klinik *Medical Check-Up* MP ditemukan ketidaksesuaian prinsip keamanan sistem informasi yakni antar *user* masih saling bertukar informasi terkait *user-id* dan *password*-nya. Selain itu, satu *user-id* digunakan oleh beberapa orang juga sangat biasa dilakukan. Hal ini tentu saja akan berakibat fatal jika terjadi kesalahan penginputan, dimana menyulitkan untuk proses identifikasi pelaku. Jika hal ini terus berlanjut, dikhawatirkan akan mengakibatkan pada penggunaan informasi oleh pihak-pihak yang tidak bertanggung jawab.

Melalui pemaparan diatas, maka saya tertarik untuk meninjau aspek keamanan informasi dalam penerapan rekam medis elektronik di klinik *Medical Check-Up* MP.

Metode Penelitian

Prosedur Pengumpulan Data

Adapun metode yang digunakan dalam pengumpulan data adalah sebagai berikut :

1. Observasi
   Pada metode ini, peneliti mengamati alur kerja sistem informasi klinik MP yakni meliputi *input* (masukan data), *process* (pengolahan data), dan *output* (informasi yang dihasilkan) sehingga dapat mengetahui gambaran kegiatan rekam medis elektronik berdasarkan *aspek privacy, integrity, authentication, availability, access control* dan *non repudiation*.
2. Wawancara
   Dalam kegiatan wawancara, peneliti melakukan tanya jawab kepada perwakilan *user* sistem informasi klinik MP yang terdiri dari 1 (satu) petugas *medical record*, 1 (satu) manajer klinik, dan 1 (satu) petugas IT.

Instrumen Pengumpulan Data

Adapun instrumen pengumpulan data yang digunakan adalah *Gap Analysis : Status of ISO 27001 Implementation – Checklist* dan pedoman wawancara yang terdiri dari sejumlah pertanyaan.

Pengolahan dan Analisis Data

1. Pengolahan Data
   Pengolahan data dilakukan dengan 2 (dua) tahap, yakni sebagai berikut :
   a. Persiapan Data
      Dalam tahap ini data yang telah terkumpul dilakukan penerjemahan, yakni penghitungan skor yang diperoleh dari *Gap Analysis : Status of ISO 27001 Implementation – Checklist* dan pembuatan transkrip hasil wawancara.
   b. Penyeleksian Data
      Tahap selanjutnya setelah tahap penyeleksian data, yakni tahap membedakan antara data yang penting dan tidak. Hal ini bertujuan memudahkan proses analisis data.
2. Analisis Data
   Metode analisis yang digunakan dalam analisis data ini adalah model alur Miles dan Huberman, yakni analisis data kualitatif dilakukan secara interaktif dan berlangsung secara terus menerus sampai tuntas. Metode ini terdiri dari *data reduction, data display*, dan *conclusion drawing/verification*. Adapun penjelasan menurut Sugiyono (2013) adalah sebagai berikut :
   a. *Data reduction* (reduksi data) yaitu proses merangkum, memilih hal-hal pokok, memfokuskan pada hal-hal yang penting, dicari tema dan polanya.
   b. *Data display* (penyajian data) yaitu menyajikan data agar dapat mudah untuk memahami apa yang terjadi, merencanakan kerja selanjutnya berdasarkan apa yang telah dipahami tersebut. Penyajian data dalam penelitian kualitatif adalah dengan teks yang bersifat naratif.
   c. *Conclusion drawing/verification* (penarikan kesimpulan/verifikasi) yaitu langkah penarikan kesimpulan. Kesimpulan awal yang dikemukakan masih bersifta sementara, dan akan berubah bila ditemukan bukti-bukti yang valid dan konsisten saat peneliti kembali ke lapangan mengumpulkan data, maka kesimpulan yang dikemukakan merupakan kesimpulan yang kredibel (10).

Hasil dan Pembahasan

Berdasarkan kegiatan observasi, maka diperoleh informasi bahwa persentase pencapaian implementasi aspek keamanan informasi rekam medis elektronik pada Sistem Informasi Klinik MP adalah 40%, dimana hanya 43 (empat puluh tiga) dari 108 (seratus delapan) persyaratan yang terpenuhi. Adapun rinciannya adalah sebagai berikut :

1. Aspek kerahasiaan (*privacy*)

Aspek kerahasiaan memenuhi 3 (tiga) dari 5 (lima) persyaratan, dengan persentase sebesar 60%. Adapun persyaratan yang telah terpenuhi adalah sebagai berikut :

Tabel 1.
Persyaratan ISO 27001 Aspek Kerahasiaan Terpenuhi

Klausa	Persyaratan	Keterangan Terpenuhi
4.3.2 (a)	Menyetujui dokumen untuk kecukupan sebelum diterbitkan	Ditunjukkan dengan adanya lembar persetujuan pelaksanaan dan pemberian hak atas informasi peserta MCU. Lembar tersebut diberikan dan ditandatangani oleh peserta MCU saat proses registrasi
4.3.2 (b)	Tinjau dan perbarui dokumen sebagaimana diperlukan dan setujui ulang dokumen	Ditunjukkan dengan adanya kegiatan revisi (pembaruan) kebijakan maupun hal yang berkaitan dengan kerahasiaan informasi, contohnya revisi lembar persetujuan pelaksanaan dan pemberian hak atas informasi peserta MCU
4.3.3	Rekaman harus dilindungi dan dikendalikan.	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP yang berjudul "MP-P-IT-009 Standar Keamanan Penggunaan Komputer"

Sedangkan 2 (dua) persyaratan yang tidak terpenuhi adalah sebagai berikut :

Tabel 2.
Persyaratan *ISO 27001* Aspek Kerahasiaan Tidak Terpenuhi

Klausa	Persyaratan	Keterangan Tidak Terpenuhi
4.2.3 (c)	Ukur efektivitas kontrol untuk memverifikasi bahwa persyaratan keamanan telah dipenuhi.	Belum dilakukannya audit *ISO 27001*
4.2.3 (g)	Perbarui rencana keamanan untuk memperhitungkan temuan kegiatan pemantauan dan peninjauan	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga

Dengan demikian keamanan sistem informasi klinik dilihat dari aspek kerahasiaan sudah baik. Dimana seluruh kegiatan pengoperasiaan sistem informasi telah diatur oleh SOP, termasuk ketentuan penjagaan kerahasiaan informasi. Namun, perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*.

Aspek kerahasiaan dibuktikan dengan bentuk tidak aktifnya (melakukan *log-out* secara otomatis) sistem informasi klinik MP jika dalam kurun waktu 5 (lima) menit tidak terjadi aktivitas yang dilakukan oleh *user*. Hal ini berfungsi sebagai bentuk pertahanan ataupun pencegahan dari bentuk penyalahgunaan *user id*. Namun, hal ini tidak akan berguna dengan baik jika saat *user* melakukan *log in* dengan tindakan "*remember user id & password*" karena sistem akan secara langsung menyimpan data tsb, dan memudahkan siapapun *log in*.

Begitupun dengan komputer, jika tidak terjadi aktiivitas selama kurun waktu 5 (lima) menit, maka dengan otomatis akan melakukan *log out*. Dengan demikian, bentuk pertahanan terdiri dari 2 tahap yakni *log in computer / desktop & log in* sistem informasi klinik MP.

Selain itu, pertahanan dari pihak luar sudah sangat bagus, karena untuk dapat melakukan *log in* pada komputer / *desktop* menggunakan *password* yg unik (hanya pihak internal saja yang mengetahuinya).

Disamping pengamanan dari segi sistem, pengamanan aspek kerahasiaan juga berlaku dalam kegiatan pelepasan informasi. Pelepasan informasi hasil MCU dilakukan dengan cara *by phone & email* baik kepada pihak internal maupun eksternal. Hal ini berdasarkan pada nota kesepahaman (*memorandum of understanding*) dan lembar persetujuan (*informed consent*) yang telah disepakati oleh MP dan pihak klien.

Seperti halnya yang dinyatakan oleh Nugrahaeni dan Nurhayati (2018) bahwa aspek kerahasiaan *(privacy)* dapat dibuktikan dengan penjagaan informasi dari pihak yang tidak memiliki hak akses melalui *username* dan *pasword* bagi tiap pengguna. Dalam hal ini sistem informasi klinik MP telah memenuhi ketentuan *Health Insurance Portability and Accountability Act* (*HIPAA*) seperti yang telah disampaikan pada halaman 14, dimana sistem informasi harus dapat memastikan kerahasiaan semua informasi kesehatan yang dilindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan. Selain itu, ketentuan melindungi dari

penggunaan atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan peraturan privasipun sudah terfasilitasi dengan baik.

2. Aspek integritas *(integrity)*

Aspek integritas memenuhi 11 (sebelas) dari 35 (tiga puluh lima) persyaratan, dengan persentase sebesar 31%. Adapun persyaratan yang telah terpenuhi adalah sebagai berikut :

Tabel 3.
Persyaratan *ISO 27001* Aspek Integritas Terpenuhi

Klausa	Persyaratan	Keterangan Terpenuhi
4.1	Organisasi harus membuat, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI yang terdokumentasi	Ditunjukkan dengan adanya sistem informasi klinik MP, selain itu perusahaan senantiasa melakukan perbaikan untuk meningkatkan performa serta kualitas sistem informasi
4.2.2 (e)	Laksanakan program pelatihan dan penyadaran (lihat 5.2.2)	Ditunjukkan dengan kegiatan pendidikan dan pelatihan oleh lembaga luar kepada petugas *IT*, selain itu dilakukan juga sosialisasi terhadap *user* sistem informasi klinik MP yang baru bergabung
4.3.3	Catatan harus dibuat dan dipelihara untuk memberikan bukti kesesuaian dengan persyaratan dan operasi efektif SMKI	Ditunjukkan dengan adanya kegiatan revisi (pembaruan) SOP yang mengatur kegiatan sistem informasi klinik MP
7.2 (c)	Teknik, produk atau prosedur, yang dapat digunakan dalam organisasi untuk meningkatkan kinerja dan efektivitas SMKI	Ditunjukkan dengan adanya sistem informasi klinik MP, selain itu perusahaan senantiasa melakukan perbaikan untuk meningkatkan performa serta kualitas sistem informasi
5.1 (d)	Mengkomunikasikan kepada organisasi pentingnya memenuhi tujuan keamanan informasi dan menyesuaikan diri dengan kebijakan keamanan informasi, tanggung jawabnya di bawah undang-undang dan kebutuhan untuk perbaikan.	Ditunjukkan dengan kegiatan pendidikan dan pelatihan oleh lembaga luar kepada petugas *IT*, selain itu dilakukan juga sosialisasi terhadap *user* sistem informasi klinik MP yang baru bergabung
5.1 (e)	Menyediakan sumber daya yang cukup untuk membangun, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI (lihat 5.2.1)	Ditunjukkan dengan kegiatan pendidikan dan pelatihan oleh lembaga luar kepada petugas *IT*, selain itu dilakukan juga sosialisasi terhadap *user* sistem informasi klinik MP yang baru bergabung
5.2.1 (b)	Pastikan bahwa prosedur keamanan informasi mendukung persyaratan bisnis	Ditunjukkan dengan SOP sistem informasi klinik MP
7.3 (d)	Kebutuhan sumber daya	Ditunjukkan dengan perusahaan menyediakan sumber daya sistem informasi klinik seperti SDM, *hardware*, *software*, dsb
5.2.2 (b)	Memberikan pelatihan atau mengambil tindakan lain (mis. Mempekerjakan karyawan yang kompeten) untuk memenuhi kebutuhan ini	Ditunjukkan dengan kegiatan pendidikan dan pelatihan oleh lembaga luar kepada petugas *IT*, selain itu dilakukan juga sosialisasi terhadap *user* sistem informasi klinik MP yang baru bergabung
5.2.2 (d)	Menyimpan catatan pendidikan, pelatihan, keterampilan, pengalaman dan kualifikasi (lihat 4.3.3)	Ditunjukkan dengan adanya website khusus yang memfasilitasi dokumen pelatihan maupun lainnya

5.2.2	Organisasi juga harus memastikan bahwa semua personil yang relevan mengetahui relevansi dan pentingnya kegiatan keamanan informasi mereka dan bagaimana mereka berkontribusi pada pencapaian tujuan SMKI.	Ditunjukkan dengan sosialisasi terhadap seluruh *user* maupun pihak internal yang terkait

Sedangkan 24 (dua puluh empat) yang tidak terpenuhi adalah sebagai berikut :

Tabel 4.
Persyaratan *ISO 27001* Aspek Integritas Tidak Terpenuhi

Klausa	Persyaratan	Keterangan Tidak Terpenuhi
4.2.2 (a)	Merumuskan rencana perawatan risiko	Belum dilakukannya audit internal maupun eksternal *ISO 27001*) secara berkala
4.2.2 (b)	Menerapkan rencana perawatan risiko untuk mencapai tujuan kontrol yang diidentifikasi	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.2 (c)	Terapkan kontrol yang dipilih dalam 4.2.1g untuk memenuhi tujuan kontrol	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.2 (d)	Tetapkan bagaimana mengukur efektivitas kontrol atau kelompok kontrol yang dipilih dan tentukan bagaimana pengukuran ini akan digunakan untuk menilai efektivitas kontrol untuk menghasilkan hasil yang sebanding dan dapat direproduksi (lihat 4.2.3c)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.3 (h)	Catat tindakan dan peristiwa yang dapat berdampak pada efektivitas atau kinerja SMKI (lihat 4.3.3)	Belum adanya kegiatan dokumentasi (pencatatan) resmi atas temuan (*gap*) terhadap sistem informasi klinik, temuan tsb hanya dibahas melalui *meeting*
4.3.3	SMKI harus memperhitungkan segala persyaratan hukum atau peraturan yang relevan dan kewajiban kontrak.	Belum dilakukannya audit *ISO 27001*
5.1 (g)	Memastikan bahwa audit internal SMKI dilakukan (lihat 6)	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
5.2.1 (c)	Identifikasi dan alamat persyaratan hukum dan peraturan dan kewajiban keamanan kontraktual	Belum dilakukannya audit *ISO 27001*
5.2.2 (c)	Mengevaluasi efektivitas tindakan yang diambil	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
6	Manajemen yang bertanggung jawab untuk area yang diaudit harus memastikan bahwa tindakan diambil tanpa penundaan yang tidak perlu untuk menghilangkan ketidaksesuaian yang terdeteksi dan penyebabnya. Kegiatan tindak lanjut harus mencakup verifikasi tindakan yang diambil dan pelaporan hasil verifikasi (lihat 8).	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.1	Manajemen harus meninjau SMKI organisasi pada interval yang direncanakan (setidaknya setahun sekali) untuk memastikan kesesuaian,	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga

	kecukupan, dan efektivitasnya yang berkelanjutan	
7.2 (a)	Hasil audit dan ulasan SMKI	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.2 (b)	Umpan balik dari pihak yang berkepentingan	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.2 (d)	Status tindakan preventif dan korektif	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.2 (e)	Kerentanan atau ancaman yang tidak ditangani secara memadai dalam penilaian risiko sebelumnya	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.2 (f)	Hasil dari pengukuran efektivitas	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.2 (g)	Tindakan tindak lanjut dari tinjauan manajemen sebelumnya	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.2 (h)	Setiap perubahan yang dapat memengaruhi SMKI	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.3 (a)	Peningkatan efektivitas SMKI	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.3 (b)	Pembaruan penilaian risiko dan rencana perawatan risiko	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.3 (c)	Modifikasi prosedur dan kontrol yang memengaruhi keamanan informasi, sebagaimana diperlukan, untuk merespons peristiwa internal atau eksternal yang dapat berdampak pada SMKI	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
7.3 (e)	Peningkatan bagaimana efektivitas kontrol diukur	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
8.1	Organisasi harus terus meningkatkan efektivitas SMKI melalui penggunaan kebijakan, tujuan, hasil audit, analisis peristiwa yang dipantau, (lihat 7).	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga

Dengan demikian keamanan sistem informasi klinik dilihat dari aspek integritas belum cukup baik. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*. Seperti yang kita ketahui bahwa informasi dapat dikatakan dapat dipertanggungjawabkan jika informasi tersebut memiliki integritas. Salah satu hal yang menjadi kekhawatiran yakni sistem informasi klinik belum cukup mampu merekam data baru tanpa menghilangkan data lama. Sehingga, memang sangat dibutuhkan integritas dari *user* agar memastikan kegiatan *input* data berjalan dengan baik dan benar.

Aspek integritas pada sistem informasi klinik MP ditunjukkan dengan ketika *user* melakukan *log in*, *user* diberikan kewenangan megoperasikan sistem informasi klinik. Dimana dapat terjadi perubahan (baik penambahan maupun pengurangan) data secara *real time*. Hal ini yang menjadi kunci, apakah integritas data maupun sistem dinilai.

Disamping itu, sistem informasi klinik memiliki kemampuan merekam perubahan yang terjadi atas aksi yang dilakukan oleh *user*. Dimana nama *user* yang melakukan akan terekam dalam sistem, namun tidak dengan data yang diubah.

Dalam hal ini sistem informasi klinik MP belum memenuhi ketentuan *Health Insurance Portability and Accountability Act* (*HIPAA*) seperti yang telah disampaikan pada halaman 14, yakni memastikan integritas semua informasi, karena masih harus dapat dipastikan kembali kepatuhan oleh tenaga kerjanya.

3. Aspek autentikasi *(authentication)*

Aspek autentikasi memenuhi 10 (sepuluh) dari 21 (dua puluh satu) persyaratan, dengan persentase sebesar 48%. Adapun persyaratan yang telah terpenuhi adalah sebagai berikut :

Tabel 5.
Persyaratan *ISO 27001* Aspek Autentikasi Terpenuhi

Klausa	Persyaratan	Keterangan Terpenuhi
4.2.1 (b)	Tetapkan kebijakan SMKI	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
4.3.1 (a)	Pernyataan dan dokumentasi kebijakan SMKI (lihat 4.2.1b) dan sasarannya	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
4.3.1 (b)	Lingkup SMKI (lihat 4.2.1a)	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
4.3.1 (g)	Prosedur diperlukan oleh organisasi untuk memastikan perencanaan, operasi, dan kontrol yang efektif dari proses keamanan informasinya dan menggambarkan bagaimana mengukur efektivitas kontrol (lihat 4.2.3c)	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
4.3.1 (h)	Catatan yang diperlukan oleh Standar Internasional ini (lihat 4.3.3)	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
4.3.2 (c)	Pastikan bahwa perubahan & status revisi dokumen diidentifikasi	Ditunjukkan dengan adanya kegiatan revisi (pembaruan) SOP yang mengatur kegiatan sistem informasi klinik MP
5.1 (a)	Menetapkan kebijakan SMKI	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
5.1 (b)	Memastikan bahwa sasaran dan rencana SMKI dibuat	Ditunjukkan dengan proposal kegiatan pengajuan sistem informasi klinik
5.1 (c)	Menetapkan peran dan tanggung jawab untuk keamanan informasi	Ditunjukkan dengan adanya rincian deskripsi pekerjaan *(job description*) petugas *IT*
5.2.1 (d)	Pertahankan keamanan yang memadai dengan aplikasi yang benar dari semua kontrol yang diterapkan	Ditunjukkan dengan sistem infomasi klinik MP yang memiliki spesifikasi mendukung keamanan informasi, yakni dengan penggunaan anti virus; backup secara berkala & otomatis; fitur *log-out* secara otomatis; dsb

Sedangkan 11 (sebelas) persyaratan yang tidak terpenuhi adalah sebagai berikut :

Tabel 6.
Persyaratan *ISO 27001* Aspek Autentikasi Tidak Terpenuhi

Klausa	Persyaratan	Keterangan Tidak Terpenuhi
4.2.3 (d)	Tinjau penilaian risiko pada interval yang direncanakan dan tinjau risiko residual dan tingkat risiko yang dapat diterima yang diidentifikasi	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.3 (e)	Lakukan audit SMKI internal pada interval yang direncanakan (lihat 6)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala

4.2.3 (f)	Melakukan tinjauan manajemen terhadap SMKI secara teratur (lihat 7.1)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.1 (i)	Pernyataan Keberlakuan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.2 (g)	Pastikan dokumen yang berasal dari luar diidentifikasi	Belum dilakukannya pencatatan atas dokumen terkait sistem informasi klinik yang diperoleh dari luar MP
5.1 (f)	Memutuskan kriteria untuk menerima risiko dan tingkat risiko yang dapat diterima	Belum dilakukannya penentuan indikator mutu tim *IT*
5.1 (h)	Melakukan tinjauan manajemen terhadap SMKI (lihat 7)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
8.3 (a)	Identifikasi potensi ketidaksesuaian dan penyebabnya	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
8.3 (b)	Mengevaluasi perlunya tindakan untuk mencegah terjadinya ketidaksesuaian	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
8.3 (c)	Menentukan dan mengimplementasikan tindakan pencegahan diperlukan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
8.3	Organisasi harus mengidentifikasi risiko yang berubah dan mengidentifikasi persyaratan tindakan pencegahan yang memusatkan perhatian pada risiko yang berubah secara signifikan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala

Dengan demikian keamanan sistem informasi klinik dilihat dari aspek kerahasiaan belum cukup baik. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001* serta kejelasan ketidaksesuaian yang terjadi, bahkan jika terdapat temuan ketidaksesuaian hanya dibahas dalam pertemuan saja tanpa pencatatan atau pembuatan berita acara untuk evaluasi di masa mendatang.

Aspek autentikasi pada sistem informasi klinik MP ditunjukkan dengan edukasi yang dilakukan oleh pihak manajemen khususnya tim *IT* kepada para *user* untuk selalu menjaga kerahasiaan *user id* dan *password* masing-masing, serta tidak saling memberitahu hal tersebut pada *user* lain. Hal ini serupa dengan hasil penelitian Nugrahaeni dan Nurhayati (2018) bahwa aspek autentikasi *(authentication)* dibuktikan dengan akses terhadap informasi menggunakan *Personal Identification Number* (*PIN*), dengan catatan masing-masing *user* tidak saling berbagi *PIN* tersebut.

Selain itu tim *IT* MP juga membakukan anjuran tersebut dalam bentuk Standar Operasional Prosedur (SOP) "Pemeliharaan Komputer dan Sistem Informasi". SOP tersebut disimpan pada laman berbasis *intranet* yang bertujuan agar seluruh *user* dapat membaca dan memahaminya.

4. Aspek ketersediaan *(availability)*

Aspek ketersediaan memenuhi 3 (tiga) dari 12 (dua belas) persyaratan, dengan persentase sebesar 25%. Adapun persyaratan yang telah terpenuhi adalah sebagai berikut :

Tabel 7.
Persyaratan *ISO 27001* Aspek Ketersediaan Terpenuhi

Klausa	Persyaratan	Keterangan Terpenuhi
4.3.2 (e)	Pastikan bahwa dokumen tetap terbaca dan mudah diidentifikasi	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat diakses dimana saja (tanpa perlu menggunakan jaringan internet khusus)

4.3.2 (f)	Pastikan bahwa dokumen tersedia untuk mereka yang membutuhkannya, dan ditransfer, disimpan, dan pada akhirnya dibuang sesuai dengan prosedur yang berlaku untuk klasifikasi mereka	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat diakses dimana saja (tanpa perlu menggunakan jaringan internet khusus)
4.3.3	Rekaman harus tetap terbaca, mudah diidentifikasi, dan dapat diambil kembali.	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat diakses dimana saja (tanpa perlu menggunakan jaringan internet khusus)

Sedangkan 9 (sembilan) persyaratan yang tidak terpenuhi adalah sebagai berikut :

Tabel 8.
Persyaratan *ISO 27001* Aspek Ketersediaan Tidak Terpenuhi

Klausa	Persyaratan	Keterangan Tidak Terpenuhi
4.2.3 (b)	Melakukan tinjauan berkala terhadap efektivitas SMKI	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.4 (a)	Menerapkan perbaikan yang diidentifikasi dalam SMKI.	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.4 (b)	Ambil tindakan korektif dan preventif yang sesuai sesuai dengan 8.2 dan 8.3	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.4 (c)	Komunikasikan tindakan dan peningkatan kepada semua pihak yang berkepentingan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.2.4 (d)	Pastikan bahwa perbaikan mencapai tujuan yang dimaksudkan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.2 (d)	Pastikan versi relevan dari dokumen yang berlaku tersedia di tempat penggunaan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
5.2.1 (a)	Menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
5.2.1 (e)	Lakukan tinjauan bila perlu, dan untuk bereaksi secara tepat terhadap hasil tinjauan ini	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
5.2.1 (f)	Jika diperlukan, tingkatkan efektivitas SMKI	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala

Dengan demikian keamanan sistem informasi klinik dilihat dari aspek kerahasiaan belum cukup baik. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*. Meskipun dari kemampuan sistem informasi klinik sudah sangat mendukung kegiatan pelayanan MCU yakni dengan kemudahan akses oleh *user* dimanapun, kapanpun, serta oleh siapapun yang memiliki *user id* & *password*, serta terhubung dengan koneksi internet. Dengan begitu, ketentuan *Health Insurance Portability and Accountability Act* (*HIPAA*) seperti yang telah disampaikan pada halaman 14, yakni memastikan ketersediaan semua informasi kesehatan yang dilindungi yang dilindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan sudah terpenuhi.

5. Aspek kontrol akses *(access control)*

Aspek kontrol akses memenuhi 10 (sepuluh) dari 17 (tujuh belas) persyaratan, dengan persentase sebesar 56%. Adapun persyaratan yang telah terpenuhi adalah sebagai berikut :

Tabel 9.
Persyaratan *ISO 27001* Aspek Kontrol Akses Terpenuhi

Klausa	Persyaratan	Keterangan Terpenuhi
4.2.1 (a)	Tentukan ruang lingkup dan batas-batas SMKI	Ditunjukkan dengan sistem infomasi klinik MP yang memiliki spesifikasi yang tertuang dalam SOP
4.2.2 (f)	Kelola pengoperasian SMKI	Ditunjukkan dengan kegiatan penggunaan sistem informasi klinik MP dalam kegiatan operasional perusahaan, dimana dalam hal ini perusahaan mendapatkan profit
4.2.2 (g)	Kelola sumber daya untuk SMKI (lihat 5.2)	Ditunjukkan dengan perusahaan menyediakan sumber daya sistem informasi klinik seperti SDM, *hardware*, *software*, dsb
4.2.2 (h)	Menerapkan prosedur dan kontrol lain yang mampu memungkinkan deteksi cepat terhadap peristiwa keamanan dan respons terhadap insiden keamanan (lihat 4.2.3a)	Ditunjukkan dengan adanya SOP yang mengatur kegiatan sistem informasi klinik MP
4.3.2 (h)	Pastikan distribusi dokumen terkontrol	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*
4.3.2 (i)	Mencegah penggunaan dokumen usang yang tidak disengaja	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*
4.3.2 (j)	Terapkan identifikasi yang sesuai untuk dokumen jika disimpan untuk tujuan apa pun	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*
5.2.2 (a)	Menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan yang mempengaruhi SMKI	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*
8.2 (a)	Mengidentifikasi ketidaksesuaian	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*
8.2 (b)	Menentukan penyebab ketidaksesuaian	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*

Sedangkan 7 (tujuh) persyaratan yang tidak terpenuhi adalah sebagai berikut :

Tabel 10.
Persyaratan *ISO 27001* Aspek Kontrol Akses Tidak Terpenuhi

Klausa	Persyaratan	Keterangan Tidak Terpenuhi
4.2.3 (a)	Jalankan prosedur pemantauan dan peninjauan serta kontrol lainnya	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.1 (c)	Prosedur dan kontrol untuk mendukung SMKI	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.1 (d)	Deskripsi metodologi penilaian risiko (lihat 4.2.1c)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.1 (e)	Laporan penilaian risiko (lihat 4.2.1c hingga 4.2.1g)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
4.3.1 (f)	Rencana penanganan risiko (lihat 4.2.2b)	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
8.2 (c)	Mengevaluasi perlunya tindakan untuk memastikan bahwa ketidaksesuaian tidak terulang	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala
8.2 (d)	Menentukan dan mengimplementasikan tindakan korektif yang diperlukan	Belum dilakukannya audit internal maupun eksternal (*ISO 27001*) secara berkala

Dengan demikian keamanan sistem informasi klinik dilihat dari aspek kerahasiaan sudah cukup baik. Namun perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*.

Aspek kontrol akses sistem pada sistem informasi klinik MP ditunjukkan dengan telah ditentukannya hak masing-masing *user* dalam mengoperasikan sistem informasi klinik. Hak *user* merupakan menu yang dapat diakses oleh *user* tsb. Adapun batasan-batasan menu sistem informasi klinik ditentukan oleh manajer klinik, yang tentu saja merujuk pada deskripsi pekerjaan (*job description*) serta menu sistem informasi klinik MP yang dapat menunjang pekerjaan *user* tersebut. Hal ini senada dengan hasil penelitian Nugrahaeni dan Nurhayati (2018) bahwa aspek kontrol akses *(access control)* dapat terfasilitasi dengan adanya keterbatasan hak akses pengguna.

Penentuan batasan akses pada menu sistem informasi klinik diawali dengan pengajuan *form account accsess* kepada tim *IT*. Selanjutnya permintaan tersebut disetujui oleh kepala kepala departemen terkait, manajemen klinik, dan kepala departemen *IT*. Ketentuan ini diatur dalam SOP departemen *IT* "Prosedur Permintaan Pembuatan dan Perubahan Aplikasi" dan "Prosedur Permintaan *Access*".

6. Aspek nir-sangkal *(non repudiation)*

Aspek nir-sangkal memenuhi 6 (enam) dari 18 (delapan belas) persyaratan, dengan persentase sebesar 33%. Adapun persyaratan yang telah terpenuhi adalah sebagai berikut :

Tabel 11.
Persyaratan *ISO 27001* Aspek Nir-sangkal Terpenuhi

Klausa	Persyaratan	Keterangan Terpenuhi
4.2.1 (i)	Dapatkan otorisasi manajemen untuk mengimplementasikan dan mengoperasikan SMKI	Ditunjukkan dengan adanya penetapan hak akses pada masing-masing *user*
4.3.3	Kontrol yang diperlukan untuk identifikasi, penyimpanan, perlindungan, pengambilan, waktu penyimpanan, dan disposisi catatan harus didokumentasikan dan diimplementasikan.	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat merekam dan menampilkan riwayat penggunaan sistem berdasarkan *user-id*, hal ini berguna untuk mengetahui siapa yang telah melakukan perubahan atas data tsb
4.3.3	Rekaman harus disimpan dari kinerja proses sebagaimana diuraikan dalam 4.2 dan dari semua kejadian insiden keamanan yang signifikan terkait dengan SMKI.	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat merekam dan menampilkan riwayat penggunaan sistem berdasarkan *user*-id, hal ini berguna untuk mengetahui siapa yang telah melakukan perubahan atas data tsb
6 (c)	Diimplementasikan dan dipelihara secara efektif	Ditunjukkan dengan kegiatan perbaikan untuk meningkatkan performa serta kualitas sistem informasi
8.2 (e)	Merekam hasil tindakan yang diambil (lihat 4.3.3)	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat merekam dan menampilkan riwayat penggunaan sistem berdasarkan *user-id*, hal ini berguna untuk mengetahui siapa yang telah melakukan perubahan atas data tsb
8.3 (d)	Merekam hasil tindakan yang diambil (lihat 4.3.3)	Ditunjukkan dengan kemampuan sistem informasi klinik yang dapat merekam dan menampilkan riwayat penggunaan sistem berdasarkan *user-id*, hal ini berguna untuk mengetahui siapa yang telah melakukan perubahan atas data tsb

Sedangkan 12 (dua belas) persyaratan yang tidak terpenuhi adalah sebagai berikut :

Tabel 12.
Persyaratan *ISO 27001* Aspek Nir-sangkal Tidak Terpenuhi

Klausa	Persyaratan	Keterangan Tidak Terpenuhi
4.2.1 (c)	Tetapkan pendekatan penilaian risiko	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
4.2.1 (d)	Identifikasi risikonya	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
4.2.1 (e)	Analisis dan evaluasi risiko	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
4.2.1 (f)	Identifikasi dan evaluasi opsi untuk perawatan risiko	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
4.2.1 (g)	Pilih tujuan dan kontrol kontrol untuk perawatan risiko	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
4.2.1 (h)	Dapatkan persetujuan manajemen dari risiko residual yang diusulkan	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
4.2.1 (j)	Mempersiapkan Pernyataan Keberlakuan [lihat spreadsheet SoA]	Belum dilakukannya audit *ISO 27001*
6 (a)	Mematuhi persyaratan Standar Internasional ini dan perundang-undangan atau peraturan yang relevan	Belum dilakukannya audit *ISO 27001*
6 (b)	Mematuhi persyaratan keamanan informasi yang diidentifikasi	Belum dilakukannya audit *ISO 27001*
6 (d)	Lakukan sesuai harapan.	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
8.2 (f)	Meninjau tindakan korektif yang diambil	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga
8.3 (e)	Meninjau tindakan pencegahan yang diambil	Belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga

Dengan demikian keamanan sistem informasi klinik dilihat dari aspek kerahasiaan belum cukup baik. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*.

Aspek nir-sangkal pada sistem informasi klinik MP ditunjukkan dengan fungsi sistem informasi klinik yang dapat merekam jejak perubahan (penambahan maupun pengurangan) data yang dilakukan oleh *user*. Para *user* tidak dapat menyangkal perubahan yang ia lakukan karena seluruh aktivitas yang dilakukan akan terekam secara otomatis dalam sistem. Rekaman jejak tersebut hanya dapat dibuka oleh tim *IT*. Hal yang sama juga disampaikan oleh Nugrahaeni dan Nurhayati (2018) bahwa aspek nir-sangkal *(non repudiation)* dibuktikan dengan identifikasi terhadap pihak yang melakukan pengisian dan perubahan informasi.

Berdasarkan kegiatan observasi, ditemukan ketidaksesuaian implementasi aspek keamananan sistem informasi yakni *user* masih saling bertukar informasi terkait *id user* dan *password*-nya. Selain itu, satu *id user* digunakan oleh beberapa orang juga sangat biasa dilakukan. Hal ini tentu saja akan berakibat fatal jika terjadi kesalahan penginputan, dimana menyulitkan untuk proses identifikasi pelaku.

Kesimpulan

Berdasarkan hasil penilaian *Gap Analysis : Status of ISO 27001 Implementation – Checklist*, maka diperoleh kesimpulan aspek kemanan informasi dalam penerapan rekam medis elektronik di klinik *Medical Check-Up* MP adalah sebagai berikut : 1) Persentase pencapaian aspek kerahasiaan (*privacy*) adalah 60%. Hal ini disebabkan oleh belum dilakukannya audit *ISO 27001* dan belum dilakukannya audit internal secara resmi, *gap* (temuan) yang terjadi hanya dibahas melalui *meeting* dan diselesaikan saat itu juga; 2) Persentase pencapaian aspek integritas *(integrity)* adalah 31%. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*; 3) Persentase pencapaian aspek autentikasi (*authentication*) adalah 48%. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*, selain itu jika terdapat temuan ketidaksesuaian hanya dibahas dalam pertemuan saja tanpa pencatatan atau pembuatan berita acara untuk evaluasi di masa mendatang; 4) Persentase pencapaian aspek ketersediaan (*availability*) adalah 25%. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*; 5) Persentase pencapaian aspek kontrol akses (*access control*) adalah 56%. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*; 6) Persentase pencapaian aspek nir-sangkal (*non repudiation*) adalah 33%. Hal ini disebabkan oleh perusahaan belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*.

Daftar Pustaka

1. Siagian S. Analisis Ancaman Keamanan Pada Sistem Informasi Manajemen di Rumah Sakit Rimbo Medica Jambi 2015. 2015;4(March, 2016). Available from: https://s3.amazonaws.com/academia.edu.documents/57094957/163-Article_Text-265-1-10-20180417.pdf?response-content-disposition=inline%3B filename%3DANALISIS_ANCAMAN_KEAMANAN_PADA_SISTEM_IN.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y
2. Ningtyas AM, Lubis IK. Literatur Review Permasalahan Privasi pada Rekam Medis Elektronik. 2018;V. Available from: https://ejournal.unib.ac.id/index.php/pseudocode/article/view/5902 diakses pada 14 November 2019
3. Badan Siber dan Sandi Negara. Urgensi Struktur Organisasi Keamanan Informasi pada Sektor Kesehatan. 2019; Available from: https://bssn.go.id/urgensi-struktur-organisasi-keamanan-informasi-pada-sektor-kesehatan/ diakses pada 14 November 2019
4. Akbar D. Lima Kasus Cybersecurity yang Paling Heboh Sepanjang Tahun 2017 [Internet]. 26 Mei. 2018. Available from: https://infokomputer.grid.id/read/12708655/lima-kasus-cybersecurity-yang-paling-heboh-sepanjang-tahun-2017?page=all
5. Neidig S. Is Zoom HIPAA Compliant? [Internet]. 5 April. 2019. Available from: https://gazelleconsulting.org/is-zoom-hipaa-compliant/
6. Amatayakul MK. Electronic Health Record A Practical Guide For Professionals And Organizations. Fifth Edit. Chichago: AHIMA; 2013.
7. Chazar C. Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. 2015;VII No. 2. Available from: http://informasi.stmik-im.ac.id/wp-content/uploads/2016/05/04-Chalifa.pdf
8. Rahardjo B. Dalam Rekam Medis Pasien (Studi Kasus di Rumah Sakit Islam AT-TIN HUSADA Ngawi Jawa Timur). 2019;02(01):1–8.
9. Nugraheni SW. Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi Legal Aspects of Electronic Medical Record in RSUD Dr Moewardi ada dua , yaitu aspek finansial dan aspek legal dan security . Secara umum rekam medis. 2018;1:92–7.
10. Sugiyono. Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta; 2013.