TESIS

EVALUASI FITUR KEAMANAN DATA PADA SISTEM INFORMASI RAWAT JALAN BERBASIS KOMPUTER di RS Dr.KARIADI SEMARANG

Magister Ilmu Kesehatan Masyarakat
Konsentrasi Sistem Informasi Manajemen Kesehatan

Rano Indradi Sudra
E.4A099024

PROGRAM PASCASARJANA
UNIVERSITAS DIPONEGORO
SEMARANG
2003

PENGESAHAN TESIS

EVALUASI FITUR KEAMANAN DATA
PADA SISTEM INFORMASI RAWAT JALAN
BERBASIS KOMPUTER
di RS Dr.KARIADI SEMARANG

Dipersiapkan dan disusun oleh

Rano Indradi Sudra
E.4A099024

Telah dipertahankan dihadapan Tim Penguji
pada tanggal 8 Juli 2003
dan dinyatakan telah memenuhi syarat untuk diterima.
Menyetujui

Pembimbing I

dr.H.Bambang Shofari, MMR
NIP.140 170 075

Pembimbing II

Ir.Kodrat IS, MT
NIP.132 046 696

Penguji

Ir.Edi Noersasongko, M.Kom

Penguji

dra.Atik Mawarni, M.Kes
NIP.131 918 670

Ketua Program Studi

Magister Ilmu Kesehatan Masyarakat

Universitas Diponegoro

dr.Sudiro, MPH, Dr.PH
NIP. 131 252 965

TESIS

EVALUASI FITUR KEAMANAN DATA PADA SISTEM INFORMASI RAWAT JALAN BERBASIS KOMPUTER di RS Dr.KARIADI SEMARANG

Magister Ilmu Kesehatan Masyarakat
Konsentrasi Sistem Informasi Manajemen Kesehatan

Rano Indradi Sudra
E.4A099024

PROGRAM PASCASARJANA
UNIVERSITAS DIPONEGORO
SEMARANG
2003

PERNYATAAN

Dengan ini saya menyatakan bahwa tesis ini adalah hasil pekerjaan saya sendiri dan didalamnya tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi & lembaga pendidikan lainnya. Pengetahuan yang diperoleh dari hasil penelitian maupun yang belum / tidak diterbitkan, sumbernya dijelaskan di dalam tulisan & daftar pustaka.

Semarang, Juli 2003

Rano Indradi Sudra

RIWAYAT HIDUP

Nama : Rano Indradi Sudra

Tempat lahir : Bandung

Tanggal lahir : 27 Desember 1965

Agama : Islam

Alamat : Jl.Kauman 50 Majapahit – Semarang

Pendidikan :

- Mengikuti Program Pascasarjana MIKM UNDIP konsentrasi SIMKES mulai tahun 1999
- Lulus Fakultas Kedokteran UNDIP tahun 1992
- Lulus SMU Negeri 1 Semarang tahun 1984
- Lulus SMP Negeri 3 Semarang tahun 1981
- Lulus SD St.Yusup Semarang tahun 1978

Untuk teman sejatiku, EMH,

semoga Allah SWT menjadikanmu wanita sholehah

yang senantiasa dan semakin dicintaiNya.

Amin.

DAFTAR ISI

Halaman

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamin, segala puji hanya bagi Allah SWT yang telah melimpahkan rahmat dan petunjukNya sehingga penyusunan tesis untuk memenuhi sebagian persyaratan guna mencapai derajat S-2 Magister Ilmu Kesehatan Masyarakat (MIKM) Konsentrasi Sistem Informasi Manajemen Kesehatan (SIMKES) UNDIP ini dapat selesai.

Rasa terima kasih yang tulus dan penghargaan yang tinggi kami sampaikan untuk segala bentuk bimbingan, masukan dan bantuan yang telah diberikan dengan penuh kesabaran, kesungguhan dan kepercayaan dari pembimbing yang terhormat dr.H.Bambang Shofari, MMR selaku pembimbing I dan Ir.Kodrat.IS, MT selaku pembimbing II.

Terima kasih dan penghargaan yang tulus pula kami sampaikan utuk saran dan arahan dari tim penguji tesis yaitu Ir.Edi Noersasongko, M.Kom dan dra.Atik Mawarni, M.Kes.

Terima kasih dan penghargaan yang tulus untuk yang terhormat Direktur Program Pascasarjana UNDIP, Dosen dan Pengelola Prodi IKM, Ketua Konsentrasi SIMKES beserta Bapak / Ibu dosen dan staf untuk kesempatan, fasilitas dan bantuan selama mengikuti pendidikan di MIKM ini.

Terima kasih yang tulus dan penghargaan yang tinggi juga kami sampaikan kepada Ketua Yayasan Dian Nuswantoro, Rektor Universitas Dian Nuswantoro

(UDINUS) dan Dekan Fakultas Kesehatan Masyarakat UDINUS yang telah memberi kesempatan untuk menempuh pendidikan jenjang S-2 di MIKM UNDIP.

Terima kasih pula kepada Direktur, Manajer Divisi SIM RS & Kom, Asisten Manajer Divisi SIM RS & Kom, Manajer Divisi RM & Medikolegal, beserta seluruh Asisten Manajer dan staf rekam medis RS Dr.Kariadi yang telah memberi ijin, dukungan, bantuan dan masukan dalam segala bentuknya.

Terima kasih disertai cinta kasih yang tulus untuk teman sejatiku – EMH, yang menjadi sumber api semangat terbesar untuk menyelesaikan penyusunan tesis ini.

Sadar bahwa tesis ini masih belum sempurna, kami sangat mengharapkan kritik dan saran yang membangun guna penyempurnaannya.

Semoga penyusunan tesis ini dapat memberi manfaat bagi pembaca dan bagi pengembangan keilmuan SIMKES di Indonesia. Amin.

Semarang, Juli 2003

Penulis

DAFTAR GAMBAR

DAFTAR LAMPIRAN

Nomor

DAFTAR SINGKATAN dan ISTILAH

AKS	: Administrator Keamanan Sistem
Backup	: proses penyalinan data atau perangkat lunaknya
CD	: Compact Disc, piringan yang digunakan sebagai media penyimpan data atau perangkat lunak
Coding	: penentuan dan pemberian kode untuk penyakit atau tindakan medis
Copy	: proses penyalinan
CPR	: Computer-based Patient Record
Diskless	: tanpa penggerak disk (disk drive)
EHR	: Electronic Health Record
EMRs	: Electronic Medical Records
Evaluation	: evaluasi, proses penilaian hasil dari suatu proyek setelah dioperasionalkan dalam kurun waktu tertentu, dari beberapa bulan hingga beberapa tahun bergantung kepada tipe proyeknya
Field	: kolom data / ruang pengisian data
File	: berkas (manual maupun elektronik)
Filing	: penyimpanan dan penjajaran rekam medis
Gb	: Giga byte
Harddisk	: salah satu bentuk media penyimpanan data
ICD	: International Classification of Disseases
Idle time	: waktu tunggu / waktu sela

Interface : kartu antar muka pada perangkat komputer

Kb : Kilo byte

KIB : Kartu Identitas Berobat

KIP : Kode Identitas Pengguna

KIUP : Kartu Indeks Utama Pasien

LAN : Local Area Network

Log file : berkas (manual maupun elektronik) yang berisi hasil pemantauan dan pencatatan kegiatan akses komputer / jaringan komputer

Login : tahap awal yang harus dilewati oleh pengguna komputer / jaringan komputer untuk pengesahan penggunaan

Logout : tahap pengakhiran penggunaan komputer / jaringan komputer

MHz : Mega Herz

Password : kata kunci yang seharusnya hanya diketahui oleh pemiliknya dan digunakan untuk menyatakan keberadaannya sebagai pengguna sistem yang sah

RAM : Random Access Memory

Required field : ruang isian data yang harus diisi (tidak boleh kosong)

Review : proses monitoring dan penyelesaian proyek yang dilaksanakan selama proyek pengembangan sistem sedang dilaksanakan sampai selesai

RM : Rekam medis

RS : Rumah sakit

Server	: komputer yang bertindak sebagai pusat kendali proses dan data dalam suatu jaringan
SIM-RS	: Sistem Informasi Manajemen Rumah Sakit
SI-RJ	: Sistem Informasi Rawat Jalan
Tipologi star	: salah satu bentuk koneksi jaringan komputer
TPPRJ	: Tempat Pendaftaran Pasien Rawat Jalan
URJ	: Unit Rawat Jalan
USB	: Universal Serial Board
Workstation	: komputer yang bertindak sebagai stasiun kerja dalam suatu jaringan

Program Magister Ilmu Kesehatan Masyarakat
Universitas Diponegoro
Semarang
Konsentrasi Sistem Informasi Manajemen Kesehatan
2003

ABSTRAK

Rano Indradi Sudra

Evaluasi Fitur Keamanan Data Pada Sistem Informasi Rawat Jalan Berbasis Komputer Di RS Dr.Kariadi Semarang
xvii + 102 + 5 gambar + 7 lampiran

Pengelolaan aspek keamanan data dalam sistem informasi kesehatan berbasis komputer merupakan kombinasi dari segi teknologi dan segi organisasi. RS Dr.Kariadi telah mengimplementasikan Sistem Informasi Rawat Jalan (SI-RJ) berbasis komputer sejak tahun 1997 dan hingga saat ini belum pernah melakukan evaluasi secara terstruktur terhadap aspek keamanan data dan informasi yang dikelola di dalamnya.

Penelitian ini bertujuan untuk mengetahui kinerja fitur keamanan data dalam SI-RJ berbasis komputer di RS Dr.Kariadi dari segi teknologi dan segi organisasi. Penelitian ini dilaksanakan dengan metode deskriptif evaluatif melalui observasi dan wawancara dengan pendekatan *cross sectional.* Hasil penelitian dianalisis dengan menggunakan metode content analysis dan mengacu pada hasil analisis pada penelitian sebelumnya oleh Computer-based Patient Record Institute (1999) dan National Academy of Sciences (1997).

Hasil penelitian menunjukkan bahwa fitur keamanan data telah digunakan dalam SI-RJ berbasis komputer dengan penyesuaian terhadap tingkat kemampuan sistem, pengetahuan; sikap; dan praktek (etos kerja) pengguna, serta dukungan komitmen pihak manajemen. Namun sistem ini masih belum memenuhi kriteria fitur keamanan data berbasis komputer sehingga belum berfungsi secara penuh dalam menjaga keamanan data dan informasi yang terkandung dalam sistem tersebut.

Untuk meningkatkan dan memperbaiki kinerja fitur-fitur ini, perlu kebijakan pendukung yang khusus diterbitkan untuk mendasari pengelolaan dan penggunaan sistem. Pelatihan untuk membentuk pengetahuan; sikap; dan praktek (etos kerja) yang menunjang *privacy* dan *security* juga perlu dilaksanakan. Penggunaan segi teknologi dan *anonymous patient IDs* serta pemilihan tempat penyimpanan fisik media penyimpan data akan dapat meningkatkan kinerja fitur saat ini.

Kata kunci : kerahasiaan, keamanan, informasi, medis, komputer
Kepustakaan : 17, 1989-2002

Master's Degree Program of Public Health Science
Majoring on Health Information Management System
Diponegoro University
Semarang
2003

ABSTRACT

Rano Indradi Sudra
Evaluation of Data Security Features in Computer-based Outpatient Information System in Dr.Kariadi Hospital Semarang
xvii + 102 pages + 5 figures + 7 appendixes

Data security in computer-based outpatient information system is build by the combination of technological and organizational aspect. Computer-based outpatient information system in Dr.Kariadi Hospital has been implemented since 1997 and never have been evaluated structurally yet until now.

The aim of this research was to evaluate the performance of data security features in computer-based outpatient information system in Dr.Kariadi hospital, from technological and organizational aspect. Descriptive-evaluative method was used in this research. Observation and interview were done by cross sectional approach. Content analysis was used to analyze the data and the result will be compare with the result of research from Computer-based Patient Record Institute (1999) and National Academy of Sciences (1997).

This research shows that the data security features have been used within the computer-based outpatient information system with customization to system, user's work ethos and the compliment of the management commitment. The data security features within the system are not comply with the standard yet. This condition makes the performance of the data security of the system is not strong enough to protect data and information stored in the system.

Policies that focus on basic maintenance and usage of computer-based outpatient information system are needed to improve the performance of data security features. The users also need to trained in work ethos related to privacy and security of medical records. The effective use of technological aspect, anonymous patient IDs and the right choose of location to keep data storage media would increase the performance of data security features.

Keyword : confidentiality, security, information, medical, computer
Reference : 17, 1989-2002

BAB I

PENDAHULUAN

1.1 Latar belakang

Teknologi informasi telah berkembang dan menjadi bagian yang sangat penting bagi industri kesehatan, termasuk upaya untuk menurunkan biaya pelayanan dan meningkatkan kualitas pelayanan. Secara umum, estimasi biaya yang dibelanjakan oleh industri kesehatan untuk bidang teknologi informasi mencapai 10-15 juta dolar AS pada tahun 1996. Sistem informasi rumah sakit (*Hospital Information System / HIS*) turut berkembang seiring dengan perkembangan teknologi informasi. HIS merupakan integrasi berbagai sistem dalam pelayanan kesehatan di rumah sakit, misalnya sistem rekam medis, sistem penagihan pembayaran, sistem farmasi, sistem akuntansi rumah sakit, dan sebagainya. Catatan pelayanan kesehatan yang bersifat komprehensif ini meliputi berbagai hal, misalnya data status kesehatan pasien, data yang dibutuhkan oleh penanggung biaya (asuransi), data sosial administratif, dan sebagainya. Data pelayanan kesehatan ini pada saatnya akan dibutuhkan oleh berbagai pihak untuk berbagai keperluan, antara lain oleh pihak menejemen rumah sakit, keuangan, pendidikan dan penelitian, asuransi, dan kepolisian. Pusat dari semua inisiatif perkembangan ini adalah pengembangan dan implementasi rekam medis elektronik (*electronic medical records (EMRs) / computer-based patient record (CPR)*). CPR menjadi pusat informasi klinis dan administrasi yang berkaitan dengan pelayanan pasien. Dalam perannya untuk memperlancar proses administrasi, CPR memegang

peranan penting untuk peningkatan pelayanan. Hal ini diperkirakan akan terus berkembang seiring dengan pembaruan sistem administrasi dan pembayaran, penerapan sistem jaringan internal untuk penggunaan informasi bersama, serta penggunaan jaringan umum seperti internet untuk mendistribusikan informasi yang berkaitan dengan kesehatan dan memungkinkan akses terhadap basis data klinis dari jarak jauh.(National Academy of Sciences, 1997; Skurka, M F, 1994)

Sejalan dengan hal tersebut diatas, maka sejak tahun 1997 RS Dr. Kariadi telah mengaplikasikan sistem informasi rawat jalan berbasis komputer. Sebagai rumah sakit rujukan tingkat lanjut untuk wilayah Indonesia bagian Tengah-Utara dengan jumlah kunjungan rawat jalan mencapai 1000 pasien per harinya, maka pengaplikasian sistem informasi rawat jalan berbasis komputer ini sangat diharapkan dapat menunjang kelancaran proses pelayanan kesehatan.

Dalam suatu organisasi, sistem informasi elektronik dan EMRs berpotensi untuk disalahgunakan oleh pengguna yang sah maupun yang tidak sah. Mereka dapat melanggar aturan akses terhadap informasi pasien, untuk kepentingan pribadi maupun untuk keuntungan ekonomi. Pengguna yang sah dapat menyalahgunakan hak akses mereka untuk mendapatkan informasi yang sebenarnya tidak berhak untuk mereka lihat (misalnya informasi yang berkaitan dengan teman, saudara, atau selebritis), atau mereka bisa jadi menyebarluaskan informasi tersebut kepada orang lain. Pengacau dari luar organisasi bisa juga "masuk" ke sistem informasi berbasis komputer untuk

mencuri, merusak, atau mengacaukan fungsi sistem sehingga sistem tersebut tidak bisa lagi dimanfaatkan oleh pengguna yang sah, misalnya dokter atau petugas lainnya, untuk mendapatkan informasi yang penting bagi pelayanan pasien.

Suatu sistem yang menerapkan terlalu sedikit sarana pengendalian keamanan data bisa menimbulkan kerugian operasional akibat gangguan keamanan yang mungkin timbul. Sebaliknya, sistem yang memiliki terlalu banyak sarana pengendalian keamanan datanya bisa menimbulkan gangguan operasional akibat melambatnya kinerja sistem tersebut.(Computer-based Patient Record Institute, 1999; Whitten J L dkk, 1989)

Pengelolaan aspek keamanan data dalam informasi kesehatan elektronik merupakan kombinasi dari segi teknologi dan segi organisasi. Metoda yang dipilih untuk ini akan berdampak pula terhadap biaya, kompleksitas, dan tingkat keamanan yang dihasilkan. Dalam hal ini, peranan kedua segi tersebut sama pentingnya. Segi teknologi dapat didayagunakan untuk mengendalikan otentikasi dan otorisasi pengguna (*authentication & authorization*), penelusuran jejak penggunaan sistem (*audit trails*), pemulihan gangguan sistem pasca bencana (*disaster recovery*), serta pengaturan penyimpanan dan transmisi data yang aman (*secure data storage & transmission*). Segi organisasi sangat berperan dalam hal menentukan kebijakan formal, memformulasikan struktur untuk mengembangkan dan mengimplementasikan kebijakan dan prosedur, mengatur pelaksanaan pendidikan dan pelatihan karyawan / petugas, serta menentukan prosedur

untuk memonitor dan sangsi terhadap pelanggaran kebijakan privasi dan keamanan data.(National Academy of Sciences, 1997)

Sebagai rumah sakit yang telah mengaplikasikan sistem informasi rawat jalan berbasis komputer, RS Dr.Kariadi selayaknya mempertimbangkan kemungkinan timbulnya ancaman terhadap *privacy* dan *security* data pasien yang dikelolanya. Ancaman ini dapat diantisipasi dengan mendayagunakan fitur-fitur keamanan data dalam sistem informasi berbasis komputer. Penerapan fitur keamanan segi teknologi secara benar memerlukan pemantauan dan evaluasi dalam pelaksanaannya, agar fitur-fitur tersebut dapat berfungsi dengan baik dan benar.

Sebuah survey tentang kecenderungan dan penggunaan EHR terhadap 477 responden telah dilaksanakan oleh Medical Records Institute sebagai rangkaian kegiatan dalam *Toward an Electronic Patient Record Conference.* Beberapa hasil dari survey ini yang patut dicermati berkaitan dengan keamanan informasi rekam kesehatan pasien, antara lain menyatakan bahwa fokus pemikiran utama dalam penerapan dan operasional EHR menunjukkan :

a. akses informasi rekam kesehatan oleh yang tidak berwenang : 59%
b. akses informasi rekam kesehatan yang tidak semestinya oleh pengguna sah dari dalam organisasi : 47%
c. pelanggaran terhadap peraturan dan kebijakan keamanan data : 46%
d. akses yang tidak semestinya oleh pengguna sah dari luar organisasi : 32%
e. penerapan keamanan data yang tidak adekuat : 29% (Medical Records Institute, 2001)

RS Dr.Kariadi selayaknya memiliki kebijakan dalam hal penggunaan sistem ini. Demikian pula dengan prosedur pengoperasian sistem dan deskripsi tugas personalia sub bagian rekam medis unit rawat jalan. Dokumen-dokumen ini sangat penting untuk kepastian tanggung jawab dalam operasional sistem yang ada. Tanpa adanya dukungan pihak manajemen puncak yang diwujudkan dalam bentuk penerbitan dokumen-dokumen tersebut, maka keterikatan moral, ketaatan, dan kepastian tanggung jawab penggunaan sistem menjadi lemah, atau bahkan tidak jelas lagi siapa yang bertanggung jawab terhadap suatu keadaan / gangguan yang timbul.

Sejak diaplikasikan, belum pernah dilakukan evaluasi terhadap sistem tersebut, terutama terhadap aspek keamanan datanya. Evaluasi ini sangat penting mengingat data yang dikelola disini adalah data pasien dari hasil pelayanan kesehatan yang telah dilakukan. Hal ini dapat menimbulkan kerugian materi (perangkat keras, dana) maupun non-materi (data, informasi) apabila terjadi gangguan atau kerusakan data baik karena bencana maupun karena kesengajaan pengguna.

1.2 Perumusan masalah

Bagaimana kinerja fitur keamanan data dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.3 Manfaat penelitian

1.3.1 Bagi RS Dr.Kariadi

Sebagai bahan masukan mengenai kinerja fitur keamanan data dalam sistem informasi rawat jalan berbasis komputer yang telah diimplementasikan selama lima tahun ini. Rekomendasi hasil evaluasi ini juga dapat digunakan untuk *maintenance* sistem tersebut guna memperbaiki dan meningkatkan fitur keamanan data agar *privacy* dan *security* informasi kesehatan dalam sistem tersebut semakin terjaga.

1.3.2 Bagi Pengembangan Ilmu Pengetahuan

Sebagai referensi pustaka hasil penelitian dalam bidang sistem informasi manajemen kesehatan, khususnya mengenai evaluasi sistem informasi berbasis komputer dalam administrasi pelayanan kesehatan.

Dengan mengadopsi dan memodifikasi instrumen evaluasi untuk penelitian sejenis yang telah digunakan dan diakui dalam profesi *Health Information Management* maka instrumen penelitian dan instrumen analisa dalam penelitian ini dapat menjadi masukan bagi peneliti lain untuk lebih dikembangkan dalam bidang serupa, khususnya di Indonesia.

1.3.3 Bagi peneliti

Sebagai wahana untuk mengaplikasikan keilmuan yang telah dipelajari dibidang sistem informasi manajemen kesehatan dan pelayanan kesehatan berbasis komputer.

1.4 Tujuan penelitian

1.4.1 Tujuan umum

Mengetahui kinerja fitur keamanan data dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.4.2 Tujuan khusus

1.4.2.1 Mengetahui kinerja fitur otentikasi (*authentication*) dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.4.2.2 Mengetahui kinerja fitur otorisasi (*authorization*) dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.4.2.3 Mengetahui kinerja fitur integritas (*integrity*) dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.4.2.4 Mengetahui kinerja fitur penelusuran jejak (*audit trails*) dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.4.2.5 Mengetahui kinerja fitur pemulihan pasca bencana (*disaster recovery*) dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.4.2.6 Mengetahui kinerja fitur penyimpanan dan transmisi data yang aman (*secure data storage & transmission*) dalam sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi Semarang.

1.5 Keaslian penelitian

Sebuah penelitian yang dilakukan oleh Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure (1997) menunjukkan beberapa hal penting antara lain :

1. organisasi pelayanan kesehatan perlu segera meningkatkan aspek keamanan pada sistem informasi kesehatan yang digunakan untuk meningkatkan perlindungan terhadap informasi kesehatan berbasis komputer,
2. organisasi pelayanan kesehatan terlalu lamban dalam mengaplikasikan sistem keamanan yang kuat,
3. keamanan sistem informasi kesehatan berbasis komputer masih rentan, baik terhadap pengguna yang sah yang menyalahgunakan hak mereka untuk melakukan hal yang dilarang maupun terhadap pengguna yang tidak sah yang "masuk" dan mencuri informasi atau merusak sistem,
4. pengamanan yang adekuat terhadap sistem informasi kesehatan berbasis komputer bergantung kepada segi teknologi dan organisasi.(National Academy of Sciences, 1997)

Untuk melakukan evaluasi terhadap aspek keamanan data dalam sistem informasi kesehatan berbasis komputer dibutuhkan suatu instrumen yang bisa digunakan untuk menilai baik segi teknologi maupun segi organisasinya. Instrumen yang akan digunakan dalam penelitian ini mengadopsi dan memodifikasi instrumen dari penelitian sejenis yang telah digunakan oleh *National Academy of Sciences* di Washington DC tahun 1997,

Computer-based Patient Record Institute di Bethesda tahun 1999, dan juga digunakan oleh *Medical Record Institute* di Newton MA tahun 1999, serta penelitian yang dilaksanakan oleh *UK Institute of Helath Informatics (Project Review and Objective Evaluation for Electronic Patient and Health Record Projects)* di Winchester tahun 2001. Metode penelitian yang digunakan oleh lembaga-lembaga tersebut beserta hasil penelitiannya telah diakui dan menjadi referensi resmi dalam profesi Manajemen Informasi Kesehatan di dunia.(National Academy of Sciences, 1997; Computer-based Patient Record Institute, 1999; Medical Records Institute, 2001; Heather H dkk, 2001)

Berbeda dengan beberapa penelitian terdahulu seperti telah disebutkan diatas, dalam penelitian ini tidak dilakukan uji langsung terhadap sistem. Uji sistem yang bersifat mengintervensi sistem ini tidak dapat dilaksanakan karena tidak diijinkan oleh penanggung jawab sistem informasi di RS Dr. Kariadi. Dengan demikian, penelitian hanya dapat dilaksanakan dengan cara mengamati sistem yang sedang berjalan dan melengkapi informasi yang diperlukan dengan melakukan wawancara terhadap subyek penelitian.

Penelitian ini juga berbeda dengan penelitian terdahulu dalam hal fokus penelitiannya. Dalam penelitian ini fokus yang akan diambil adalah aspek keamanan data dalam sistem, sedangkan dalam penelitian sebelumnya berfokus pada manfaat dan *outcome* implementasi sistem dan persepsi pengguna.

Masukan berupa rekomendasi dari hasil evaluasi ini diharapkan akan menjadi dasar perawatan dan pengembangan selanjutnya dari sistem yang

telah diaplikasikan. Instrumen yang digunakan dalam penelitian inipun selanjutnya diharapkan akan dapat dikembangkan dan didayagunakan oleh peneliti lain untuk melakukan evaluasi serupa terhadap sistem informasi kesehatan berbasis komputer di rumah sakit lainnya. Pengembangan instrumen ini sebaiknya diarahkan untuk menghasilkan instrumen evaluasi keamanan data dalam berbagai tingkat sistem informasi, sesuai dengan tingkat teknologi yang diterapkan dalam sistem tersebut. Hal ini mengingat masih sangat beragamnya bentuk, lingkup, dan tingkat teknologi yang diaplikasikan di berbagai rumah sakit di Indonesia.

BAB II

TINJAUAN PUSTAKA

2.1 Sistem Informasi Rawat Jalan (SI-RJ)

Dalam sistem pelayanan kesehatan di rumah sakit, tempat pendaftaran pasien rawat jalan (TPPRJ) merupakan tempat kontak pertama antara calon pasien dan rumah sakit. Di TPPRJ, data yang berkaitan dengan identitas dan tujuan kunjungan pasien sudah mulai "ditangkap" dan direkam untuk selanjutnya menjadi bagian dari kesatuan berkas rekam medis (RM) pasien yang bersangkutan.

Meskipun data pasien yang dicatat di TPPRJ bersifat data administratif, namun tetap bersifat rahasia sesuai dengan PP no.10 tahun 1966 tentang Wajib Simpan Rahasia Kedokteran.

Sebagai bagian dari rangkaian pelayanan kesehatan, TPPRJ merupakan tempat pemberian dokumen RM baru sekaligus penentuan nomor RM bagi pasien baru (kunjungan pertama). Pencarian nomor RM bagi lama (kunjungan ulang) juga dilakukan di TPPRJ dengan menggunakan kartu indeks utama pasien (KIUP) baik secara manual maupun elektronis.

Dengan memperhatikan hal-hal tersebut diatas, maka dapat dilihat bahwa tugas pokok dan fungsi TPPRJ adalah :

1. pintu masuk pertama dalam penerimaan dan pendaftaran rawat jalan,
2. memberi informasi yang lengkap kepada pasien dan keluarganya tentang pelayanan di rumah sakit,
3. mencatat identitas pasien dengan jelas, lengkap, dan benar,

4. membubuhkan nomor RM pada setiap berkas RM,
5. membuat kartu identitas berobat (KIB) dan KIUP bagi pasien baru,
6. mencari nomor RM lama bagi pasien kunjungan ulang, dan
7. mendistribusikan dokumen RM ke unit rawat jalan (URJ).

Data yang dicatat di TPPRJ selanjutnya akan diolah untuk menghasilkan berbagai informasi yang diperlukan oleh pihak manajemen rumah sakit. Beberapa informasi tersebut misalnya jumlah kunjungan pasien rawat jalan, rasio kunjungan pasien baru dan lama, rasio kunjungan pasien poli umum dan spesialis, jumlah pasien rujukan, pemetaan area cakupan pelayanan, jumlah kunjungan pasien tertanggung asuransi kesehatan, jumlah pelayanan yang dilakukan oleh masing-masing dokter di unit rawat jalan, jumlah pendapatan karcis; pendapatan dari tindakan; dan pendapatan total dari pelayanan rawat jalan, jumlah kunjungan per kelompok usia, dan sebagainya. Untuk dapat menghasilkan berbagai informasi penting tersebut, maka dibutuhkan suatu sistem informasi rawat jalan yang berfungsi untuk menangkap dan mencatat data (*capture*), menyimpan (*storage*), mengolah (*process*), menampilkan (*presentation*), transmisi (*transmition*), pelepasan informasi (*disclosure*), dan pemusnahan data. Keseluruhan fungsi sistem informasi rawat jalan ini dapat dilakukan secara manual maupun elektronis. Teknologi komputer dan informatika yang telah berkembang pesat saat ini sangat memungkinkan penerapan dan pemanfaatan berbagai perangkat keras dan lunak untuk membangun sistem informasi rawat jalan berbasis komputer.(Medical Records Institute, 2001; Shofari B, 1998)

2.2 Rekam Kesehatan Berbasis Elektronik (*Electronic Health Record / EHR*)

2.2.1 Definisi

Computer-based Patient Record Institute (1999) mendefinisikan EHR / Computer-based Patient Record (CPR) sebagai pengelolaan informasi berbasis komputer terhadap status kesehatan dan pelayanan kesehatan sepanjang hidup seorang individu. Hal ini tidak berarti bahwa EHR hanya mengubah bentuk rekam medis berbasis kertas menjadi lembar formulir elektronik saja, tapi meliputi semua bentuk media yang digunakan dalam informasi kesehatan. Jadi, EHR meliputi riwayat medis, penatalaksanaan yang sedang diberikan, hasil pemeriksaan laboratorium, gambar x-ray, dan sebagainya.

Rekam kesehatan berbasis elektronik dapat menunjang aktifitas perekaman data (*capture*), penyimpanan data (*storage*), pengolahan data (*processing*), komunikasi data (*communication*), keamanan data (*security*), dan penyajian informasi kesehatan (*presentation of health information*). Rekam kesehatan berbasis elektronik juga memungkinkan penyediaan kemampuan yang menghasilkan data pasien yang lengkap dan akurat (*complete and accurate patient data*), sistem peringatan dan pengingat klinis (*clinical reminders and alerts system*), sistem penunjang pengambilan keputusan (*decision support system*), serta hubungan keterkaitan dengan sistem penyedia basis data pengetahuan atau data yang terkait (*related data and knowledge bases links*).

2.2.2 Keuntungan

Rekam kesehatan berbasis elektronik memungkinkan akses yang luas-menyeluruh dan tepat waktu untuk mendapatkan informasi kesehatan bagi petugas kesehatan dan pihak lain yang berwenang, dengan tetap menjaga kerahasiaan pribadi pasien dan informasi dari petugas kesehatan. Komputerisasi sangat meningkatkan proteksi terhadap kerahasiaan informasi melalui penerapan kunci dan kendali akses yang memadai. Sistem ini menunjang kesinambungan pelayanan dan berperan sebagai sumber daya bagi pihak manajemen dari sistem pelayanan kesehatan dan untuk pengembangan pengetahuan. (Computer-based Patient Record Institute, 1999; Wilson; Randy, 2000)

Hawkins F (2002) menyimpulkan hasil dari evaluasi yang dilakukannya terhadap implementasi sistem informasi kesehatan berbasis komputer (EHR) bahwa EHR secara signifikan telah meningkatkan hasil dokumentasi rekam medis setelah enam bulan dan satu tahun implementasi. Data klinis dalam EHR menjadi lebih terorganisasi dan lebih mudah didapatkan saat dibutuhkan. Tingkat kelengkapan pengisian data klinis juga meningkat setelah enam bulan dan satu tahun implementasi.

2.2.3 Keamanan

Sejalan dengan perkembangan teknologi informasi dan upaya memenuhi kebutuhan penerapannya dalam sistem pelayanan kesehatan, sudah banyak pihak yang berusaha mengembangkan sistem informasi

pelayanan kesehatan berbasis komputer. Pihak institusi pelayanan kesehatan memiliki kesempatan untuk memilih dan mengimplementasikan aplikasi komputer dan sistem penunjangnya yang komprehensif. Tahap memilih ini dilaksanakan dengan melakukan evaluasi berdasarkan beberapa kriteria tertentu, termasuk salah satunya yaitu fitur keamanannya.

Fitur keamanan data dalam informasi kesehatan elektronik (*electronic health information*) merupakan kombinasi dari segi teknologi dan segi organisasi. Metoda yang dipilih untuk ini akan berdampak pula terhadap biaya, kompleksitas, dan tingkat keamanan yang dihasilkan. Peranan segi organisasi sama pentingnya dengan segi teknologi.

Fitur keamanan dalam sistem ini dibutuhkan untuk menjaga integritas dan konfidensialitas informasi kesehatan yang terkandung didalamnya. Selain itu juga dibutuhkan untuk melindungi privasi pasien dan memenuhi tuntutan kebutuhan perlindungan hukum bagi pasien, petugas kesehatan, serta institusi kesehatan.

Fitur keamanan yang dimaksud meliputi hal-hal sebagai berikut (National Academy of Sciences, 1997) :

1. otentikasi (*authentication*),
2. otorisasi (*authorization*),
3. integritas (*integrity*),
4. penelusuran jejak (*audit trails*),
5. pemulihan pasca bencana (*disaster recovery*),
6. penyimpanan dan transmisi data yang aman (*secure data storage & transmission*).

Keberadaan fitur keamanan ini diharapkan dapat menjaga informasi kesehatan dalam sistem rekam kesehatan berbasis komputer terhadap :

1. akses dari yang tidak berhak,
2. modifikasi yang tidak sah, baik dalam media penyimpan data, selama proses pengolahan data maupun dalam pengiriman data,
3. timbulnya hambatan penggunaan sistem, dan
4. pengambilalihan sistem oleh pengguna yang tidak sah.

Penjagaan informasi kesehatan ini juga termasuk pengawasan akses untuk mendeteksi, mencatat, dan melawan/menahan ancaman-ancaman terhadap sistem. Penjagaan ini dilaksanakan dari mulai lapis terendah dalam transportasi data meliputi kabel, *switch*, *router*, dan *transmitter*, sampai lapis-lapis berikutnya yaitu lapis jaringan (*network layer*), lapis informasi (*information layer*), lapis perangkat lunak (*software application layer*), dan lapis manajerial

(*managerial layer*). Lapis manajerial bertanggung jawab terhadap pengelolaan struktur administrasi dan proses operasional sistem yang semua ini dibutuhkan untuk menjamin dan memantau terlaksananya kebijakan keamanan data.(Computer-based Patient Record Institute, 1999)

Empat prinsip dasar yang harus dipenuhi oleh berkas rekam kesehatan agar dapat diterima sebagai bukti / catatan fakta, yaitu :

1. didokumentasikan sesuai dengan aturan prosedur yang berlaku
2. disimpan sesuai dengan aturan prosedur yang berlaku
3. dibuat pada saat, atau segera setelah pelayanan diberikan
4. dibuat oleh petugas kesehatan yang berwenang (memiliki hak, pengetahuan, dan kemampuan sesuai standar dalam tugasnya)

Empat prinsip dasar tersebut juga berlaku bagi rekam kesehatan berbasis elektronik. Untuk menunjang aspek keakuratan dan kepercayaan dari rekam kesehatan berbasis komputer, *The Comprehensive Guide to Electronic Health Records* merekomendasikan hal-hal berikut ini untuk diperhatikan :

1. jenis komputer yang digunakan dan penerimaannya sebagai peralatan yang standar dan efisien,
2. metode perekaman yang digunakan dalam pengoperasiannya,
3. metode dan keadaan dari persiapan perekaman data, meliputi :
    a. sumber dari informasi;
    b. prosedur untuk memasukkan data/informasi dan untuk mengambil informasi dari komputer;

c. pengendalian dan pengujian untuk memastikan akurasi dan reliabilitas data,

4. keaslian data / informasi yang direkam (belum dimodifikasi).(Austin dkk, 1998; Dougherty dkk, 2002, Merida L J, 2001)

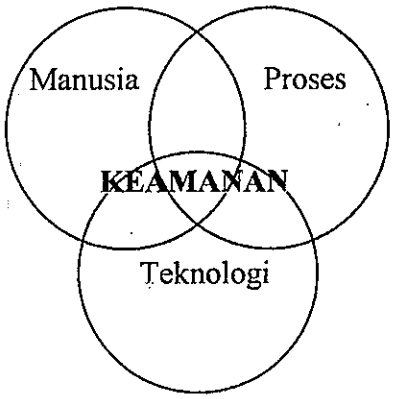
Keamanan dari rekam kesehatan berbasis komputer tidak lepas dari 2 aspek yang saling berkait erat yaitu *privacy* dan *security*. *Privacy* mengandung makna penjagaan keamanan berkas dari pelepasan informasi yang tidak semestinya (*wrongful disclosure*), sedangkan *security* mengandung makna penjagaan berkas dari kerusakan (*destruction*), pengubahan data yang tidak sah (*tampering*), dan gangguan akses (*unavailable access*).(Medical Records Institute, 2001; Woloszyn, William, 2002)

Ancaman terhadap keamanan sistem rekam kesehatan berbasis komputer, baik secara fisik maupun non fisik / informasi, semakin nyata dan komplek. Untuk membangun sistem pengamanan yang handal dan efektif, dibutuhkan langkah yang mengintegrasikan model tradisional dan teknologi informasi. Tiga keuntungan utama yang diharapkan dari integrasi ini yaitu :

1. integritas data: informasi yang dihasilkan akan memiliki akurasi tinggi, sehingga petugas klinis, peneliti, dan petugas kesehatan lainnya menjadi yakin bahwa setiap tindakan yang direkomendasikan sudah berdasarkan data yang valid.
2. kerahasiaan: petugas klinis dan staf lainnya akan lebih tenang dan yakin dalam menjalankan tugasnya, berkaitan dengan adanya peraturan penjagaan keamanan dan kerahasiaan data dalam hal pelepasan informasi.

3. ketersediaan informasi: petugas pelayanan kesehatan akan lebih lancar menjalankan tugasnya bila informasi yang dibutuhkan selalu siap pada saat dibutuhkan.

Kinerja sistem pengamanan data yang baik bergantung kepada tiga komponen esensial, yaitu manusia (*people*), proses (*process*), dan teknologi (*technology*). Ketiga komponen ini dibutuhkan untuk membangun dan mengembangkan sistem pengamanan dan program manajemen resiko.(Medical Records Institute, 2001; Wagner, Lew, 2002)



Gambar 2.1

Tiga sub komponen dalam
keamanan data (Wagner, Lew, 2002)

Jenis-jenis ancaman terhadap keamanan data dalam sistem rekam kesehatan berbasis komputer meliputi :

1. kesalahan pada aspek pengguna (*human error*), termasuk diantaranya yaitu terhapus, kerusakan tak disengaja, pembuangan sampah yang tidak sepatutnya, dan sebagainya
2. gangguan dari alam (*nature*), termasuk api, air, petir, gempa, dan sebagainya

3. gangguan teknis (*technical*), termasuk kegagalan *backup*, kegagalan sistem, virus komputer, kehilangan daya listrik, dan sebagainya
4. tindakan yang disengaja, misalnya mencari informasi diluar kewenang-annya, mengubah data diluar kewenangannya.(Medical Records Institute, 2001; Amatayakul, Margret, 2002)

Setiap bentuk ancaman bisa memiliki karakteristik yang berbeda dalam hal motif, sumber daya, jalur akses, dan kemampuan teknis. Latar belakang karak-teristik yang berbeda-beda ini bisa menimbulkan tingkat resiko yang berbeda dan membutuhkan cara pengendalian yang berbeda pula.(National Academy of Sciences, 1997)

2.3 Fitur Keamanan dalam Rekam Kesehatan Berbasis Komputer

2.3.1 Otentikasi (*authentication*)

Otentikasi mengandung pengertian berkaitan dengan penjaminan / pemastian terhadap identitas suatu subyek atau obyek. Misalnya, pemastian bahwa seorang pengguna yang akan menggunakan sistem adalah memang pengguna yang sah / terdaftar (otentikasi pengguna). Pemastian bahwa sekumpulan sumber data yang diterima adalah sesuai dengan yang dibutuhkan juga merupakan contoh otentikasi, dalam hal ini otentikasi keaslian data.

Metode untuk menerapkan otentikasi yang aman merupakan kebutuhan yang esensial dalam sistem rekam kesehatan berbasis komputer. Setiap pengguna memikul tanggung jawab terhadap informasi

kesehatan yang mereka masukkan, tambahkan, validasi, dan mereka lihat dalam sistem. Oleh karena itu, setiap pengguna harus bisa diidentifikasi secara unik, dibedakan satu dari lainnya. Kebijakan khusus harus diterbitkan oleh pihak institusi untuk mengatur disiplin penggunaan berikut sangsi bagi individu yang membocorkan identitas otentikasinya kepada pengguna lain.

Dengan perkembangan teknologi, saat ini otentikasi dapat berupa sistem identifikasi biometrik, misalnya uji sidik jari; pemindaian retina; dan pengenalan suara. Otentikasi juga bisa berupa penggunaan kartu pintar (*smart card*), *token*, *password*, atau kombinasi dari bentuk-bentuk tersebut. Bentuk yang paling umum digunakan dalam sistem rekam kesehatan berbasis komputer adalah password. Jika password turut dicatat dan disimpan dalam sistem, maka harus diacak (*encrypted*) untuk menjaga keamanannya. Password juga perlu dibatasi penggunaannya dengan menen-tukan batas waktu kedaluarsanya.

Untuk meminimalkan kemungkinan dimana pengguna yang tidak sah memanfaatkan sistem yang sedang aktif yang ditinggalkan oleh pengguna lain yang sah, maka perlu ditunjang dengan kemampuan *automatic logoff* apabila sistem ditinggalkan tanpa aktifitas dalam selang waktu tertentu atau bila pengguna yang sah tersebut mengakses kembali ke dalam sistem melalui terminal kerja yang lain.

2.3.2 Otorisasi (*authorization*)

Otorisasi mengandung pengertian berkaitan dengan pengesahan hak yang meliputi pengesahan akses berdasarkan hak akses.

Otorisasi mengatur lingkup hak dari seorang pengguna yang sah, meliputi hak akses terhadap fungsi sistem dan informasi yang terkandung didalamnya. Otorisasi diperkuat dengan kemampuan kendali akses (*access controls*), pelayanan kerahesiaan (*confidentiality services*), dan pelayanan non-repudiasi (*non-repudiation services*).

2.3.2.1 Kendali akses (*access control*)

Fitur ini melindungi sistem terhadap penggunaan dari yang tidak berhak, termasuk penggunaan sistem komputer, jaringan, aplikasi perangkat lunak, dan berkas (*file*) data. Kendali akses berperan dalam memastikan bahwa pengguna, sistem komputer, dan program hanya dapat menggunakan sumber data yang memang berhak mereka gunakan dan untuk tujuan yang memang menjadi hak mereka. Kendali akses juga melindungi sistem dari penggunaan oleh yang tidak berhak, pelepasan informasi (*disclosure*), modifikasi (*modification*) dan perusakan / penghancuran (destruction) sumber data.

2.3.2.2 Pelayanan kerahasiaan (*confidentiality services*)

Fitur ini menjaga sistem dari kemungkinan pelepasan informasi kepada pihak yang tidak berhak untuk mendapatkan informasi tersebut. Bila kendali akses melindungi file data dalam media penyim-pan dari kemungkinan dibaca oleh pengguna yang tidak berhak, maka pelayanan kerahasiaan menjaga kemungkinan dibacanya file data tersebut diluar media penyimpan data, misalnya setelah digandakan (di*copy*) secara tidak sah. Bentuk paling umum dari fitur ini adalah dengan melakukan penyandian data (*encryption*).

2.3.2.3 Pelayanan non-repudiasi (*non-repudiation services / nrs*)

Fitur ini menjamin terpenuhinya tuntutan pengguna yang dinyatakan maupun yang ditampilkan, baik yang berasal dari *nrs* maupun yang bukan. Repudiasi mengandung pengertian dimana pengguna secara tidak sengaja menginterupsi atau membatalkan proses yang tengah berlangsung. Dengan kata lain, *nrs* mencegah pengguna dari kemungkinan memodifikasi data / informasi secara sepihak atau membatalkan proses transaksi data yang tengah berlangsung, yang mana hal ini dapat menyebabkan kerusakan data.

Penggunaan *anonymous patient IDs* merupakan metode untuk mengatur tampilan informasi baik di layar komputer maupun di kertas dengan hanya mencantumkan nomor rekam medis atau kode identitas

lain tanpa menampilkan nama pasien. Penerapan metode ini dapat mengurangi kemungkinan bocornya informasi kepada pihak yang tidak berwenang atau tidak perlu mengetahui. (National Academy of Sciences, 1997)

2.3.3 Integritas (*integrity*)

Integritas mengandung pengertian bahwa informasi yang tersedia hanya diubah / diolah untuk kebutuhan tertentu dan oleh pengguna tertentu yang berhak. Pengertian ini dapat diterapkan pada data (*data integrity*), program (*program integrity*), sistem (*system integrity*), dan jaringan komputer (*network integrity*).

Integritas data berkaitan dengan akurasi (*accuracy*), konsistensi (*consistency*), dan kelengkapan (*completeness*) dari data. Hal ini terkait secara langsung dengan kualitas data yang bersangkutan dan dapat berpe-ngaruh terhadap kualitas pelayanan kesehatan yang diberikan. Pemantauan integritas data harus dapat memastikan bahwa data tidak diubah atau dirusak melalui cara yang tidak sah. Kebijakan pengendalian integritas data memiliki empat komponen esensial yaitu pemantauan keamanan (*security measures*), pengendalian prosedur (*procedural controls*), penentuan tanggung jawab (*assigned responsibility*), dan penelusuran jejak (*audit trails*). Untuk memastikan integritas informasi, maka harus bisa memantau sumber data, tanggal dan waktu, dan isi dari setiap pengubahan. Jadi penambahan dan pengubahan harus bisa terlacak sampai ke sumbernya.

Integritas program berkaitan dengan kualitas dari disain perangkat lunak dan penjagaannya dari kemungkinan pengubahannya. Gangguan pada perangkat lunak (*software bugs*) dan kompleksitas disain perangkat lunak dapat berperan dalam mengakibatkan ketidaklengkapan atau bahkan kehilangan informasi yang seharusnya dihasilkan.

Integritas sistem merupakan kemampuan dari suatu sistem otomatis untuk menjaga fungsinya dari gangguan dan manipulasi yang tidak sah. Fitur-fitur dari perangkat keras dan perangkat lunak harus diuji secara periodik untuk memastikan berfungsinya sistem tersebut secara benar. Tersedianya sistem penyalinan dan prosedur pemulihan data (*backup and recovery procedure*) sangat penting untuk mengantisipasi pemulihan sistem secara cepat dan aman apabila terjadi kegagalan sistem.

Integritas jaringan merupakan perluasan fitur integritas sistem dalam jaringan lokal maupun jaringan yang lebih luas (*local and wide area networks*).

2.3.4 Penelusuran jejak (*audit trails*)

Fitur ini berfungsi untuk memantau setiap operasi terhadap sistem informasi. Penelusuran jejak harus mampu mencatat secara kronologis setiap aktifitas terhadap sistem. Pencatatan ini dilakukan segera dan sejalan dengan aktifitas yang terjadi (konkuren). Fitur ini dapat dimanfaatkan untuk mendeteksi dan melacak penyalahgunaan dan pelanggaran keamanan, menentukan dilaksanakan tidaknya kebijakan

dan prosedur operasional yang berlaku, serta untuk merekonstruksi rangkaian aktifitas yang dilakukan terhadap sistem.

Catatan yang dihasilkan oleh fitur penelusuran jejak hendaknya berisi informasi tentang identitas pengguna, sumber data yang diakses, identitas pasien yang diakses datanya, identitas fasilitas pelayanan kesehatan, kode lokasi akses, tanggal dan waktu akses, dan jenis aktifitas yang dilakukan (termasuk fungsi sistem yang diaktifkan dan jenis informasi yang diakses).

2.3.5 Pemulihan pasca bencana (*disaster recovery*)

Fitur pemulihan pasca bencana merupakan proses yang memungkin-kan institusi untuk memulihkan kembali data-data yang hilang atau rusak setelah terjadinya suatu gangguan / bencana, misalnya kebakaran; banjir; huru-hara; bencana alam; atau kegagalan sistem.

Sistem yang difungsikan harus menunjang kemampuan tersedianya cadangan terhadap komponen sistem seperti misalnya prosesor, jalur jaring-an (*network links*), dan basis data. Sistem juga harus memiliki kemampuan untuk penyalinan data (*backup*) tanpa mengganggu fungsi-fungsi lainnya dan mampu membangun kembali informasi dari salinan data tersebut.

2.3.6 Penyimpanan dan transmisi data yang aman (*secure data storage & transmission*)

Penyimpanan data berkaitan dengan media fisik dan lokasi dimana data disimpan dan dikelola. Transmisi data berkaitan dengan

aktifitas pertukaran data antara pengguna dan program atau antara program dan program, dimana pengirim dan penerima dipisahkan oleh suatu jarak.

Pertimbangan fisik dari media penyimpanan data meliputi keamanan fisik dari prosesor, media penyimpan, kabel, terminal kerja, dan sebagainya. Perawatan dan pengelolaan terhadap media ini ditujukan untuk menjaga media penyimpan data terhadap kemungkinan sabotase dan gangguan fisik lainnya. Jadwal retensi juga perlu dipertimbangkan dan diterapkan dalam penggunaan media penyimpan data elektronik ini. Jadwal retensi ini disesuaikan dengan peraturan yang berlaku dan juga dengan kebutuhan di lingkungan institusi yang bersangkutan, misalnya untuk kebutuhan pelayanan pasien; penelitian; dan pendidikan.

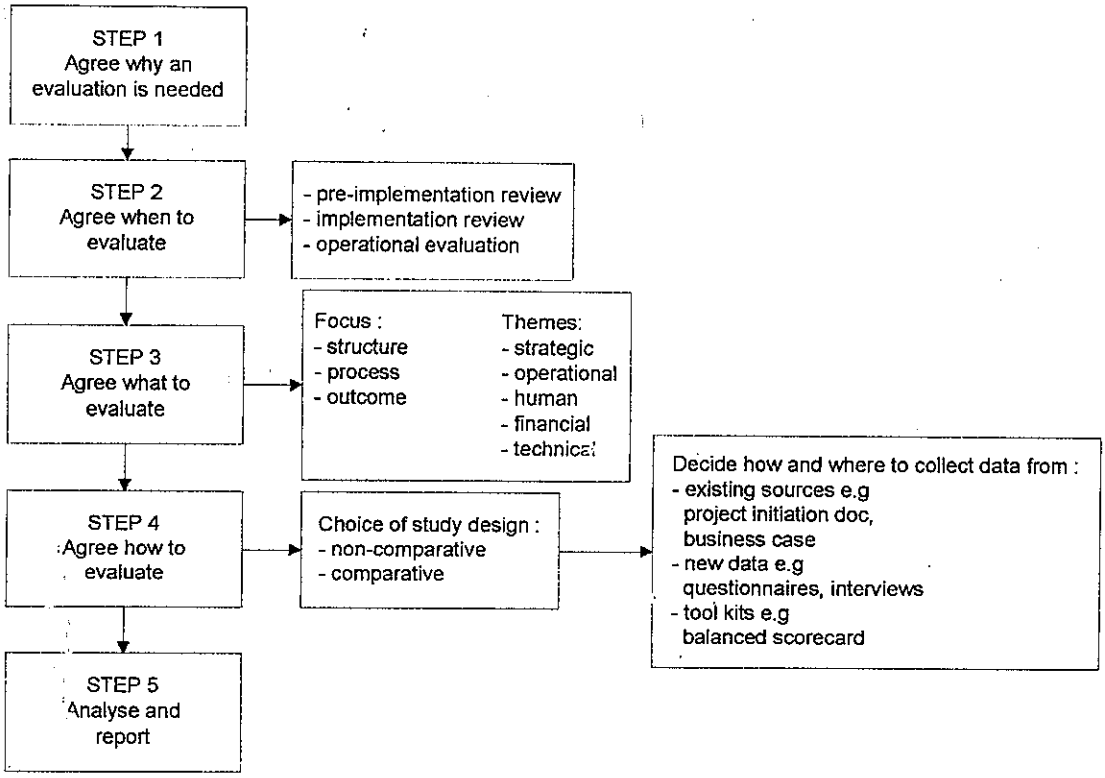
Transmisi data yang diimplementasikan dalam sistem rekam kesehatan berbasis komputer menjadi hal yang penting untuk diperhatikan karena sistem pelayanan kesehatan saat ini membutuhkan kemampuan untuk "menangkap" data dari berbagai tempat terpisah. Data yang telah terkumpul dari berbagai sumber ini juga akan ditransmisikan ke berbagai tempat untuk berbagai keperluan. Sistem yang menunjang kemampuan untuk transmisi data harus juga mampu menjamin integritas dan kerahasiaan data yang dikelola. (Computer-based Patient Record Institute, 1999; National Academy of Sciences, 1997)

2.4 Evaluasi EHR

Evaluasi terhadap EHR dilaksanakan dalam enam tahap, yaitu :

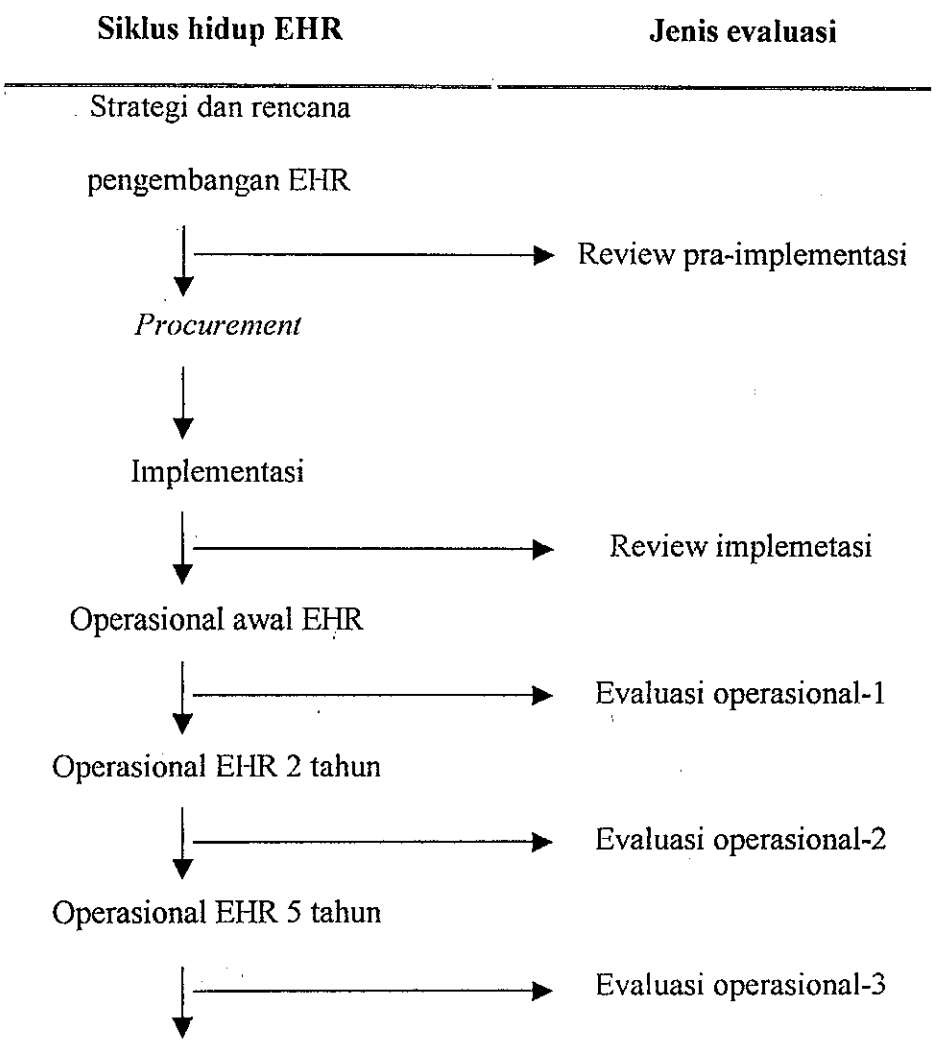
1. menyepakati latar belakang perlunya evaluasi dilaksanakan,
2. menyepakati kapan evaluasi akan dilaksanakan,
3. menyepakati hal-hal yang akan dievaluasi,
4. menyepakati bagaimana evaluasi akan dilaksanakan,
5. melaksanakan evaluasi dan melaporkan hasilnya,
6. menentukan rekomendasi dan tindak lanjutnya.

Evaluasi terhadap sistem informasi berbasis komputer dapat dilaksanakan dengan berfokus pada struktur, proses dan outcome-nya dengan desain studi *non-comparative* yang menggunakan data dari sumber data yang telah ada (dokumen, kasus, dan sebagainya) atau dengan menggali data baru, misalnya melalui kuesioner sebagai instrumen pengumpulan data. Heather (2001) merumuskan model evaluasi yang digambarkan sebagai *the six step to evaluation* adalah sebagai berikut :



Gambar 2.2
The six step to evaluation
(Heather H, dkk, 2001)

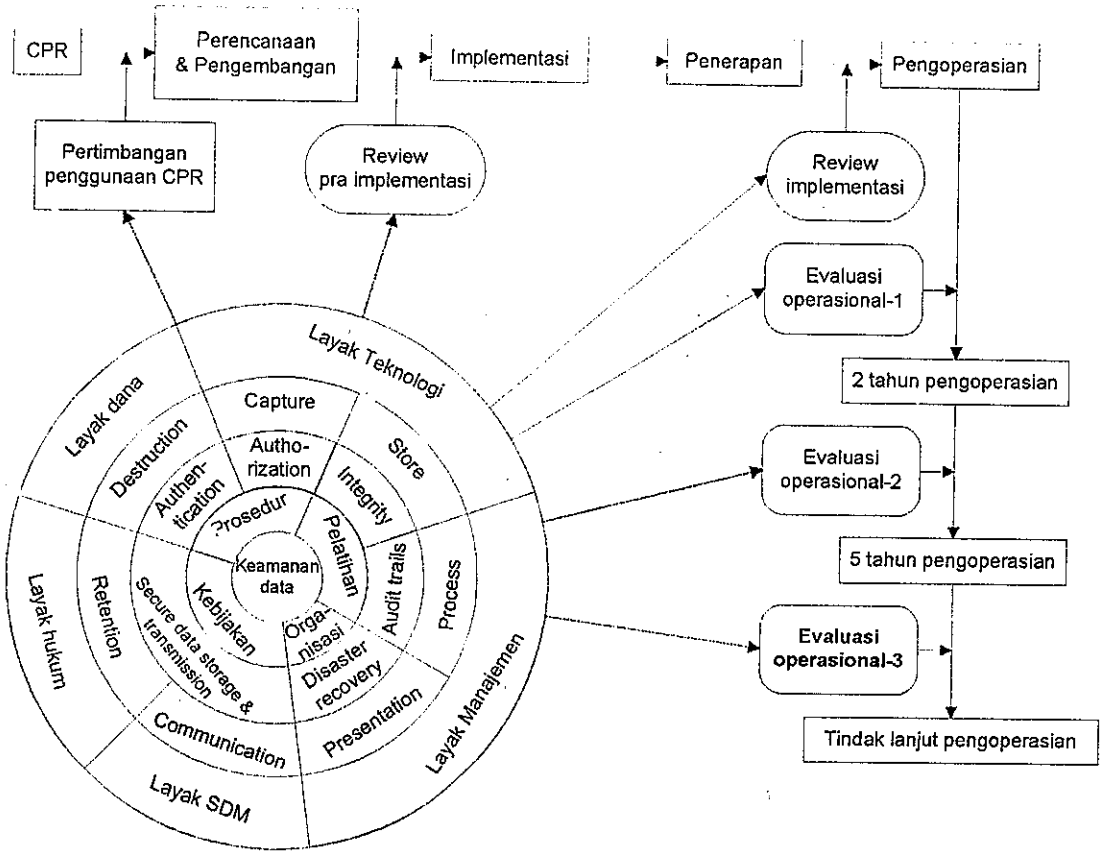
Skema alur berikut ini menjelaskan kaitan antara penentuan waktu pelaksanaan evaluasi dengan siklus hidup dari EHR dalam hal jenis evaluasi :



Beberapa prinsip dasar berkaitan dengan evaluasi EHR yaitu :

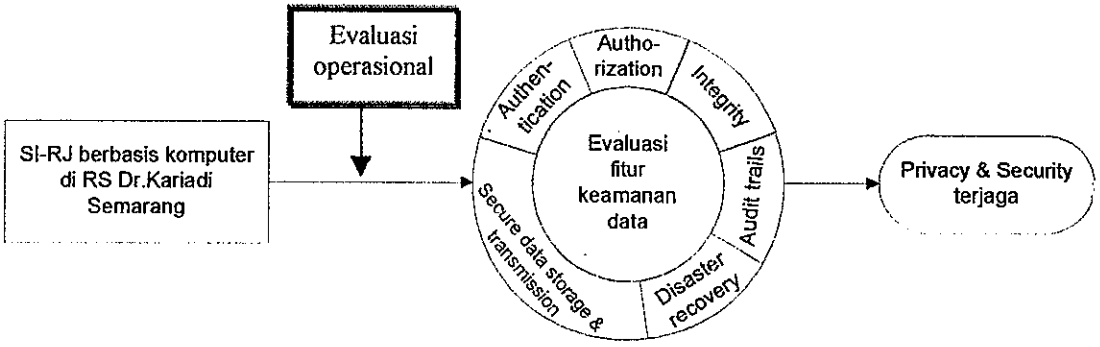
1. evaluasi harus dipahami sebagai komponen esensial dari suatu organisasi yang berkembang dan membutuhkan dukungan aktif dari tingkat manajemen tertinggi,
2. komitmen untuk melaksanakan evaluasi harus diwujudkan dengan adanya perencanaan yang baik dan ketersediaan sumber daya,
3. kriteria evaluasi harus didefinisikan sejak awal kegiatan meliputi awal dari setiap langkah ke langkah berikutnya,
4. tujuan dan manfaat dari dicanangkan harus disetujui oleh setiap pihak yang terkait dan didokumentasikan secara formal,
5. evaluasi membutuhkan keterlibatan pengelola yang sekaligus juga bertanggung jawab terhadap disain, implementasi, dan pelaksanaan tahap-tahap perencanaan,
6. pemantauan harus dilaksanakan untuk memastikan bahwa kegiatan evaluasi sudah didisain dengan cermat sehingga semua aspek dan sumber daya informasi telah tercakup didalamnya,
7. temuan dan rekomendasi yang timbul dari evaluasi selayaknya didiseminasikan dengan baik sehingga efek kemanfaatannya dapat tercapai secara maksimal.(Heather H dkk, 2001)

2.5 Kerangka Teori



(National Academy of Sciences, 1997; Computer-based Patient Record Institute, 1999; Heather H, dkk, 2001; Medical Records Institute , 2001; Amatayakul M, 2002)

2.6 Kerangka Konsep



BAB III

METODE PENELITIAN

3.1 Disain Penelitian

3.1.1 Jenis penelitian

Penelitian ini akan menggunakan metode deskriptif evaluatif. Dalam pelaksanaannya, peneliti akan berusaha untuk mendapatkan gambaran kualitatif yang nyata dan jelas mengenai obyek dan subyek yang diteliti. Penelitian ini bersifak evaluatif karena dilaksanakan terhadap obyek (sistem informasi rawat jalan berbasis komputer) yang telah diimplementasikan. Data yang didapatkan akan disusun dan disampaikan dalam bentuk narasi, tabel, dan grafik untuk membantu mendeskriptifkan hasil yang diperoleh. (Heather H dkk, 2001)

3.1.2 Metode

Dalam melaksanakan pengumpulan data, akan digunakan metode observasi terhadap obyek penelitian dan wawancara terhadap subyek penelitian. Data yang diperoleh merupakan gambaran keadaan saat penelitian dilaksanakan (*cross sectional*).

3.2 Unit Pengamatan

3.2.1 Obyek penelitian :

1. struktur organisasi dan tata kerja RS Dr.Kariadi,
2. struktur organisasi dan tata kerja Divisi SIM RS & Kom
3. struktur organisasi dan tata kerja Divisi RM & Medikolegal

4. kebijakan yang berkaitan dengan penerapan dan penggunaan SI-RJ berbasis komputer,
5. prosedur tetap (protap) mengenai pengoperasian SI-RJ berbasis komputer,
6. pelatihan untuk petugas / operator SI-RJ berbasis komputer
7. *server* (1 unit),
8. *workstation* SI-RJ (12 unit),
9. media penyimpan data / *harddisk*,
10. *printer* (10 unit)

3.2.2 Subyek penelitian :

1. Manajer Divisi SIM RS & Kom,
2. Manajer Divisi RM & Medikolegal,
3. Administrator Keamanan Sistem
4. operator SI-RJ berbasis komputer (12 orang),

3.3 Variabel dan Definisi Operasional

3.3.1 Otentikasi (*authentication*) :

Penjaminan / pemastian terhadap identitas suatu subyek atau obyek yang diwujudkan dengan :

1. ada tidaknya identitas terdaftar dari pengguna yang sah beserta passwordnya,
2. ada tidaknya kebijakan dan prosedur yang mengatur tata cara penggunaan identitas dan password,

3. ada tidaknya kebijakan dan prosedur penggunaan sistem, dan
4. ada tidaknya kebijakan yang mengatur wewenang administrator keamanan sistem.

3.3.2 Otorisasi (*authorization*) :

Pengaturan hak akses pengguna yang sah, meliputi :

1. ada tidaknya pengaturan menu yang dapat diakses,
2. ada tidaknya pengaturan waktu akses,
3. ada tidaknya pengaturan obyek yang dapat diakses, dan
4. ada tidaknya pengaturan media yang dapat diakses.

3.3.3 Integritas (*integrity*) :

Fitur yang mengatur agar data yang tersedia hanya dapat diubah / diolah untuk kebutuhan tertentu dan oleh pengguna tertentu yang berhak.

Fitur ini diwujudkan melalui ada tidaknya kemampuannya sebagai :

1. pengendali kelengkapan pengisian data,
2. pemantau data transaksi yang batal dilaksanakan,
3. penangkal aktifitas virus komputer, dan
4. pencegah kemungkinan akses data dari luar organisasi.

3.3.4 Penelusuran jejak (*audit trails*) :

Pemantauan terhadap setiap penggunaan sistem informasi secara kronologis dan dilakukan segera dan sejalan dengan aktifitas yang terjadi (konkuren).

Fitur ini diwujudkan melalui ada tidaknya kemampuan sistem untuk melaksanakan pencatatan :

1. identitas pengguna,
2. aktifitas pengguna,
3. area data yang diakses,
4. rentang waktu akses,
5. tempat akses,
6. kesalahan akses, dan
7. penggunaan perangkat lunak pembantu (*debugging tools*).

Seluruh hasil pemantauan dan pencatatan ini tersimpan dalam sistem dan hanya dapat diakses untuk dilihat laporannya oleh petugas yang berhak (Manajer Divisi SIM RS & Kom, Manajer Divisi RM & Medikolegal, Administrator Keamanan Sistem).

Kebijakan dan peraturan pelaksanaan penelusuran jejak ini harus secara tegas menyebutkan penanggung jawab beserta tugas, tata kerja dan kewenangannya.

3.3.5 Pemulihan pasca bencana (*disaster recovery*) :

Pemulihan kembali data yang hilang atau rusak setelah terjadinya suatu gangguan / bencana, misalnya kebakaran; banjir; huru-hara; bencana alam; atau kegagalan sistem.

Fitur ini diwujudkan melalui ada tidaknya kemampuan sistem untuk melakukan :

1. penggandaan / penyalinan data secara terjadwal,

2. penggunaan salinan data untuk pemrosesan dan pengolahan sesuai kebutuhan sistem pada saat pemulihan data pasca bencana,

Keberadaan fitur ini juga harus ditunjang adanya kebijakan dan prosedur pelaksanaan yang mengatur penyalinan dan pemulihan data pasca bencana yang menyebutkan dengan jelas tentang :

1. ada tidaknya penanggung jawab,
2. ada tidaknya lingkup kewenangan petugas,
3. ada tidaknya petunjuk teknis pelaksanaan, dan
4. ada tidaknya alternatif aktifitas lain untuk mendukung operasional pelayanan pada situasi dimana sistem sedang terganggu kinerjanya.

3.3.6 Penyimpanan dan transmisi data yang aman (*secure data storage & transmission*) :

Penyimpanan data berkaitan dengan fisik media data dan lokasi dimana media data disimpan serta dikelola. Fitur ini diwujudkan melalui ada tidaknya pengamanan media data dari kemungkinan gangguan manusia (pencurian, perusakan) dan gangguan alam (kebakaran, banjir, debu, hewan, huru-hara, gempa).

Kebijakan dan peraturan yang jelas harus tersedia dan menyebutkan tentang ada tidaknya :

1. tata cara penyimpanan media data,
2. penanggung jawab penyimpanan media data, dan
3. kewenangan petugas yang ditunjuk untuk mengatur hal ini.

Transmisi data berkaitan dengan aktifitas pertukaran data dimana pengirim dan penerima dipisahkan oleh suatu jarak. Kebijakan dan peraturan yang mengatur prosedur transmisi data harus menyebutkan dengan jelas tentang ada tidaknya pencatatan mengenai :

1. identitas pengguna,
2. batasan kewenangan,
3. lokasi akses,
4. waktu akses, dan
5. durasi koneksi.

3.4 Sumber-Sumber Data

3.4.1 Data primer

Data primer dikumpulkan melalui observasi terhadap perangkat keras dalam sistem informasi rawat jalan berbasis komputer, baik secara individu maupun terkait dalam jaringan. Observasi ini menggunakan pedoman observasi. Data juga dikumpulkan melalui wawancara terhadap Manajer Divisi SIM RS & Kom, Manajer Divisi RM & Medikolegal, Administrator Keamanan Sistem, dan operator SI-RJ berbasis komputer. Wawancara dilakukan berdasarkan pedoman wawancara.

3.4.2 Data sekunder

Data sekunder dikumpulkan melalui observasi terhadap dokumen penunjang, yaitu kebijakan yang berkaitan dengan SI-RJ berbasis komputer, prosedur tetap mengenai SI-RJ berbasis komputer, struktur organisasi RS Dr.Kariadi, struktur organisasi Divisi RM & Medikolegal,

deskripsi tugas personalia sub bagian rekam medis unit rawat jalan (urj), dan pedoman penggunaan perangkat lunak dalam SI-RJ berbasis komputer.

3.5 Cara dan Instrumen Pengumpulan Data

3.5.1 Cara pengumpulan date : observasi dan wawancara

3.5.2 Instrumen pengumpulan data : pedoman observasi dan pedoman wawancara

3.6 Analisis

Data yang terkumpul melalui instrumen pengumpulan data akan dianalisis dengan menggunakan *content analysis.* Instrumen dalam penelitian ini mengadopsi dan memodifikasi instrumen dari penelitian sejenis yang telah digunakan oleh *National Academy of Sciences* di Washington DC tahun 1997, *Computer-based Patient Record Institute* di Bethesda tahun 1999. Instrumen ini juga dipadukan dengan standar dari *Comprehensive Accreditation Manual For Hospital – Self Assessment With Scoring and Plan For Improvement* tahun 2003 dengan berfokus pada fungsi *Management of Information*-nya. Instrumen ini mencakup penilaian terhadap aspek organisasi dan teknologi untuk penjagaan kerahasiaan dan keamanan data dalam sistem informasi kesehatan berbasis komputer. Metode penelitian yang digunakan oleh lembaga-lembaga tersebut beserta hasil penelitiannya menjadi referensi resmi dalam profesi Manajemen Informasi Kesehatan di dunia.(National Academy of Sciences, 1997; Computer-based Patient Record Institute, 1999)

BAB IV

HASIL PENELITIAN dan PEMBAHASAN

4.1 Hasil Penelitian

4.1.1 Gambaran umum RS Dr.Kariadi

Mengacu pada keputusan direksi Perusahaan Jawatan Rumah Sakit Dokter Kariadi Semarang nomor OT.01.01-1529 tentang susunan organisasi dan tata kerja perusahaan jawatan rumah sakit Dr. Kariadi (RS Dr. Kariadi) Semarang, maksud dan tujuan RS Dr. Kariadi adalah menyelenggarakan kegiatan jasa pelayanan, pendidikan dan penelitian serta usaha-usaha lain di bidang kesehatan yang profesional dan bertujuan untuk meningkatkan status kesehatan dan senantiasa berorientasi kepada kepentingan masyarakat.

Visi RS Dr. Kariadi adalah menjadi rumah sakit mandiri terutama dalam manajemen operasional, pendapatan dan biaya serta sebagai rumah sakit pusat rujukan dalam pelayanan dan penunjang medik, dan pendidikan serta penelitian di bidang kesehatan.

Misi RS Dr. Kariadi adalah menyelenggarakan pelayanan kesehatan paripurna, profesional dan bermutu yang terjangkau oleh segenap lapisan masyarakat, dan menyelenggarakan pendidikan, pelatihan, penelitian dan pengembangan, demi tercapainya derajat kesehatan masyarakat yang optimal dan merata.

Visi dan misi tersebut diatas merupakan rumusan baru yang telah disesuaikan dengan perubahan bentuk organisasi RS Dr. Kariadi saat ini.

Dalam kaitannya dengan pengelolaan rekam medis dan informasi kesehatan, misi unit rekam medis RS Dr. Kariadi adalah mencapai efektifitas, efisiensi dan kualitas optimal layanan penyusunan dan pengelolaan rekam medis pada pelayanan medis dan keperawatan di lingkungan rumah sakit dalam rangka menunjang kegiatan rekam medis (RM) Rumah Sakit. Visi unit rekam medis RS Dr. Kariadi yaitu :

1. dalam masa lima tahun mendatang dicapai pelayanan RM yang optimal,
2. dalam masa lima tahun mendatang terlaksana pelaporan Rumah Sakit yang akurat dan tepat waktu,
3. dalam masa lima tahun mendatang tersedia morbiditas dan mortalitas rawat jalan,
4. dalam masa lima tahun mendatang terlaksana tahapan komputerisasi RM rawat jalan dan rawat inap,
5. dalam masa lima tahun mendatang tenaga rekam medis merupakan tenaga profesi dan mampu meningkatkan profesionalismenya.

Susunan organisasi RS Dr. Kariadi terdiri atas Direktur Utama, Direktur Pelayanan, Direktur Penunjang, Direktur Keuangan, Direktur Sumber Daya Manusia (SDM), Komite Profesi dan Satuan Pengawas Intern (SPI). Selain itu, terdapat pula Divisi, Bagian dan Sub Bagian. Bagan struktur organisasi ini seperti pada lampiran 1.

Menurut bagan organisasi RS Dr. Kariadi dalam keputusan direksi Perusahaan Jawatan Rumah Sakit Dokter Kariadi Semarang nomor

OT.01.01-1529 tentang susunan organisasi dan tata kerja Perusahaan Jawatan Rumah Sakit Dr. Kariadi, Divisi Sistem Informasi Manajemen Rumah Sakit dan Komunikasi (SIM RS & Kom) berada dibawah dan bertanggung jawab kepada Direktur Keuangan, demikian pula dengan Divisi Rekam Medis & Medikolegal (RM&M).

Divisi adalah tempat penyelenggaraan pelayanan fungsional RS Dr. Kariadi kepada masyarakat, baik pelayanan privat maupun pelayanan publik. Divisi dipimpin oleh seorang kepala dengan sebutan Manajer dalam jabatan non struktural yang setara dengan eselon III-a, dibawah dan bertanggung jawab kepada Direktur yang terkait. Manajer diangkat dan diberhentikan oleh Direktur Utama.

Manajer Divisi SIM RS & Kom bertugas mengelola dan mengkoordinasikan seluruh kegiatan sistem informasi manajemen dan telekomunikasi di lingkungan RS Dr. Kariadi. Sebagai pelaksana teknis harian, Manajer Divisi SIM RS & Kom menunjuk seorang Asisten Manajer yang sekaligus diberi kewenangan sebagai Administrator Keamanan Sistem (AKS).

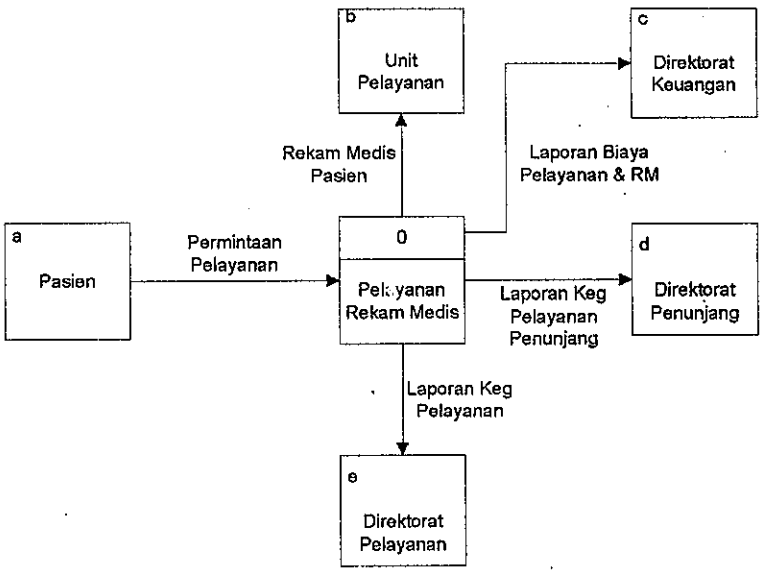
Divisi RM&M dipimpin oleh seorang Manajer yang berada dibawah dan bertanggung jawab kepada Direktur Keuangan. Manajer Divisi RM&M bertugas mengelola dan mengkoordinasikan seluruh kegiatan RM dan Medikolegal di lingkungan RS Dr. Kariadi. Manajer RM&M dibantu oleh 2 orang Asisten Manajer, yaitu Asisten Manajer Pelayanan dan Asisten Manajer Umum & Pelaporan. Dalam melaksanakan

tugasnya, Asisten Manajer Pelayanan dibantu oleh seorang Supervisor Pendaftaran Pasien & Registrasi dan seorang Supervisor Penyimpanan; Logistik & Pemusnahan. Asisten Manajer Umum & Pelaporan dibantu oleh 3 orang Supervisor, masing-masing mengelola urusan Pencatatan & Pengolahan Data; Administrasi Umum & Diklat; serta Pelaporan & Evaluasi. Bagan struktur organisasi RM di RS Dr. Kariadi adalah seperti pada lampiran 2.

4.1.2 Gambaran umum pengelolaan RM di RS Dr.Kariadi

Falsafah penyelenggaraan RM di RS Dr. Kariadi adalah :

> "Rekam medis merupakan bukti tertulis tentang proses pelayanan yang diberikan oleh dokter dan tenaga kesehatan lainnya kepada pasien di RS Dr. Kariadi Semarang. Rekam medis merupakan catatan (rekaman) yang harus mencantumkan nilai administrasi, legal, finansial, riset, edukasi, dokumen, akurat, informatif dan dapat dipertanggung jawabkan."



Gambar 4.1
Diagram konteks
pelayanan rekam medis RS Dr.Kariadi

Tujuan umum penyelenggaraan RM di RS Dr. Kariadi adalah untuk menunjang tertib administratif dalam upaya peningkatan pelayanan kesehatan, pendidikan dan penelitian di RS Dr. Kariadi. Tujuan khusus penyelenggaraan RM di RS Dr. Kariadi adalah :

1. dalam bidang administrasi: untuk menciptakan tertib administrasi pelayanan kesehatan di RS Dr. Kariadi Semarang;
2. dalam bidang medis: untuk dasar perencanaan pengobatan perawatan yang harus diberikan kepada seorang pasien;
3. dalam bidang hukum: untuk menjamin kepastian hukum atas dasar keadilan, karena RM merupakan bukti tertulis yang otentik dari segala tindakan dan pelayanan kesehatan;
4. dalam bidang keuangan: untuk mengetahui kepastian finansial biaya yang harus diselesaikan oleh seorang pasien;
5. dalam bidang penelitian: untuk dipergunakan sebagai bahan penelitian dan pengembangan ilmu pengetahuan dibidang kesehatan;
6. dalam bidang pendidikan: untuk mengetahui perkembangan kronologis dari kegiatan pelayanan medis yang diberikan kepada pasien, informasi ini dapat dipergunakan sebagai bahan operasi pengajaran dibidang profesi;
7. dalam bidang dokumentasi: untuk bukti tertulis pelayanan yang harus didokumentasikan sebagai bahan pertanggungjawaban pelayanan rumah sakit.

Direktur RS Dr. Kariadi telah menerbitkan SK Direktur nomor KP.08.02-027 tanggal 8 April 2000 revisi ke III tentang Penggunaan Petunjuk Pelaksanaan, Petunjuk Tehnis dan Prosedur Tetap (Protap) Penyelenggaraan RM di RS Dr. Kariadi Semarang.

Kebijakan tentang keamanan rekam medis di RS Dr. Kariadi Semarang dilaksanakan melalui cara sebagai berikut:

1. memasang stiker "Dilarang masuk selain petugas" pada tempat tempat tertentu (misalnya pintu ruang *filing*);
2. rekam medis tidak diperbolehkan dibawa keluar RS Dr. Kariadi bila tidak ada ijin dari Direktur;
3. pengambilan dan pengembalian RM dalam filing harus oleh petugas filing;
4. melakukan penagihan terhadap RM yang dipinjam dan sudah lewat batas waktu pengembaliannya;
5. mencatat dalam buku kendali untuk RM yang sudah dikirim ke Sub Bag RM;
6. menyediakan catatan peminjaman RM untuk monitoring & keamanan RM.

Kebijakan manajemen RS Dr. Kariadi yang mengatur tentang pelepasan informasi medis menyatakan bahwa pada prinsipnya berkas RM adalah milik rumah sakit sedangkan isinya / informasinya adalah milik pasien. Untuk memberikan informasi medis kepada pihak ketiga harus ada ijin / kuasa dari pasien atau walinya (jika pasien secara mental tidak

kompeten). Ketentuan-ketentuan lain yang mengatur pelepasan informasi medis kepada pihak ketiga menyatakan bahwa :

1. setiap informasi yang bersifat medis yang dimiliki rumah sakit tidak boleh disebarkan oleh pegawai rumah sakit kecuali bila pimpinan rumah sakit itu mengijinkan;
2. rumah sakit tidak boleh menggunakan rekam medis dengan cara yang dapat membahayakan kepentingan pasien kecuali jika rumah sakit membutuhkan rekam medis tersebut untuk melindungi dirinya atau mewakilinya;
3. Para asisten dan dokter yang bertanggung jawab boleh dengan bebas berkonsultasi dengan bagian rekam medis selama masih ada hubungan dengan pekerjaannya. Andaikata ada keragu – raguan di pihak staf rekam medis, maka persetujuan masuk ke tempat rekam medis boleh ditolak dan persoalannya hendaknya diserahkan kepada keputusan pimpinan rumah sakit. Salinan rekam medis tidak boleh dibuat tanpa persetujuan khusus dari Kepala Bagian RM yang akan bermusyawarah dengan pimpinan rumah sakit jika ada keragu–raguan. Tidak seorangpun boleh memberikan informasi lisan atau tertulis kepada orang diluar organisasi rumah sakit tanpa persetujuan tertulis dari pihak pimpinan rumah sakit (perkecualian untuk mengadakan diskusi dengan keluarga atau wali pasien yang mempunyai kepentingan yang sah, mengenai kemajuan dari pasien);

4. dokter tidak boleh memberikan persetujuan kepada perusahaan asuransi atau badan lain untuk memperoleh RM;
5. badan–badan sosial boleh mengetahui isi data sosial dari RM apabila mempunyai alasan–alasan yang sah untuk memperolehnya, namun untuk data medisnya tetap diperlukan surat persetujuan dari pasien yang bersangkutan;
6. permohonan pasien untuk memperoleh informasi mengenai catatan dirinya diserahkan kepada dokter yang merawatnya;
7. permintaan informasi secara lisan sebaiknya ditolak karena permintaan informasi harus secara tertulis;
8. informasi RM hanya dikeluarkan dengan surat kuasa yang ditandatangani dan diberi tanggal oleh pasien / walinya (jika pasien tersebut secara mental tidak kompeten) / keluarga terdekat kecuali jika ada ketentuan lain dalam peraturan. Surat kuasa hendaknya juga ditandatangani dan diberi tanggal oleh orang yang mengeluarkan RM dan disimpan di dalam berkas RM tersebut;
9. informasi dalam RM boleh diperlihatkan kepada perwalian rumah sakit yang sah untuk melindungi kepentingan rumah sakit dalam hal–hal yang bersangkutan dengan pertanggungjawaban;
10. informasi boleh diberikan kepada rumah sakit lain tanpa surat kuasa yang ditandatangani pasien berdasarkan permintaan dari rumah sakit itu yang menerangkan bahwa si pasien sekarang dalam perawatan mereka;

11. dokter–dokter dari luar rumah sakit yang mencari keterangan mengenai pasien pada suatu rumah sakit, harus memiliki surat kuasa dari pasien tersebut. Seseorang tidak boleh beranggapan bahwa seorang dokter lebih berhak untuk memperoleh informasi dibandingkan pemohon yang bukan dokter. Dalam hal ini, rumah sakit akan berusaha memberikan segala pelayanan yang pantas kepada dokter luar dengan tetap selalu berusaha untuk lebih memperhatikan kepentingan pasien dan rumah sakit;
12. ketentuan ini tidak saja berlaku bagi Bagian RM saja, tetapi juga berlaku bagi semua orang yang menangani RM di Bagian Perawatan, bangsal – bangsal dan lain – lain;
13. rekam medis yang asli tidak boleh dibawa keluar dari rumah sakit, kecuali bila atas perintah pengadilan, dengan surat kuasa khusus tertulis dari pimpinan rumah sakit;
14. rekam medis tidak boleh diambil dari tempat penyimpanan untuk dibawa ke bagian lain dari rumah sakit, kecuali jika diperlukan untuk transaksi dalam kegiatan di rumah sakit itu;
15. dengan persetujuan pimpinan rumah sakit, pemakain RM untuk keperluan riset diperbolehkan. Mereka yang bukan dari staf medis rumah sakit, apabila ingin melakukan riset harus memperoleh persetujuan tertulis dari pimpinan rumah sakit;
16. apabila berkas RM diminta untuk dibawa ke pengadilan, hendaklah diupayakan supaya pengadilan bersedia menerima salinan / fotocopy

RM yang dimaksud. Apabila hakim meminta RM yang asli, harus ada tanda terima dan disimpan di folder RM yang bersangkutan sampai RM yang asli tersebut dikembalikan;

17. fakta bahwa seorang majikan telah membayar atau menyetujui untuk membayar ongkos rumah sakit bagi seorang pegawainya, tidak dapat dijadikan alasan bagi Rumah Sakit untuk memberikan informasi medis pegawai tersebut kepada majikan tadi tanpa surat kuasa / persetujuan tertulis dari pasien atau walinya yang sah;
18. Pengesahan untuk memberikan informasi hendaklah berisi indikasi mengenai periode–periode perawatan tertentu. Surat kuasa / persetujuan itu hanya berlaku untuk informasi medis yang termasuk dalam jangka waktu / tanggal yang tertulis didalamnya.

Kebijakan lain yang telah diterbitkan guna menunjang kelancaran pelayanan RM adalah kebijakan pemilikan RM, kebijakan penyimpanan RM, kebijakan peminjaman RM dan kebijakan pemusnahan RM.

Berkaitan dengan diimplementasikannya SI-RJ berbasis komputer, RS Dr. Kariadi belum menyusun kebijakan yang secara khusus mengatur tentang:

1. tata cara penggunaan Kode Identitas Pengguna (KIP) dan password untuk menjaga kerahasiaan dan keamanan datanya;
2. kewenangan Administrator Keamanan Sistem (AKS);
3. hak akses pengguna seperti batasan menu yang dapat diakses; waktu akses; obyek yang diakses serta media yang dapat diakses;

4. uraian tugas dari masing-masing penanggung jawab bagian atau sub bagian;
5. sistem penyalinan data; penyimpanan dan pendayagunaan salinan data;

Dalam proses pengelolaan RM secara manual, RS Dr. Kariadi telah menyusun prosedur-prosedur yang dibutuhkan sebagai acuan bagi petugas dalam melaksanakan pelayanan RM. Prosedur-prosedur yang telah disusun untuk tujuan ini yaitu:

1. prosedur kerja dan uraian tugas;

   berisi daftar tugas dan tata cara pelaksanaan tugas dari masing-masing petugas
2. prosedur orientasi pegawai baru unit RM;

   berisi uraian program pengenalan pekerjaan (orientasi) bagi pegawai baru di unit RM
3. prosedur pemberian informasi medis kepada orang / badan;

   berisi tata cara berikut batasan pemberian informasi medis kepada pihak yang membutuhkan
4. prosedur pembuatan visum et repertum;

   berisi tata cara pengisian dan pengiriman formulir visum et repertum
5. prosedur penerimaan pasien rawat jalan;

   berisi tata cara registrasi terhadap pasien rawat jalan
6. prosedur penerimaan pasien rawat inap;

   berisi tata cara registrasi terhadap pasien rawat inap

7. prosedur pengisian RM rawat jalan;

   berisi tata cara dan aturan pengisian lembar-lembar RM rawat jalan

8. prosedur pengisian RM rawat inap;

   berisi tata cara dan aturan pengisian lembar-lembar RM rawat inap

9. prosedur pengisian RM rawat darurat;

   berisi tata cara dan aturan pengisian lembar-lembar RM rawat darurat

10. prosedur pengisian buku register rawat jalan;

    berisi tata cara dan aturan pengisian buku catatan pelayanan rawat jalan

11. prosedur pengisian buku register rawat inap;

    berisi tata cara dan aturan pengisian buku catatan pelayanan rawat inap

12. prosedur penyusunan berkas rekam medis;

    berisi tata cara dan aturan perakitan formulir RM

13. prosedur analisis kelengkapan pengisian data rekam medis;

    berisi tata cara pengecekan kelengkapan lembar dan isian formulir RM

14. prosedur pengisian index penyakit;

    berisi tata cara pengisian kartu-kartu index penyakit dari berkas RM yang telah di-*coding*

15. prosedur pemberian kode penyakit ICD-10;

    berisi tata cara dan aturan pencarian dan pencantuman kode penyakit berdasarkan ICD-10

16. prosedur pengumpulan sensus harian rawat inap (SHRI);

    berisi tata cara pengisian dan pengumpulan lembar SHRI dari setiap bangsal

17. prosedur penyimpanan dokumen RM;

    berisi tata cara dan aturan penyimpanan berkas RM di ruang *filing*

18. prosedur peminjaman RM;

    berisi tata cara dan aturan peminjaman dan penggunaan berkas RM oleh pihak yang membutuhkan

19. prosedur pemberian *informed consent*;

    berisi tata cara dan aturan pemberian informasi kepada pasien sebelum dilakukannya suatu tindakan medis dan tata cara pengisian lembar formulir *informed consent*

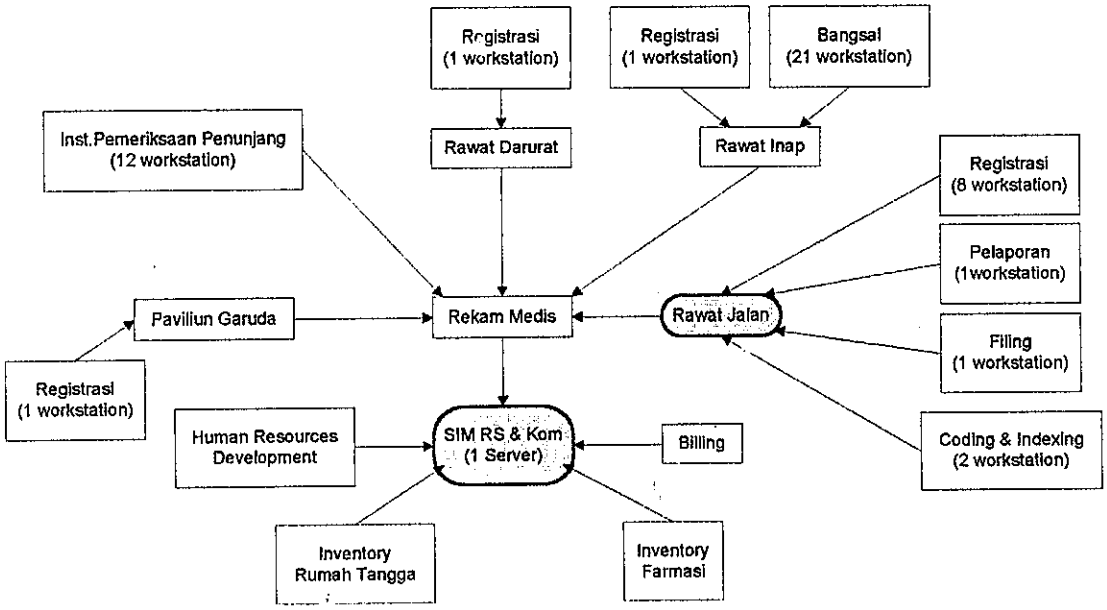
Hingga saat ini belum diterbitkan prosedur yang secara khusus mengatur tata cara penggunaan KIP dan password yang ditujukan untuk menjaga kerahasiaan dan keamanan datanya. Juga belum disusun prosedur penyalinan data, penyimpanan dan pendayagunaan salinan data untuk RM berbasis komputer.

Unit RM RS Dr. Kariadi telah memiliki prosedur orientasi bagi pegawai baru di lingkungannya. Tujuan dari prosedur orientasi bagi pegawai baru ini adalah untuk memberikan bekal pengalaman bekerja dan rasa tanggung jawab serta memahami semua pekerjaan di unit RM. Pelaksanaan prosedur orientasi ini membutuhkan alokasi waktu selama 6 hari kerja. Materi yang diberikan selama masa orientasi meliputi semua

jenis pelaksanaan pelayanan RM secara manual. Belum terdapat prosedur khusus yang melatih pegawai baru di unit RM untuk memahami aspek keamanan data dalam SI-RM berbasis komputer.

4.1.3 Gambaran umum SI-RJ berbasis komputer di RS Dr.Kariadi

Sistem informasi manajemen rumah sakit (SIM-RS) berbasis komputer di RS Dr. Kariadi telah dirintis sejak tahun 1997 dan masih terus dikembangkan. Saat ini telah dikembangkan sistem jaringan komputer berupa *local area network* (LAN) di bagian rekam medis (SI-RM), farmasi, rumah tangga (inventory), billing, dan kepegawaian (*human resources development*).



Gambar 4.2

Skema jaringan komputer di RS Dr.Kariadi

Masing-masing LAN disetiap bagian tersebut terdiri dari sebuah *server* sebagai induk jaringan dan beberapa buah *workstation* yang terhubung ke *server* melalui tipologi *star*. Jumlah *workstation* disetiap LAN tidak sama, bergantung kepada tingkat kebutuhan dimasing-masing bagian. Seluruh LAN tersebut dijalankan dengan sistem operasi perangkat lunak Novell Netware versi 4.2. Keseluruhan sistem LAN tersebut terhubung ke "pusat" kendali di Divisi SIM RS & Kom.

Sebagai pusat pengelola, Divisi SIM RS & Kom mengendalikan arus data, penyimpanan, pengolahan dan penggunaan data serta informasi yang dihasilkan dari kegiatan pelayanan di RS Dr. Kariadi. Keseluruhan kegiatan pengendalian ini dilakukan melalui kewenangan Divisi SIM RS & Kom dalam mengatur fungsi tiap LAN dan fungsi keseluruhan jaringan SIM RS berbasis komputer di RS Dr. Kariadi.

Divisi SIM RS & Kom dipimpin oleh seorang Manajer yang berada dibawah dan bertanggung jawab kepada Direktur Keuangan. Manajer Divisi SIM RS & Kom bertugas mengelola dan mengkoordinasikan seluruh kegiatan sistem informasi manajemen dan telekomunikasi di lingkungan RS Dr. Kariadi. Sebagai pelaksana teknis harian, Manajer Divisi SIM RS & Kom menunjuk seorang Asisten Manajer yang sekaligus diberi kewenangan sebagai Administrator Keamanan Sistem (AKS).

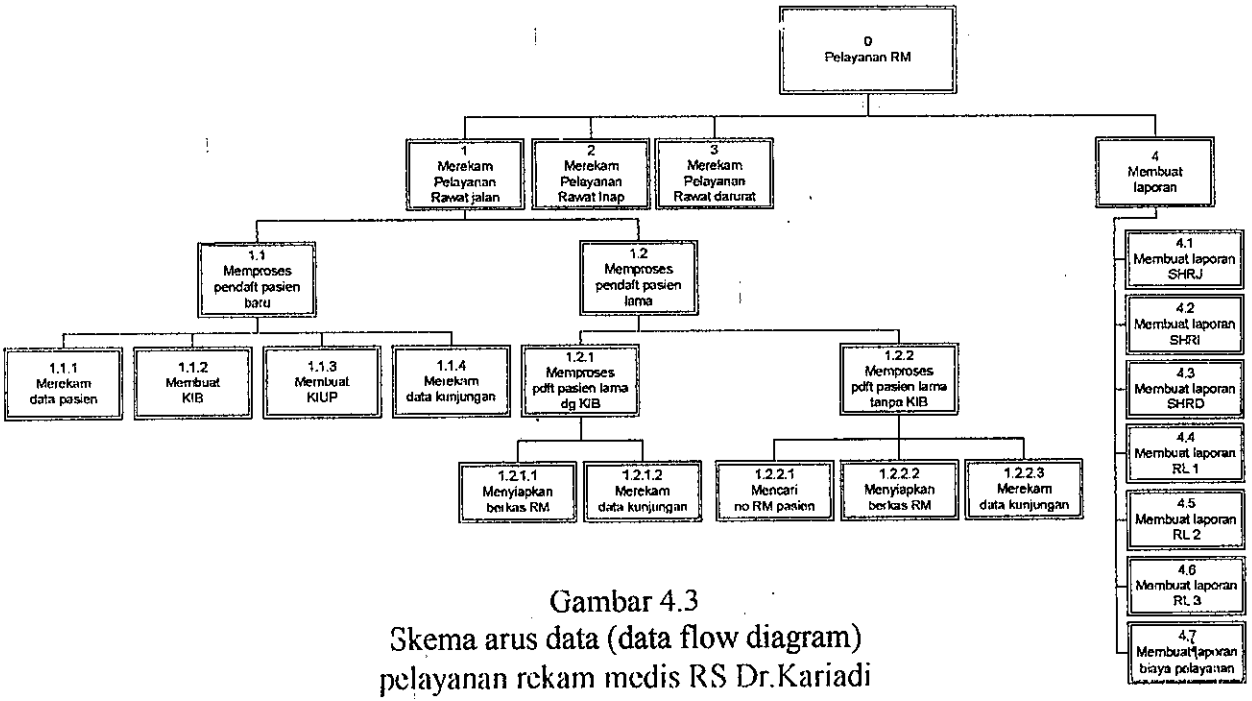
Perancangan, pembangunan, perawatan dan pengembangan SIM RS Dr. Kariadi melibatkan pihak ketiga sebagai bagian tim bersama Divisi

SIM RS & Kom. Pihak ketiga ini terutama membuat perangkat lunak SIM RS yang kemudian dikembangkan oleh Divisi SIM RS & Kom. Pengadaan perangkat keras berikut instalasinya juga dari pihak ketiga. Dalam hal ini, seringkali Divisi SIM RS & Kom masih harus membenahi instalasi jaringan komputernya apabila ada penyesuaian lokasi *workstation* atau *peripheral* lainnya.

Jaringan komputer lokal di unit RM yang membentuk Sistem Informasi Rekam Medis / SI-RM (*Computer-based Patient Record / CPR*) di RS Dr. Kariadi diimplementasikan dan dikembangkan sejak tahun 1997. Jaringan CPR ini tidak dimaksudkan untuk menggantikan sistem RM manual yang telah ada tetapi untuk mendukung kecepatan pelayanan RM dan meningkatkan tertib administrasi penyelenggaraan RM.

Saat ini terdapat 1 buah *active server* (Pentium-II 233 MHz, *harddisd* 2,8 GigaByte mirroring, RAM 64 Kb), 1 buah *backup server* (Pentium 233 MHz, harddisk 2,8 Gigabyte, RAM 64 Kb) dan 77 buah *diskless workstation* (62 diantaranya menggunakan processor dibawah Pentium 100 MHz dan sisanya menggunakan processor Pentium 100 MHz) yang terhubung dalam jaringan sistem informasi rumah sakit di RS Dr.Kariadi melalui *interface* yang bekerja pada 10 Mbps dengan konstruksi koneksi IPx. Semua monitor yang digunakan dalam jaringan bertipologi *star* ini merupakan monitor hitam-putih. Sistem informasi rawat jalan merupakan bagian dari sistem informasi rekam medis. Jaringan komputer yang membentuk sistem informasi rekam medis terdiri dari 48

workstation termasuk 12 diantaranya merupakan workstation di unit rawat jalan. *Server* terletak di ruang Divisi SIM RS & Kom sedangkan *workstation* tersebar di beberapa unit pelayanan seperti dalam gambar 4.1 di atas. Penyimpanan dan pengolahan data dilaksanakan dalam media dan prosesor *server*, sedangkan *workstation* hanya digunakan untuk pemasukan data dan penampilan informasi. *Workstation* yang digunakan adalah jenis *diskless* sehingga segala aktifitas *workstation* harus melalui koneksi dengan *server*. Media penyimpanan data dalam *server* menggunakan *harddisk* utama berkapasitas 2,8 giga bytes (GB) dan *harddisk* cadangan berkapasitas 2,8 GB. *Harddisk* cadangan digunakan sebagai media penyalin (*backup*) dari data yang terdapat dalam *harddisk* utama. *Server* selalu dalam keadaan *on* selama 24 jam dan siap mengendalikan seluruh jaringan komputer di RS Dr.Kariadi.



Gambar 4.3
Skema arus data (data flow diagram)
pelayanan rekam medis RS Dr.Kariadi

4.1.4 Fitur keamanan data dalam SI-RJ di RS Dr.Kariadi

Fitur keamanan data dalam SI-RJ di RS Dr.Kariadi merupakan hasil keterpaduan antara segi organisasi dan segi teknologi.

Segi organisasi meliputi pengaturan struktur organisasi, penerbitan dan pelaksanaan kebijakan yang berkaitan dengan SI-RJ, penyusunan dan penerbitan prosedur pengoperasian SI-RJ serta pelatihan pengoperasian SI-RJ di RS Dr.Kariadi.

Segi teknologi meliputi kemampuan sistem dalam menjaga keamanan data didalamnya melalui fitur-fitur otentikasi, otorisasi, integritas, penelusuran jejak, pemulihan pasca bencana serta penyimpanan dan transmisi data yang aman.

4.1.4.1 Otentikasi (*authentication*)

Otentikasi mengandung pengertian berkaitan dengan penjaminan / pemastian terhadap identitas suatu subyek atau obyek. Misalnya, pemastian bahwa seorang pengguna yang akan menggunakan sistem adalah memang pengguna yang sah / terdaftar (otentikasi pengguna). Pemastian bahwa sekumpulan sumber data yang diterima adalah sesuai dengan yang dibutuhkan juga merupakan contoh otentikasi, dalam hal ini otentikasi keaslian data.

Metode untuk menerapkan otentikasi yang aman merupakan kebutuhan yang esensial dalam sistem rekam kesehatan berbasis komputer. Setiap pengguna memikul tanggung jawab terhadap informasi kesehatan yang mereka masukkan, tambahkan, validasi,

dan mereka lihat dalam sistem. Oleh karena itu, setiap pengguna harus bisa diidentifikasi secara unik, dibedakan satu dari lainnya. Kebijakan khusus harus diterbitkan oleh pihak institusi untuk mengatur disiplin penggunaan berikut sangsi bagi individu yang membocorkan identitas otentikasinya kepada pengguna lain.

Personalia unit RM di RS Dr. Kariadi saat ini terdiri dari 69 orang. Seluruh petugas ini telah memiliki Kode Identifikasi Pengguna (KIP) dan password masing-masing. Kode Identitas Pengguna ditentukan oleh Administrator Keamanan Sistem (AKS). Password pengguna ditentukan oleh AKS pada saat pertama kali pengguna didaftarkan sebagai pengguna sistem, selanjutnya password ini dapat diubah dan ditentukan sendiri susunannya oleh pengguna dengan format alfanumerik dengan kapasitas 1 hingga 12 karakter. Pengguna dapat mengubah passwordnya kapanpun dia menghendaki (dalam jam kerja sistem). Administrator Keamanan Sistem dapat melakukan dan memiliki kewenangan untuk menentukan atau bahkan me*reset* password pengguna ke suatu nilai yang ditentukannya. Password pengguna tidak ditentukan masa berlakunya oleh AKS. Keadaan ini seperti disampaikan oleh AKS :

> "Semua operator disini sudah dibuatkan inisial dan password, lalu mereka bisa mengubah passwordnya kapanpun terserah mereka. Saya cuma menentukan password awalnya saja."

Setiap pengguna telah ditentukan tingkatan hak aksesnya oleh AKS sehingga hanya dapat mengakses menu tertentu saja sesuai

dengan kewenangannya. Misalnya, petugas pendaftaran pasien rawat jalan hanya bisa mengakses menu-menu yang berkaitan dengan tugasnya saja dan tidak bisa mengakses menu lainnya (misalnya tidak bisa mengakses menu untuk laporan pasien rawat inap atau menu-menu bagian keuangan / akuntansi). Pembatasan hak akses ini juga berlaku bagi *vendor*, sehingga mereka hanya bisa mengakses menu untuk *maintenance* sistem saja dan tidak bisa mengakses menu lainnya.

Setiap kali mulai menggunakan sistem, pengguna harus memasukkan KIP dan passwordnya. Apabila pengguna salah memasukkan KIP dan/atau passwordnya, maka sistem akan memberikan pesan kesalahan "Kode Identitas Pengguna & Password tidak sah" kepada pengguna.

Setelah berada di dalam sistem, untuk mengakses menu-menu yang berkaitan dengan keuangan, penayangan laporan (di layar maupun di kertas) dan menu perbaikan data tertentu, pengguna akan diminta untuk memasukkan passwordnya kembali. Apabila terjadi 3 kali kesalahan password untuk mengakses menu-menu ini, maka sistem secara otomatis akan melakukan *log out* terhadap pengguna tersebut.

Administrator Keamanan Sistem dapat menentukan batas tanggal atau waktu dari hak akses pengguna. Dengan demikian, pengguna hanya dapat "masuk" ke sistem pada saat-saat yang telah

ditentukan saja, misalnya hanya dalam jam kerja. Sistem juga memiliki kemampuan untuk menonaktifkan KIP yang sedang berada dalam sistem setelah jeda waktu tertentu (15 menit) tanpa aktifitas (*idle time*). Dalam hal ini AKS menyatakan bahwa :

> "kalau komputernya ditinggal nganggur 15 menit dan tidak diapa-apakan, nanti akan langsung *mbalik* sendiri ke menu utama. Kalau mau dipakai lagi ya harus ngetik passwordnya lagi."

Dalam keadaan tertentu, hak akses seorang pengguna dapat dinonaktifkan oleh AKS tanpa menghapus *file* datanya dari sistem. Keadaan yang dimaksud misalnya pegawai tersebut sudah pindah bagian atau keluar dari RS Dr. Kariadi, atau pegawai tersebut dikenai sangsi karena pelanggaran penggunaan sistem. Pemutusan aktifitas akses pengguna ini dapat dilakukan secara *real time* (segera dan saat ini) oleh AKS.

Catatan tentang KIP dan password dari seluruh pengguna sistem disimpan dalam bentuk file dalam sistem, namun tidak dalam bentuk enkripsi (diacak menurut rumus dengan sandi). Fungsi-fungsi dan menu dalam sistem yang menjadi hak AKS (misalnya pemantauan sistem, pengubahan data selewat 24 jam sejak pengisian data tersebut ke komputer, dan aktivasi & deaktifasi sistem, dll), dipisahkan dari menu lainnya yang dioperasikan oleh pengguna. Seluruh peralatan dan aktifitas sistem dapat dipantau oleh AKS melalui menu khusus (menu administrator sistem) yang memang disediakan untuk tujuan ini.

4.1.4.2 Otorisasi (*authorization*)

Otorisasi mengandung pengertian berkaitan dengan pengesahan hak yang meliputi pengesahan akses berdasarkan hak akses.

Otorisasi mengatur lingkup hak dari seorang pengguna yang sah, meliputi hak akses terhadap fungsi sistem dan informasi yang terkandung didalamnya.

Administrator Keamanan Sistem telah menentukan batasan akses bagi seorang pengguna atau suatu kelompok pengguna. Dengan demikian, pengguna hanya dapat melakukan akses terhadap menu atau fungsi tertentu saja dari sistem, sesuai dengan batasan yang telah ditentukan oleh AKS. Misalnya, operator di bagian filing menyatakan :

> "Kalau dari sini cuma bisa menampilkan index utama pasien. Petugas di bagian pendaftaran yang memasukkan datanya. Saya juga tidak bisa menampilkan tabel karcis dari bagian pendaftaran."

Setelah berada di dalam sistem, untuk mengakses menu-menu yang berkaitan dengan keuangan, penayangan laporan (di layar maupun di cetak ke kertas), dan menu perbaikan data, pengguna juga akan diminta untuk memasukkan passwordnya kembali. Apabila terjadi 3 kali kesalahan password untuk mengakses menu-menu tertentu ini, maka sistem secara otomatis akan melakukan *log out* terhadap pengguna tersebut.

Fungsi "menghapus" (*delete*) dan "mengubah" (*edit*) data dalam sistem hanya merupakan kewenangan AKS. Apabila seorang pengguna mengalami kesalahan dalam memasukkan data, maka dia masih bisa membetulkan kesalahan pada hari tersebut. Namun apabila sudah melewati batas jam kerja, maka pembetulan kesalahan harus melalui AKS sebagaimana yang diungkapkannya :

> "kalau salahnya itu langsung mau dibetulkan ya bisa, tapi kalau sudah lewat hari kerja, misalnya besoknya, harus menghubungi saya dulu. Kalau kuncinya sudah saya buka, baru petugas itu bisa membetulkan salahnya."

4.1.4.3 Integritas (*integrity*)

Integritas mengandung pengertian bahwa informasi yang tersedia hanya diubah / diolah untuk kebutuhan tertentu dan oleh pengguna tertentu yang berhak.

Integritas data berkaitan dengan akurasi (*accuracy*), konsistensi (*consistency*), dan kelengkapan (*completeness*) dari data. Hal ini terkait secara langsung dengan kualitas data yang bersangkutan dan dapat berpengaruh terhadap kualitas pelayanan kesehatan yang diberikan. Pemantauan integritas data harus dapat memastikan bahwa data tidak diubah atau dirusak melalui cara yang tidak sah.

Sistem informasi rawat jalan berbasis komputer yang diimplementasikan saat ini telah disiapkan untuk mengatur pengisian beberapa *field* data tertentu sedemikian sehingga pengguna diwajibkan untuk mengisinya (*required filed*). Hal ini bertujuan

untuk menjaga agar *field* data tersebut tidak dibiarkan diam oleh pengguna pada saat pengisian data pelayanan seorang pasien. Apabila pengguna lupa atau sengaja mengosongkan isian pada *field* tersebut maka sistem akan menampilkan jendela dialog (*dialog box*) berisi pesan yang mengingatkan pengguna untuk melengkapi isian pada *field* tersebut.

Beberapa *field* data lainnya juga diatur pengisiannya dengan metoda pilihan (*choise*) dari item yang telah disediakan (misalnya dengan *picking-up list* dan *choices*). Hal ini bertujuan untuk menjaga konsistensi isian pada *field-field* tersebut.

Sistem telah dilengkapi dengan perangkat lunak anti virus komputer (Mc Affee versi 6). Selain itu, untuk mencegah masuknya virus komputer dari *workstation*, maka digunakan metode *diskless workstation*. Keseluruhan jaringan komputer dalam SIM RS di RS Dr. Kariadi, termasuk jaringan SI-RJ tidak terhubung ke internet dan tidak memiliki jalur akses dari luar rumah sakit.

4.1.4.4 Penelusuran jejak (*audit trails*)

Fitur ini berfungsi untuk memantau setiap operasi terhadap sistem informasi. Penelusuran jejak harus mampu mencatat secara kronologis setiap aktifitas terhadap sistem. Pencatatan ini dilakukan segera dan sejalan dengan aktifitas yang terjadi (konkuren). Fitur ini dapat dimanfaatkan untuk mendeteksi dan melacak penyalahgunaan dan pelanggaran keamanan, menentukan dilaksanakan tidaknya

kebijakan dan prosedur operasional yang berlaku, serta untuk merekonstruksi rangkaian aktifitas yang dilakukan terhadap sistem.

Sistem yang digunakan saat ini mampu memantau aktifitas pengguna dan mencatatnya ke dalam suatu berkas penelusuran jejak. Setiap kegiatan akses terhadap sistem secara otomatis terekam dalam *log-file* Hal-hal yang dicatat ke dalam berkas ini meliputi:

1. kode identitas pengguna (KIP),
2. tanggal; jam; durasi dan lokasi akses,
3. menu yang diakses,
4. jenis data yang diakses berikut aktifitas terhadap data tersebut,
5. aktifitas yang berkaitan dengan otoritas akses; termasuk kesalahan penggunaan sistem dan pelanggaran terhadap prosedur keamanan.

Berkas penelusuran jejak hanya bisa diakses oleh AKS. Berkas ini sangat dibutuhkan oleh AKS terutama pada saat terjadi komplain terhadap ketidaksesuaian hasil pencatatan kegiatan pelayanan terhadap pasien, misalnya ketidaksesuaian jumlah tagihan dengan jenis pelayanan yang diberikan. Berkas ini belum digunakan sebagai sumber penyusunan laporan rutin tentang aktifitas sistem.

4.1.4.5 Pemulihan pasca bencana (*disaster recovery*)

Fitur pemulihan pasca bencana merupakan proses yang memungkinkan institusi untuk memulihkan kembali data-data yang hilang atau rusak setelah terjadinya suatu gangguan / bencana,

misalnya kebakaran; banjir; huru-hara; bencana alam; atau kegagalan sistem.

Sistem saat ini mampu membuat salinan data secara dinamis tanpa mengganggu aktifitas akses pengguna dan tanpa harus berhenti difungsikan dahulu. Dengan demikian, sistem dapat terus berfungsi 24 jam sehari. Dalam proses penyalinan data, AKS dapat menentukan kriteria penyalinan berdasarkan periode waktu tertentu. Proses penyalinan data telah diatur untuk berjalan secara otomatis setiap pukul 00:00. Penyalinan data dilakukan kedalam media penyimpan data (*harddisk*) yang juga terletak di dalam *active server*. Hasil penyalinan ini kemudian disalin lagi kedalam *harddisk* yang lain diluar *active server*. Dengan demikian AKS selalu memiliki dua salinan data dalam dua *harddisk*.

Harddisk tempat menyimpan salinan data tingkat kedua disimpan dalam ruang yang sama dengan *server*.

Bila terjadi kegagalan sistem yang mengakibatkan terganggunya fungsi media penyimpan data utama, maka salinan data dapat disalin ulang ke media penyimpan data utama untuk kemudian difungsikan kembali.

4.1.4.6 Penyimpanan dan transmisi data yang aman (*secure data storage & transmission*)

Keamanan penyimpanan data berkaitan dengan media fisik serta lokasi dimana data disimpan dan dikelola. Transmisi data

berkaitan dengan aktifitas pertukaran data antara pengguna dan program atau antara program dan program, dimana pengirim dan penerima dipisahkan oleh suatu jarak.

Sistem yang dikembangkan saat ini memiliki kemampuan untuk mengendalikan aktifitas fungsi *export* dan *import* data. Hanya AKS yang dapat memanfaatkan fungsi ini.

Proses *export* dan *import* data ini belum menggunakan metoda enkripsi untuk keamanan datanya.

File data dalam sistem saat ini disimpan dalam format *dbf* yang *compatibel* dengan dBASE III+ dan tanpa menggunakan metoda pengaman data, misalnya enkripsi, kunci *file*, ataupun kunci *field.*

4.2 **Pembahasan**

4.2.1 Pembahasan umum

Sesuai dengan fungsinya untuk menghasilkan integritas data (*integrity*), meningkatkan kerahasiaan dan keamanan (*confidentiality*), serta untuk menunjang ketersediaan informasi saat dibutuhkan (*availability*), maka sistem informasi berbasis komputer sudah harus dipertimbangkan perencanaan dan pengembangannya agar terjaga fungsinya tadi sejak dari tahap *data capturing* hingga *data destruction.* Demikian pula halnya dengan SI-RJ berbasis komputer di RS Dr.Kariadi.(Wagner, Lew, 2002)

Dalam kaitannya dengan pengelolaan rekam medis dan informasi kesehatan, misi unit RM RS Dr. Kariadi adalah mencapai efektifitas, efisiensi

dan kualitas optimal layanan penyusunan dan pengelolaan RM pada pelayanan medis dan keperawatan di lingkungan rumah sakit.

Misi dan visi ini mendorong pihak RS untuk melakukan pembenahan sistem dan peningkatan sarana pengelolaan dan pelayanan RM-nya. Pembenahan sistem dilaksanakan dengan menerbitkan kebijakan-kebijakan dan prosedur baru untuk pelayanan RM.

Peningkatan sumber daya manusia untuk menunjang tercapainya misi ini ditempuh melalui penyelenggaraan pelatihan-pelatihan bagi petugas rekam medis, pelaksanaan masa orientasi bagi petugas baru dan pengiriman tugas belajar secara bertahap bagi petugas RM senior ke Akademi Perekam dan Informatika Kesehatan di Semarang (APIKES). Hingga saat ini sudah 8 petugas RM yang menyelesaikan jenjang pendidikan DIII dan berhak atas gelar Ahli Madya Perekam Kesehatan (Amd PerKes).

Dalam struktur organisasi RS Dr.Kariadi yang disahkan Direksi melalui SK nomor OT.01.01-1529 tentang susunan organisasi dan tata kerja Perjan RS Dr.Kariadi, sudah ada Divisi yang bertanggung jawab terhadap pengelolaan SIM-RS termasuk SI-RJ, yaitu Divisi SIM-RS & Kom yang berada dibawah dan bertanggung jawab kepada Direktur Keuangan.. Dalam pelaksanaannya sehari-hari, Manajer Divisi SIM-RS & Kom dibantu oleh seorang Asisten Manajer yang sekaligus berperan sebagai Administrator Keamanan Sistem (AKS).

Adanya kepastian tentang divisi dan orang yang bertanggung jawab terhadap pengelolaan SIM-RS berbasis komputer ini sangat penting guna

menetapkan kewenangan dan kewajiban pengelola sistem. Penerapan sistem kewenangan terpusat ini sangat membantu terciptanya satu komando koordinasi pengelolaan sistem informasi berbasis komputer, terutama dalam hal penjagaan keamanan data dan informasi yang dihasilkannya. Proses perawatan sistem, pengembangan, hingga penanganan konflik yang timbul dapat langsung dikelola oleh AKS.(Amatayakul, Margret, 2002)

Wagner (2002) merumuskan proses dan upaya penjagaan keamanan sistem informasi berbasis komputer dalam tiga komponen yaitu *people, process,* dan *technology* (PPT) yang secara utuh disebutnya sebagai *the security triad.* Aspek *people* dalam PPT ini menekankan perlunya penetapan visi institusi pada level manajemen. Dalam hal ini, RS Dr.Kariadi telah menetapkan visi RS Dr.Kariadi dan visi unit rekam medisnya. Adanya visi ini diperlukan untuk menjaga arah jalannya operasional pelayanan di unit rekam medis dan untuk acuan arah pengembangannya, termasuk dalam penerapan SI-RJ berbasis komputer. Visi yang telah ada perlu dioperasionalkan melalui penerbitan kebijakan oleh pihak manajemen. Rumah sakit Dr.Kariadi belum menerbitkan kebijakan yang khusus mengatur tentang penjagaan kerahasiaan dan keamanan (*privacy and security*) dari SI-RJ berbasis komputer yang telah digunakan. Kebijakan ini perlu sebagai bukti komitmen manajemen terhadap *privacy* dan *security* tersebut.

Dengan belum adanya kebijakan yang mengatur tentang penggunaan dan pendayagunaan SI-RJ berbasis komputer, terutama dalam hal penjagaan

privacy dan *security*-nya, maka penjagaan kerahasiaan dan keamanan informasi dalam sistem tersebut juga masih lemah dari aspek organisasi.

Dari seluruh prosedur yang tercantum dalam SK Direktur nomor KP.08.02-027 tanggal 8 April 2000 revisi ke III tentang Penggunaan Petunjuk Pelaksanaan, Petunjuk Teknis dan Prosedur Tetap (Protap) Penyelenggaraan RM di RS Dr.Kariadi, yang secara langsung terkait dengan penjagaan kerahasiaan dan keamanan informasi medis adalah prosedur pemberian informasi medis kepada orang/badan, prosedur pembuatan visum et repertum dan prosedur peminjaman RM. Belum tercantum adanya prosedur yang mengatur tata cara penggunaan berikut tata cara penjagaan kerahasiaan dan keamanan data dan informasi dalam SI-RJ berbasis komputer. Prosedur-prosedur yang telah ada untuk pengelolaan RM secara manual tersebut telah didiseminasikan kepada petugas dan termasuk dalam rangkaian materi *on-the-job training* bagi petugas baru, sesuai dengan prosedur orientasi pegawai baru unit RM. Diseminasi protap-protap ini penting untuk meningkatkan pemahaman dan kewaspadaan petugas pengguna sistem, terutama dalam hal menjaga kerahasiaan dan keamanan data dan informasi di dalamnya. Hal ini sesuai dengan hasil identifikasi Wagner (2002) tentang enam resiko tertinggi yang mungkin timbul dan mengancam keamanan sistem (*top six security risks*), yaitu :

1. *internet*, terhubungnya jaringan komputer ke internet menyebabkan timbulnya pintu koneksi dengan dunia di luar organisasi. Dengan adanya koneksi ini maka pihak ai luar organisasi memiliki peluang untuk masuk

ke dalam jaringan dan mengakses sistem informasi yang sedang dijalankan sehingga kemungkinan pencurian informasi atau penyusupan program dari luar juga semakin terbuka.

2. *telecommuting*, terhubungnya jaringan komputer dengan suatu *workstation* atau jaringan lain di luar organisasi menimbulkan sisi rawan untuk pencurian informasi atau penyusupan program dari luar organisasi.
3. *host*, pemilihan sistem operasi yang akan diimplementasikan dalam *server* akan ikut mempengaruhi keamanan data yang dikelola, karena masing-masing jenis sistem operasi memiliki keunggulan dan kelemahan masing-masing.
4. *network*, masing-masing model konstruksi dan konfigurasi jaringan komputer memiliki keunggulan dan kelemahan, termasuk dalam aspek keamanan data.
5. *desktop*, setiap *workstation* dalam jaringan komputer dapat menjadi jalan masuk ke dalam jaringan untuk mendapatkan informasi.
6. *security awareness* atau pemahaman dan kesadaran pengguna tentang keamanan data akan ikut membentuk sikap dan perilaku pengguna dalam mengoperasikan jaringan koputer.(Wagner, Lew, 2002)

Kebijakan yang perlu diterbitkan oleh manajemen RS Dr.Kariadi berkaitan dengan penjagaan kerahasiaan dan keamanan dalam SI-RJ berbasis komputer meliputi :

1. kebijakan keamanan data (*security policies*) yang mencakup antara lain filosofi, tujuan, otentikasi dan kendali akses, *reliability* dan *integrity*

2. kebijakan kerahasiaan data (*confidentiality policies*) yang mengatur keseimbangan antara hak dan kebutuhan akses dengan keharusan penjagaan kerahasiaan informasi yang diakses
3. kebijakan penjagaan informasi yang sensitive (*policies to protect sensitive information*) yang mengatur pengelolaan informasi medis, misalnya yang berkaitan dengan penyalahgunaan narkoba, penyakit akibat hubungan seksual, HIV/AIDS, dan sebagainya.
4. kebijakan penggunaan informasi kesehatan untuk penelitian (*policies on research uses of health information*) yang mengatur tentang pelepasan informasi medis untuk kebutuhan penelitian.
5. kebijakan yang mengatur perihal pelepasan informasi kesehatan secara umum (*policies guiding release of health information*).
6. kebijakan yang berkaitan dengan pasien sebagai isu sentral, misalnya kebijakan akses terhadap data dan catatan penggunaannya (*access to record and audit logs policies*) yang mengatur batasan hak akses petugas pengguna sistem, termasuk juga hak akses pasien terhadap *file* rekam medisnya.

Kebijakan yang mengatur kewenangan Administrator Keamanan Sistem (AKS) juga belum disusun. Hal ini sering menyebabkan AKS ragu-ragu terhadap batasan kewenangannya dalam mengatur dan menentukan operasional sistem. Kondisi ini seringkali menghambat kecepatan pengembangan sistem. Kebijakan-kebijakan yang saat ini telah diterbitkan oleh pihak manajemen RS Dr.Kariadi merupakan rangkaian kebijakan yang

secara umum mengatur penyelenggaraan RM di RS Dr.Kariadi. Hal ini sudah bisa menjadi dasar acuan penyelenggaraan RM termasuk pengelolaan aspek keamanan data RM, baik untuk RM yang berbasis kertas maupun yang berbasis komputer. Kebijakan-kebijakan ini juga menjadi dasar penyusunan prosedur tetap (protap) dalam penyelengaraan RM yang mana protap ini berperan sebagai acuan tata cara dan aturan bagi para petugas. (Skurka M F, 1994; National Academy of Sciences, 1997)

Menurut Heather H (2001), sebuah sistem informasi yang telah dioperasionalkan harus dievaluasi kinerjanya. Heather membedakan penggunaan nomenklatur *review* dan *evaluation. Review* digunakannya untuk menyatakan proses monitoring dan penyelesaian proyek yang dilaksanakan selama proyek pengembangan sistem sedang dilaksanakan sampai selesai. *Review* merupakan bagian dari tanggung jawab manajer proyek tersebut. *Evaluation* digunakan untuk menyatakan proses penilaian hasil dari suatu proyek setelah dioperasionalkan dalam kurun waktu tertentu, dari beberapa bulan hingga beberapa tahun, bergantung kepada tipe proyeknya. Karena SI-RJ berbasis komputer di RS Dr.Kariadi telah diimplementasikan dan dioperasionalkan sejak 1997, maka seharusnya sudah dilakukan evaluasi terhadap sistem ini, termasuk evaluasi terhadap fitur keamanan datanya.

4.2.2 Pembahasan tiap fitur

4.2.2.1 Otentikasi (*authentication*)

4.2.2.1.1 Identitas terdaftar dari pengguna yang sah (KIP) beserta passwordnya

Kebijakan yang mengatur hal-hal yang berkaitan dengan pemberian dan penggunaan otentikasi kepada setiap pengguna sistem belum diterbitkan.

Secara teknis, sistem saat ini telah menerapkan penggunaan KIP dan password hingga 12 digit untuk setiap pengguna. Pengguna dapat mengubah passwordnya kapan saja bila dikehendakinya. Dengan ketersediaan ruang 12 digit untuk kombinasi password, maka terdapat lebih dari 1 milyar kombinasi password yang dapat digunakan. Hal ini sudah sangat memperkecil peluang seseorang untuk mencoba mencari password pengguna yang lain. Keleluasaan pengguna sistem untuk mengubah passwordnya kapan saja bila dikehendaki juga makin memperkecil peluang seseorang untuk melacaknya. Namun sayangnya, semua pengguna sistem saat ini ternyata hanya menentukan password satu kali saja dan tidak pernah mengubahnya lagi, apalagi secara periodik. Seluruh data otentikasi pengguna sistem disimpan dalam *file* khusus namun tidak dienkripsi. Hanya AKS yang memiliki akses untuk melihat dan memodifikasi *file* pencatat data KIP dan password seluruh pengguna sistem. Dengan demikian, apabila ada pengguna yang lupa passwordnya dapat menanyakan kepada AKS. Belum dienkripsinya *file* otentikasi pengguna ini juga membuka peluang bagi penyalahguna

sistem untuk mencuri-baca isi *file* tersebut dan mencuri-pakai KIP serta password yang dikehendakinya.(National Academy of Sciences, 1997)

4.2.2.1.2 Pengaturan tata cara penggunaan KIP dan password

Belum pernah diadakan pelatihan yang secara khusus membahas tentang teknis menentukan, menggunakan dan mengelola password untuk pengguna SI-RJ berbasis komputer di RS Dr.Kariadi. Hal ini sebenarnya sangat dibutuhkan untuk membekali pengguna sistem dengan kesadaran dan pemahaman yang benar tentang password sehingga dapat membentuk sikap dan perilaku yang benar pula dalam menggunakan dan mengelola password. Adanya kebijakan yang secara tegas menyatakan kewajiban pengguna sistem untuk menjaga kerahasiaan KIP dan passwordnya menjadi sangat diperlukan. Kepastian aturan dan sangsi pelanggaran akan ikut membentuk kebiasaan pengguna sistem dalam ketertiban penggunaan KIP dan passwordnya masing-masing.(Amayatakul, Margret; Walsh, Tom, 2001)

Selain menentukan jadwal akses, AKS juga telah menentukan *idle time* dan *automatic logout.* Bila kemudian pengguna itu hendak menggunakan sistem kembali, maka ia wajib melakukan *login* dengan memasukkan kembali KIP dan passwordnya. Mengingat banyaknya aktifitas yang dilakukan oleh seorang petugas di unit rawat jalan, maka besar kemungkinan terjadi adanya *workstation* yang ditinggalkan dalam keadaan *login.* Fasilitas *idle time* dan *automatic logout* ini bermanfaat untuk menjaga sistem dari kemungkinan digunakan orang yang tidak

berhak, yang "menemukan" sistem dalam keadaan *login* ditinggalkan begitu saja oleh penggunanya melebihi batas *idle time* tanpa melakukan *logout* terlebih dahulu. (National Academy of Sciences, 1997)

4.2.2.1.3 Kebijakan dan prosedur penggunaan sistem

Perubahan cara dan pola kerja dari basis manual ke basis komputer memerlukan waktu untuk sosialisasi, adaptasi, dan penyesuaian pengetahuan; sikap; dan praktek (etos kerja) pengguna sistem. Pengguna sistem di lingkungan RS Dr. Kariadi memiliki kebiasaan "berbagi" KIP dan password. Mereka melakukan ini dengan alasan untuk memperlancar pekerjaan apabila sedang berhalangan. Dengan demikian, apabila seorang petugas tidak masuk kerja atau sibuk dengan tugas lainnya, dia bisa minta bantuan teman kerjanya untuk menyelesaikan tugasnya dengan menggunakan KIP dan passwordnya. Kebiasaan ini jelas tidak menunjang aspek penjagaan kerahasiaan dan keamanan data dalam SIM RS berbasis komputer. Dengan diketahui dan digunakannya KIP dan password oleh lebih dari satu pengguna, penelusuran jejak penggunaan sistem menjadi lebih sulit. Dengan demikian penentuan tanggung jawab terhadap kualitas data yang terekam dan penelusuran jejak terhadap pelepasan informasi dari sistem juga menjadi lebih sulit. Demikian pula dengan perilaku mencatat KIP dan password di tempat yang mudah dibaca umum, misalnya di kertas yang ditempelkan di samping monitor, di bawah kaca meja atau di dinding belakang meja kerja.

Belum adanya kebijakan dan aturan yang menegaskan keharusan seorang pengguna untuk menjaga kerahasiaan otentikasinya menyebabkan sering terjadi "pinjam-meminjam" otentikasi antar pengguna. Keadaan ini dapat menimbulkan kesulitan bagi pengguna maupun institusi jika terjadi kesalahan atau penyalahgunaan sistem. Dari sudut pandang pengguna sistem, mereka menganggap pinjam-meminjam otentikasi antar pengguna ini untuk memperlancar penyelesaian tugas saat menggantikan petugas yang berhalangan hadir. Adapun aspek kerahasiaan data dan penetapan tanggung jawab hanya didasarkan pada saling percaya saja. Kebiasaan ini tidak sesuai dengan prinsip penjagaan keamanan data dalam pengelolaan sistem informasi berbasis komputer, termasuk juga sistem informasi rawat jalan di RS Dr.Kariadi. Seorang pengguna sistem informasi berbasis komputer harus menjaga kerahasiaan data otentikasinya (KIP dan password). Penyerahan data otentikasinya kepada orang lain sehingga menimbulkan penyalahgunaan terhadap sistem menjadi tanggung jawab sepenuhnya dari pemilik otentikasi tersebut. Pemahaman mengenai penjagaan data otentikasi dan penjagaan kerahasiaan data / informasi dalam sistem informasi berbasis komputer sangat perlu bagi pengguna dan pengelola sistem. (Computer-based Patient Record Institute, 1999; Amatayakul, Margret; Walsh, Tom, 2001)

4.2.2.1.4 Kebijakan yang mengatur wewenang AKS

Pihak manajemen RS Dr.Kariadi belum menerbitkan kebijakan yang secara khusus mengatur wewenang AKS. Administrator Keamanan Sistem (AKS) dapat melakukan pemutusan akses seketika (*real time*) terhadap seorang pengguna yang sedang berada dalam sistem apabila AKS menilai bahwa pengguna tersebut atau aktifitasnya tidak sah. Pemantauan dan pengendalian aktifitas seluruh pengguna ini dapat dilakukan AKS melalui komputer di ruang kerjanya. Keputusan yang diambil oleh AKS dalam melaksanakan tugasnya lebih berdasar pada pemahamannya tentang jaringan komputer termasuk keamanan data di dalamnya, bukan berdasar atas adanya kebijakan tentang kewenangannya.(Skurka M F, 1994; National Academy of Sciences, 1997; Computer-based Patient Record Institute, 1999)

4.2.2.2 Otorisasi (*authorization*)

Otorisasi mengatur lingkup hak dari seorang pengguna yang sah, meliputi hak akses terhadap fungsi sistem dan informasi yang terkandung didalamnya.(Computer-based Patient Record Institute, 1999)

Administrator Keamanan Sistem di RS Dr.Kariadi telah menentukan batasan akses bagi seorang pengguna atau suatu kelompok pengguna. Dengan demikian, pengguna hanya dapat melakukan akses terhadap menu atau fungsi tertentu saja dari sistem, sesuai dengan batasan yang telah ditentukan oleh AKS. Pengaturan batasan hak akses ini mengacu pada pemahaman bahwa informasi tertentu hanya ditujukan

untuk pengguna atau segmen pengguna tertentu saja. Setiap pengguna sistem terikat pada ketentuan sesuai PP nomor 10/1966 tentang wajib simpan rahasia medis. Dengan demikian, seorang pengguna wajib menyimpan rahasia yang diketahuinya berkenaan dengan hak aksesnya terhadap sistem.

4.2.2.2.1 Pengaturan menu yang dapat diakses

Pengendalian hak akses pengguna dalam sistem informasi berbasis komputer dapat dilaksanakan melalui tiga metode, yaitu *user-based access control, role-based access control* dan *context-based access control.* Selain memilih salah satu dari tiga metode, dapat pula dilakukan penggabungan dari dua atau bahkan tiga metode tersebut untuk memperkuat fitur otorisasi dalam mengendalikan hak akses pengguna sistem. Sistem informasi rawat jalan berbasis komputer di RS Dr.Kariadi menggunakan kombinasi antara *role-based access control* dan *context-based access control.* Dengan demikian, setiap petugas dalam unit kerja yang sama akan memiliki hak akses yang sama pula (*role-based access control*). Untuk menu dan fungsi tertentu (misalnya menu keuangan, fungsi menghapus, mengubah dan mencetak data) hanya "dibuka" untuk pengguna dari unit kerja yang memang memerlukan dan bertanggung jawab dengan hal itu, misalnya bagian kasir. Batasan hak akses yang dikenakan kepada seorang pengguna sekaligus juga merupakan upaya untuk mengurangi kemungkinan

lepasnya informasi kepada dan melalui orang yang tidak berhak / tidak perlu untuk mendapatkannya.

Setelah berada di dalam sistem, untuk mengakses menu-menu yang berkaitan dengan keuangan, penayangan laporan (di layar maupun di cetak ke kertas), dan menu perbaikan data, pengguna juga akan diminta untuk memasukkan passwordnya kembali. Apabila terjadi 3 kali kesalahan password untuk mengakses menu-menu tertentu ini, maka sistem secara otomatis akan melakukan *logout* terhadap pengguna tersebut. Fasilitas ini juga berkaitan dengan penjagaan keamanan data / informasi dalam sistem berbasis komputer. Seseorang yang "menemukan" sebuah *workstation* yang ditinggalkan oleh penggunanya dalam keadaan masih *login*, akan berhadapan dengan keharusan memasukkan password dari pengguna tersebut apabila ia bermaksud "melanjutkan" penggunaan *workstation* itu untuk mengakses menu atau fungsi tertentu, yang mungkin saja, bukan merupakan hak aksesnya. Jadi, perbuatan mengakses sistem dengan menggunakan otentikasi pengguna lain akan dapat dicegah.(Amatayakul, Margret; Walsh, Tom, 2001)

4.2.2.2.2 Pengaturan waktu akses

Saat ini AKS telah menentukan jadwal waktu akses untuk setiap pengguna sesuai dengan tugas masing-masing pengguna. Jadi misalnya, *workstation* milik petugas loket pendaftaran rawat jalan bisa digunakan untuk masuk ke sistem hanya pada jam kerja loket yang telah ditentukan,

yaitu jam 08.00-14.00 pada hari kerja. Sebaliknya, petugas di loket pendaftaran rawat inap dan rawat darurat dapat masuk ke sistem 24 jam penuh, sesuai dengan aktifitas loket tersebut. Pembatasan akses sesuai jam kerja melalui *workstation* ini telah dipadukan dengan pembatasan akses berdasarkan otentikasi pengguna. Jadi seorang petugas pendaftaran rawat jalan tetap tidak bisa masuk ke sistem diluar jam kerja rawat jalan meskiput dari *workstation* di lokasi lain, selama dia menggunakan otentikasinya yang telah terdaftar sebagai petugas pendaftaran rawat jalan.

Selain menentukan jadwal akses, AKS juga telah menentukan *idle time* (waktu jeda) selama 15 menit. Dengan adanya *idle time* ini, apabila seorang pengguna sistem yang sedang berada didalam sistem tidak melakukan aktifitas apapun terhadap sistem selama 15 menit, maka secara otomatis akan dilakukan *logout* terhadap pengguna tersebut. Bila kemudian pengguna itu hendak menggunakan sistem kembali, maka ia wajib melakukan *login* dengan memasukkan kembali KIP dan passwordnya. Mengingat banyaknya aktifitas yang dilakukan oleh seorang petugas di unit rawat jalan, maka besar kemungkinan terjadi adanya *workstation* yang ditinggalkan dalam keadaan *login*. Fasilitas *idle time* dan *automatic logout* ini bermanfaat untuk menjaga sistem dari kemungkinan digunakan orang yang tidak berhak, yang "menemukan" sistem dalam keadaan *login* ditinggalkan begitu saja oleh penggunanya

melebihi batas *idle* time tanpa melakukan *logout* terlebih dahulu. (National Academy of Sciences, 1997)

4.2.2.2.3 Pengaturan obyek yang dapat diakses

National Academy of Sciences (1997) mengelompokkan konsep hak akses pengguna sistem menurut empat kelompok informasi, yaitu :

1. *public information,* yaitu informasi yang dapat dilepaskan untuk semua pihak mana saja, baik dari dalam maupun luar institusi. Termasuk jenis informasi ini misalnya, materi yang bersifat promosi.
2. *internal confidential information,* yaitu informasi yang diperuntukkan bagi anggota organisasi atau yang berkaitan dengan itu dan harus melalui dasar pertimbangan memang-perlu-tahu (*need-to-know*). Termasuk jenis informasi ini misalnya, kebijakan organisasi, strategi bisnis dan informasi yang berkaitan dengan utilisasi atau *outcome*.
3. *confidential patient record information,* yaitu informasi yang diperuntukkan bagi pemberi layanan kesehatan (provider) dan pihak terkait (misalnya asuransi) yang memang-perlu-tahu tentang informasi ini. Termasuk jenis informasi ini adalah catatan kesehatan pasien.
4. *highly sensitive patient record information*, yaitu informasi yang diperuntukkan hanya bagi pihak tertentu yang memang berwenang dan memang-perlu-tahu catatan kesehatan pasien tertentu atau dalam keadaan tertentu. Termasuk jenis informasi ini misalnya rekam

medis selebritis atau *public figure* lainnya, rekam medis tentang riwayat kesehatan psikiatri, kekerasan fisik, HIV, dan abortus.(National Academy of Sciences, 1997)

Dalam SI-RJ berbasis komputer di RS Dr.Kariadi digunakan *internal confidential information* dan *confidential patient record information* dan tidak menggunakan pengelompokkan data ke dalam *public information* dan *highly sensitive patient record information.*

Penggunaan *anonymous patient IDs* belum diterapkan dalam SI-RJ berbasis komputer di RS Dr.Kariadi. Dalam metode ini, tampilan informasi baik di layar komputer maupun di kertas, hanya mencantumkan nomor rekam medis atau kode identitas lain tanpa menampilkan nama pasien. Penerapan metode ini sebenarnya mengurangi kemungkinan bocornya informasi kepada pihak yang tidak berwenang atau tidak perlu mengetahui. (National Academy of Sciences, 1997)

4.2.2.2.4 Pengaturan media yang dapat diakses

Fungsi "menghapus" (*delete*) dan "mengubah" (*edit*) data dalam sistem hanya merupakan kewenangan AKS. Apabila seorang pengguna mengalami kesalahan dalam memasukkan data, maka dia masih bisa membetulkan kesalahan pada hari tersebut. Namun apabila sudah melewati batas jam kerja, maka pembetulan kesalahan harus melalui AKS. Fungsi ini juga berkaitan dengan fungsi lain dalam sistem yaitu fungsi penyalinan data / *backup* dan berkaitan dengan fitur integritas

(*integrity*) dari sistem. Setiap hari pada jam 00.00, sistem secara otomatis melakukan penyalinan seluruh data pada hari tersebut ke media penyimpan data tingkat kedua. Jadi bila esok hari atau hari selanjutnya ada pengguna sistem yang bermaksud mengubah atau membetulkan isian data kemarin / beberapa hari yang lalu, sebetulnya data tersebut telah disalin ke media cadangan. Administrator Keamanan Sistem akan "mengembalikan" data yang dimaksud dari media cadangan ke dalam sistem. Setelah proses ini, barulah pengguna dapat membuka dan membetulkan / mengubah data yang dimaksudnya. Aktifitas perbaikan atau pengubahan data ini dicatat dalam *field* khusus sehingga AKS dapat melacak ulang perubahan yang dilakukan oleh pengguna. Catatan perubahan ini meliputi data yang diubah, perubahannya, waktu pengubahan, dan otentikasi pengguna yang melakukan perubahan tersebut.

4.2.2.3 Integritas (*integrity*)

Informasi yang tersedia dalam sistem hanya bisa dan hanya boleh diubah / diolah untuk kebutuhan tertentu dan oleh pengguna tertentu yang berhak.

Integritas data berkaitan dengan akurasi (*accuracy*), konsistensi (*consistency*), dan kelengkapan (*completeness*) dari data. Pemantauan integritas data juga harus dapat memastikan bahwa data tidak diubah atau dirusak melalui cara yang tidak sah.(Computer-based Patient Record Institute, 1999)

4.2.2.3.1 Pengendali kelengkapan pengisian data

Sistem informasi rawat jalan berbasis komputer yang diimplementasikan saat ini telah disiapkan untuk mengatur pengisian beberapa *field* data tertentu sedemikian sehingga pengguna "diwajibkan" untuk mengisinya (*required filed*). Hal ini bertujuan untuk menjaga agar *field* data tersebut tidak dibiarkan diam / kosong oleh pengguna pada saat pengisian data pelayanan seorang pasien. Apabila pengguna lupa atau sengaja mengosongkan isian pada *field* tersebut maka sistem akan menampilkan jendela dialog (*dialog box*) berisi pesan yang mengingatkan pengguna untuk melengkapi isian pada *field* tersebut. Cara ini secara langsung akan memaksa pengguna untuk memenuhi kebutuhan kelengkapan minimal dalam hal pengisian data (*data captured*) saat melayani pasien.

Beberapa *field* data lainnya juga diatur pengisiannya dengan metoda pilihan (*choise*) dari item yang telah disediakan (misalnya dengan *picking-up list* dan *choices*). Hal ini bertujuan untuk menjaga konsistensi isian pada *field-field* tersebut.

Gabungan antara penggunaan *required field* dengan metoda pilihan yang telah disediakan akan menghasilkan *field* yang terisi secara konsisten. Penggunaan metoda pilihan juga memudahkan petugas pengguna sistem dalam melengkapi pengisian data, mempercepat waktu pengisiannya dan menjaga konsistensi isian. Hal ini lebih baik daripada menyediakan *required field* yang harus diisi dengan metoda isian bebas

(petugas mengetikkan isian, tanpa pilihan yang disediakan) karena pada saat sibuk atau malas, petugas akan cenderung untuk mengisi semaunya, misalnya dengan memasukkan isian berupa spasi saja sebagai "syarat" pengisian *field* tersebut.(Computer-based Patient Record Institute, 1999)

4.2.2.3.2 Pemantau data transaksi yang batal dilaksanakan

Fungsi "menghapus" (*delete*) dan "mengubah" (*edit*) data dalam sistem hanya merupakan kewenangan AKS. Apabila seorang pengguna mengalami kesalahan dalam memasukkan data, maka dia masih bisa membetulkan kesalahan pada hari tersebut. Namun apabila sudah melewati batas jam kerja, maka pembetulan kesalahan harus melalui AKS. Digunakannya sistim pembatasan waktu untuk mengubah atau memperbaiki kesalahan pengisian data ini juga untuk meningkatkan integritas data dalam sistem tersebut.

Dengan diaktifkannya beberapa fungsi dalam fitur integritas ini, maka diharapkan integritas data dapat terjaga sejak dari tahap pengisian hingga penyimpanan dan perbaikan data.

4.2.2.3.3 Penangkal aktifitas virus komputer

Sistem telah dilengkapi dengan perangkat lunak anti virus komputer (Mc Affee versi 6). Perangkat lunak anti virus yang digunakan juga diperbarui secara berkala (*update*) untuk menjaga efektifitasnya dalam mengenali jenis virus baru. Sistem anti virus ini sudah mampu menangkal aktifitas virus komputer, baik yang di memori komputer maupun yang langsung menyerang media data dan menyebabkan *logical*

error. Selain itu, untuk mencegah masuknya virus komputer dari *workstation*, maka digunakan metode *diskless workstation*. Penggunaan *diskless workstation* ini juga sekaligus mencegah kemungkinan pencurian informasi dari dalam sistem melalui proses *copy* ke disket. Dari sisi lain, hal ini juga mencegah pengguna untuk memasukkan (meng-*install*) atau menggunakan program bantu lain dari luar sistem. Dengan perkembangan teknologi informasi saat ini, maka penggunaan *flash disk* melalui koneksi ke USB (*Universal Serial Board*) dapat menjadi pengganti keberadaan *disk drive*. Dalam hal ini, seluruh *workstation* dalam sistem ini tidak dilengkapi dengan USB-*port*. Dengan meminimalkan resiko keamanan melalui pengendalian penggunaan *workstation* ini maka aspek *network* dan *desktop* yang menduduki posisi keempat dan kelima dalam *top six security risks* dapat diatasi.

4.2.2.3.4 Pencegah kemungkinan akses data dari luar organisasi

Keseluruhan jaringan komputer dalam SIM RS di RS Dr. Kariadi, termasuk jaringan SI-RJ tidak terhubung ke internet dan tidak memiliki jalur akses dari luar rumah sakit. Tidak adanya koneksi dengan jaringan di luar RS termasuk internet, sangat mengurangi resiko gangguan terhadap keamanan data dalam sistem ini mengingat internet menduduki rangking pertama dalam *top six security risks*.(Wagner, Lew, 2002)

4.2.2.4 Penelusuran jejak (*audit trails*)

Fitur ini berfungsi untuk memantau setiap operasi terhadap sistem informasi. Fitur ini dapat dimanfaatkan untuk mendeteksi dan melacak penyalahgunaan dan pelanggaran keamanan, menentukan dilaksanakan tidaknya kebijakan dan prosedur operasional yang berlaku, serta untuk merekonstruksi rangkaian aktifitas yang dilakukan terhadap sistem.(Computer-based Patient Record Institute, 1999)

Sistem yang digunakan saat ini mampu memantau aktifitas pengguna dan mencatatnya kedalam suatu berkas penelusuran jejak. Setiap kegiatan akses terhadap sistem secara otomatis terekam dalam *log-file* Hal-hal yang dicatat kedalam *log-file* ini meliputi:

1. kode identitas pengguna (KIP),
2. tanggal; jam; durasi dan lokasi akses,
3. menu yang diakses,
4. jenis data yang diakses berikut aktifitas terhadap data tersebut,
5. aktifitas yang berkaitan dengan otoritas akses; termasuk kesalahan penggunaan sistem dan pelanggaran terhadap prosedur keamanan.

Berkas penelusuran jejak hanya bisa diakses oleh AKS. Berkas ini sangat dibutuhkan oleh AKS terutama pada saat terjadi komplain terhadap ketidaksesuaian hasil pencatatan kegiatan pelayanan terhadap pasien, misalnya ketidaksesuaian jumlah tagihan dengan jenis pelayanan yang diberikan. Berkas ini belum digunakan sebagai sumber penyusunan laporan rutin tentang aktifitas sistem. Laporan *audit trails* sebenarnya

harus di*review* secara rutin dan berkala untuk memantau aktifitas penggunaan sistem dan untuk mendeteksi secara dini gangguan dan penyalahgunaan sistem.(National Academy of Sciences, 1997)

Administrator Keamanan Sistem belum menetapkan penggunaan *log book* atau pencatatan secara manual terhadap aktifitas penggunaan sistem. Apabila akan diterapkan penggunaannya, maka dibutuhkan sosialisasi dan penyamaan persepsi terlebih dahulu tentang tujuan penggunaan dan manfaat dari *log book* tersebut. Pengguna sistem harus dengan sadar dan tertib mencatat sendiri setiap aktifitasnya kedalam *log book.* Untuk mengoptimalkan fungsinya, maka hal-hal yang dicatat kedalam *log book* dapat meliputi :

1. kode identitas pengguna (KIP),
2. tanggal; jam; durasi akses,
3. menu yang diakses,
4. jenis data yang diakses berikut aktifitas terhadap data tersebut, dan
5. aktifitas yang berkaitan dengan otoritas akses; termasuk kesalahan penggunaan sistem dan pelanggaran terhadap prosedur keamanan.

National Academy of Sciences (1997) merekomendasikan bahwa pasien seharusnya diberi hak akses terhadap berkas *audit trails* sehingga dapat mengetahui siapa yang telah mengakses informasi kesehatannya dan apa yang telah dilakukan terhadap informasinya tersebut. Hal ini juga atas pertimbangan dasar bahwa informasi yang terekam dari suatu kegiatan pelayanan kesehatan adalah milik pasien yang bersangkutan.

Dalam SI-RJ berbasis komputer di RS Dr.Kariadi, pasien tidak memiliki hak akses terhadap informasi tentang dirinya dan juga terhadap berkas *audit trails*-nya.

4.2.2.5 Pemulihan pasca bencana (*disaster recovery*)

Fitur pemulihan pasca bencana merupakan proses yang memungkinkan institusi untuk memulihkan kembali data-data yang hilang atau rusak setelah terjadinya suatu gangguan / bencana, misalnya kebakaran; banjir; huru-hara; bencana alam; atau kegagalan sistem.(Computer-based Patient Record Institute, 1999)

Penyalinan data dilakukan kedalam media penyimpan data (*harddisk*) yang juga terletak di dalam *active server*. Hasil penyalinan ini kemudian disalin lagi kedalam *harddisk* yang lain diluar *active server* (*backup server*). Dengan demikian AKS selalu memiliki dua salinan data dalam dua *harddisk*. Adanya dua salinan ini lebih menjamin ketersediaan data untuk pemulihan seandainya diperlukan. Penggunaan *harddisk* sebagai media penyimpan dapat dipertimbangkan untuk diganti atau dikombinasi dengan *Compact Disc* (CD) yang teknologinya saat ini sudah tersedia secara mudah dan relatif murah. Kapasitas CD saat ini (625 Giga bite) masih bisa menampung salinan seluruh data yang ada, mengingat kapasitas *harddisk* yang digunakan saat inipun hanya 2,8 Gigabyte. Sebagai media penyimpan data, CD lebih praktis dan lebih tahan lama. Disamping itu, harga CD-*writer* dan CD kosong saat ini sudah relatif lebih murah dan terjangkau.

Perlu dipertimbangkan untuk menyalin seluruh data terakhir saat ini kedalam satu atau beberapa CD untuk disimpan, sehingga AKS memiliki salinan data keseluruhan hingga saat penyalinan tersebut.

Harddisk tempat menyimpan salinan data tingkat kedua disimpan dalam ruang yang sama dengan *active server*. Perlu dipertimbangkan untuk menyimpan media penyimpan salinan data (*harddisk* ataupun CD) ditempat yang berbeda dengan ruang *server*. Tindakan ini sekaligus juga mengoptimalkan fitur penyimpanan dan transmisi data yang aman (*secure data storage & transmission*). Hal ini untuk menjaga agar apabila terjadi keadaan darurat seperti kebakaran, gempa bumi, pencurian, atau yang sejenisnya yang menimpa ruang *active server*, maka media salinan data tersebut tidak ikut rusak atau hilang. Mengingat hal ini, maka layak untuk dipertimbangkan pula untuk memiliki salinan program dari sistem informasi yang digunakan saat ini dan disimpan ditempat yang berbeda dengan *active server*.(National Academy of Sciences, 1997; Amatayakul, Margret, 2002)

Salinan data yang dibuat oleh sistem saat ini belum menggunakan teknologi enkripsi. Keadaan ini beresiko untuk terjadinya kebocoran informasi apabila ada pihak yang menggunakan data yang tersimpan sebagai salinan tersebut secara tidak sah, misalnya meng*copy* data dari *harddisk* atau mencuri *harddisk*-nya. Untuk mencegah resiko ini, National Academy of Sciences (1997) dan Computer-based Patient Record Institute (1999) merekomendasikan penggunaan teknologi

enkripsi terhadap salinan data dari sistem informasi berbasis komputer. Selain itu, penjagaan secara fisik terhadap *hardisk* atau media penyimpan salinan data lainnya yang disimpan di tempat terpisah dari *active server* juga sangat dibutuhkan untuk mencegah pencurian atau menggunaan secara tidak sah.

4.2.2.6 Penyimpanan dan transmisi data yang aman (*secure data storage & transmission*)

Keamanan penyimpanan data berkaitan dengan media fisik serta lokasi dimana data disimpan dan dikelola. Transmisi data berkaitan dengan aktifitas pertukaran data antara pengguna dan program atau antara program dan program, dimana pengirim dan penerima dipisahkan oleh suatu jarak.(National Academy of Sciences, 1997)

Seperti telah diuraikan di atas, saat ini seluruh perangkat keras dan perangkat lunak (termasuk salinan data) berada dan disimpan dalam satu ruang di unit kerja AKS. Selain memiliki keuntungan dalam hal kemudahan pengambilan saat dibutuhkan dan penjagaan keamanannya, cara penyimpanan ini juga memiliki kekurangan yaitu resiko kerusakan atau kehilangan yang relatif total bila terjadi gangguan fisik terhadap ruang ini, misalnya kebakaran, gempa bumi, atau pencurian. (National Academy of Sciences, 1997)

Amatayakul (2002) menekankan pentingnya penjagaan keamanan fisik jaringan beserta elemennya melalui beberapa langkah pengamanan, misalnya :

1. peletakan monitor *workstation* menghadap kearah yang menjadikan orang lain selain pengguna tidak mudah melihat apa yang sedang ditampilkan saat itu,
2. peletakan *workstation* di dalam ruang kerja yang berpintu dan dapat dikunci sehingga mencegah orang lain selain pengguna untuk masuk,
3. peletakan alat cetak (*printer*) menghadap kearah yang menjadikan orang lain selain pengguna tidak mudah melihat apa yang sedang dicetak dan tidak mudah menjangkau / mengambil hasil cetakan,
4. peletakan kertas bekas hasil cetakan di tempat yang tidak dapat dijangkau oleh lain atau bila memungkinkan dihancurkan dengan penghancur kertas (*paper shredder),*
5. peletakan kabel-kabel jaringan melalui saluran khusus sehingga tidak mudah dijangkau oleh orang yang bermaksud mengganggu atau melakukan sabotase.

Dalam SI-RJ berbasis komputer di RS Dr.Kariadi, tidak ada monitor *workstation* yang peletakannya menghadap konsumen dan memudahkan konsumen untuk melihat data yang sedang ditampilkan. Semua *workstation* terletak dalam ruang kerja yang berpintu dan dapat dikunci. Posisi *printer* dan kertas hasil cetakannya tidak mudah dijangkau oleh pasien yang sedang dilayani.

Dalam hal transmisi data, sistem yang dikembangkan saat ini memiliki kemampuan untuk mengendalikan aktifitas fungsi *export* dan *import* data. Dengan adanya fungsi ini, maka data dari dalam sistem

dapat "diambil" keluar (*export*) untuk diolah dengan menggunakan perangkat lunak pengolah data diluar sistem. Sebaliknya, sistem juga dapat "menerima" (*import*) data dari luar jalur penangkapan data dalam sistem. Fungsi ini hanya dapat dilakukan melalui komputer milik AKS karena *workstation* lainnya menggunakan model *diskless*. Hanya AKS yang dapat memanfaatkan fungsi ini. Dengan pembatasan fungsi ini yang hanya AKS yang dapat mengoperasikan, maka pencegahan terhadap pencurian data dan informasi dari dalam sistem dapat dicegah.

Proses *export* dan *import* data ini belum menggunakan metoda enkripsi untuk keamanan datanya sehingga apabila ada seseorang yang secara tidak sah menggunakan komputer milik AKS untuk meng*export* data, maka setelah berada diluar sistem data tersebut dapat langsung dibaca dan dipergunakan. Perlu dipertimbangkan untuk melengkapi fungsi *export* dan *import* ini dengan metoda enkripsi. Penjagaan terhadap akses komputer milik AKS (*server*) perlu dilakukan mengingat *host* merupakan salah satu dari 6 hal dalam *top six security risks* dan berada pada urutan ketiga.(Computer-based Patient Record Institute, 1999; Wagner, Lew, 2002)

BAB V

KESIMPULAN dan SARAN

5.1 Kesimpulan

Rumah sakit Dr.Kariadi sudah memiliki visi dan misi dalam penyelenggaraan rekam medisnya. Implementasi SI-RJ berbasis komputer di RS Dr.Kariadi merupakan pengembangan dari sistem manual yang telah ada sebelumnya. Sebagai bagian dari SI-RM, SI-RJ berada dalam tanggung jawab pengelolaan Divisi Sim-RS & Kom. Sebagai pengelola dan penanggung jawab keamanan sistem telah ditunjuk seorang Administrator Keamanan Sistem (AKS) namun belum ada kebijakan dan prosedur tetap (protap) yang menjelaskan *job description* dari AKS. Belum ada kebijakan dan protap yang secara khusus mengatur hal-hal yang berkaitan dengan tata cara pengoperasian SI-RJ berbasis komputer.

Dengan demikian, fitur keamanan data pada SI-RJ berbasis komputer di RS Dr.Kariadi Semarang belum berfungsi secara penuh dalam menjaga keamanan data dan informasi yang terkandung dalam sistem tersebut.

5.1.1 Otentikasi (*authentication*)

Metode otentikasi yang digunakan merupakan kombinasi dari Kode Identitas Pengguna (KIP) dan password hingga12 digit. Kode Identifikasi Pengguna dan password pertama kali ditentukan oleh Administrator Keamanan Sistem (AKS). Pengguna kemudian dapat mengubah password kapan saja. Fitur otentikasi dilengkapi dengan adanya batasan *idle time* dan *automatic logout*.

File data KIP dan password yang berisi catatan otentikasi seluruh pengguna tidak menggunakan metode enkripsi.

Fitur otentikasi ini menjadi lemah dengan adanya kebiasaan "pinjam-meminjam" otentikasi diantara petugas.

5.1.2 Otorisasi (*authorization*)

Metode yang digunakan merupakan gabungan dari *role-based access control* dengan *context-based access control*.

Pasien tidak memiliki hak akses terhadap data kesehatannya maupun *file audit trails*-nya.

Metode *anonymous patient IDs* tidak digunakan dalam fitur ini.

5.1.3 Integritas (*integrity*)

Required fields digunakan dalam sistem ini untuk menjaga integritas data saat pemasukan data.

Diskless / non-USB workstation juga berfungsi untuk mencegah proses *export / import* data yang bisa digunakan untuk pencurian informasi dari sistem atau untuk tujuan lain yang mengganggu sistem.

5.1.4 Pelacakan jejak (*audit trails*)

Metode pancatatan aktifitas sistem ini digunakan untuk mencatat :

1. kode identitas pengguna (KIP),
2. tanggal; jam; durasi dan lokasi akses,
3. menu yang diakses,
4. jenis data yang diakses berikut aktifitas terhadap data tersebut,

5. aktifitas yang berkaitan dengan otoritas akses; termasuk kesalahan penggunaan sistem dan pelanggaran terhadap prosedur keamanan.

Hasil *audit trails* belum digunakan untuk monitoring sistem secara rutin dan berkala. Hasil *audit trails* hanya digunakan pada saat ada kebutuhan pelacakan saja. *File audit trails* belum menggunakan metode enkripsi atau metode pengamanan data lainnya.

Hanya AKS yang memiliki hak akses terhadap *file audit tails.*

5.1.5 Pemulihan pasca bencana (*disaster recovery*)

Sudah ada metode panyalinan data rutin setiap pukul 00:00. Hasil penyalinan data disimpan dalam *harddisk* di *active server* dan *backup server.* Seluruh hasil proses penyalinan data disimpan dalam ruang yang sama dengan *active server*, yaitu di ruang kerja AKS.

Hasil penyalinan data tidak menggunakan metode enkripsi.

Untuk mencegah gangguan dari virus komputer, digunakan perangkat lunak anti virus (Mc Affee 6), *diskless / non-USB workstation*, dan tidak membuka jalur akses dari luar maupun keluar dari sistem.

5.1.6 Penyimpanan dan transmisi data yang aman (*secure data storage & transmission*)

Dalam SI-RJ berbasis komputer terdapat fungsi *export* dan *import* data. Fungsi ini tidak dilengkapi dengan metode pengaman data.

File data tidak memiliki sistem pengaman, misalnya enkripsi, kunci *file*, ataupun kunci *field.*

Jaringan SI-RJ dan SIM-RS di RS Dr.Kariadi tidak terhubungan ke internet dan tidak memiliki akses dari luar atau keluar jaringan.

Penempatan *workstation* dan *peripheral*-nya diatur dalam ruang tertutup dan dapat dikunci. Tampilan monitor komputer dan hasil *print-out* menghadap kearah yang menjadikan orang lain tidak mudah untuk melihat atau menjangkaunya.

5.2 Saran

5.2.1 Perlu disusun dan diterbitkan kebijakan yang berkaitan dengan implementasi SI-RJ berbasis komputer. Kebijakan yang dimaksud yaitu :

1. kebijakan keamanan data (*security policies*) yang mencakup antara lain filosofi, tujuan, otentikasi dan kendali akses, *reliability* dan *integrity*;
2. kebijakan kerahasiaan data (*confidentiality policies*) yang mengatur keseimbangan antara hak dan kebutuhan akses dengan keharusan penjagaan kerahasiaan informasi yang diakses;
3. kebijakan penjagaan informasi yang sensitive (*policies to protect sensitive information*) yang mengatur pengelolaan informasi medis, misalnya yang berkaitan dengan penyalahgunaan narkoba, penyakit akibat hubungan seksual, HIV/AIDS, dan sebagainya;
4. kebijakan penggunaan informasi kesehatan untuk penelitian (*policies on research uses of health information*) yang mengatur tentang pelepasan informasi medis untuk kebutuhan penelitian;
5. kebijakan yang mengatur perihal pelepasan informasi kesehatan secara umum (*policies guiding release of health information*);

6. kebijakan yang berkaitan dengan pasien sebagai isu sentral, misalnya kebijakan akses terhadap data dan catatan penggunaannya (*access to record and audit logs policies*) yang mengatur batasan hak akses petugas pengguna sistem, termasuk juga hak akses pasien terhadap *file* rekam medisnya, dan
7. kebijakan yang mengatur kewenangan Administrator Keamanan Sistem (AKS).

5.2.2 Perlu diselenggaran pelatihan yang secara khusus membahas tentang teknis menentukan, menggunakan dan mengelola password untuk pengguna SI-RJ berbasis komputer di RS Dr.Kariadi untuk membekali pengguna sistem dengan kesadaran dan pemahaman yang benar tentang password sehingga dapat membentuk sikap dan perilaku yang benar pula dalam menggunakan dan mengelola password.

5.2.3 Metode enkripsi atau metode pengaman file lainnya perlu digunakan untuk memperbaiki fitur otentikasi, integritas, pelacakan jejak, fungsi penyalinan data dan fungsi transmisi data.

5.2.4 Metode *anonymous patient IDs* perlu digunakan untuk memperbaiki fitur otorisasi.

5.2.5 Perlu digunakan sistem pengaman *file* data (misalnya enkripsi, kunci *file*, atau kunci *field*).

5.2.6 Perlu dipertimbangkan untuk memisahkan penyimpanan media penyimpan hasil salinan data (*backup*) dengan *active server* untuk mencegah kehilangan

atau kerusakan yang bersifat total jika terjadi gangguan fisik (misalnya kebakaran, gempa bumi, pencurian) terhadap ruang *active server*.

5.2.7 Perlu diadakan penelitian lanjutan untuk merumuskan kebutuhan pengembangan SIM-RS berbasis komputer, termasuk SI-RJ, di RS Dr.Kariadi untuk masa mendatang, khususnya aspek keamanan data apabila ingin mengembangkan sistem saat ini dengan memanfaatkan teknologi koneksi internet atau intranet.

--------- o0o ---------

DAFTAR PUSTAKA

Amatayakul, Margret, *HIPAA On The Job: A Reasonable Approach to Physical Security*, Journal of AHIMA, Chicago, Illinois, April 2002:16.

Amatayakul, Margret, *HIPAA On The Job:The First Line of Defense Against Privacy Complaints,* Journal of AHIMA, Chicago, Illinois, October 2002:24.

Amatayakul, Margret; Walsh, Tom, *HIPAA On The Job:Selecting Strong Passwords,* Journal of AHIMA, Chicago, Illinois, October 2001:16.

Austin, Charles J., Boxerman, Stuart B., *Information System for Health Services Administration*, 5th ed, Aupha Press/Health Administration Press, Chicago, Illinois, 1998.

Computer-based Patient Record Institute.*CPRI Tool Kit: Managing Information Security in Health Care*, Computer-based Patient Record Institute, Bethesda, 1999.

Dougherty, Michelle, *Practice Brief: Maintaining a Legally Sound Health Record*, Journal of AHIMA, Chicago, Illinois, September 2002: 64.

Hawkins, Fanny. *Working smart:Putting the EHR to the Test,* Journal of AHIMA, Chicago, Illinois, September 2002: 65-7.

Heather, Heathfield; Clamp, Susan; Felton, Derek. *Project Review and Objective Evaluation (PROBE) for Electronic Patient and Health Record Projects*, UK Institute of Health Informatic, Winchester, Hampshire, March 2001.

Medical Records Institute. *Medical Records Institute Survey of Electronic Health Record Trends and Usage*, www.medrecinst.com, accessed July 2001.

Merida L Johns. *Information Security.* In: Health Information Management Technology-an Applied Approach. AHIMA, Chicago, Illinois, 2001.

National Academy of Sciences. *For the Record – Protecting Electronic Health Information*, National Academy Press, Washington, D.C., 1997.

Shofari, Bambang, *Analisis Kebutuhan Informasi Manajemen Rumah Sakit*, Modul Program Pengembangan Profesi Magister Manajemen Rumahsakit Universitas Gadjah Mada, MMR UGM, Yogyakarta, 1998.

Skurka M F, *Health Information Management in Hospitals-Principles and Organization for Health Record Services*, American Hospital Publishing Inc., Indiana,1994.

Wagner, Lew. *Feature article:Uniting Security Forces Against Risk*, Journal of AHIMA, Chicago, Illinois, June 2002: 39-41.

Whitten J L; Bentley L D and Barlow V M. *Systems Analysis & Design Methods*, Irwin, Boston, 1989.

Wilson, Randy. *Using Computers in Health Information Systems.* In: Design and Implementation of Health Information Systems, World Health Organization, Geneva, 2000.

Woloszyn, William, *Privacy and Security: Are Two Hats Better than One?*, Journal of AHIMA, Chicago, Illinois, June 2002:59.