SURAT KEPUTUSAN
Nomor:

TENTANG

KEAMANAN INFORMASI DAN INTEGRITAS DATA DI RUMAH SAKIT

Menimbang :

a. bahwa dalam proses pelayanan pasien, perlu dilakukan keamanan informasi dan integritas data pasien Rumah Sakit Khusus Ginjal NY. R.A. Habibie. agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab;

b. bahwa hanya staf / karyawan yang mendapat kewenangan (otoriras) saja yang dapat mengakses data dan informasi sesuai dengan kebutuhannya;

c. bahwa berdasarkan pertimbangan pada poin a dan b diatas, maka perlu ditetapkan Keamanan Informasi Data dan Integritas Data di Rumah Sakit Khusus Ginjal NY. R.A. Habibie, dengan keputusan Direktur Rumah Sakit;

Mengingat :

1. Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.
2. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.
3. Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit.
4. Peraturan Menteri Kesehatan No. 269/Menkes/Per/III/2008 Peraturan Menteri Kesehatan No. 269/Menkes/Per/III/2008 tentang Rekam Medis.

Memperhatikan :

1. Perlunya usaha untuk meningkatkan kualitas keamanan data Sistem Informasi Manajemen di Rumah Sakit Khusus Ginjal NY. R.A. Habibie.

MEMUTUSKAN

Menetapkan :

PERTAMA **KEPUTUSAN DIREKTUR RUMAH SAKIT TENTANG KEAMANAN INFORMASI DAN INTEGRITAS DATA DI RUMAH SAKIT.**

KEDUA Keamanan informasi dan Integritas Data di rumah Sakit sebagaimana tercantum dalam lampiran keputusan ini.

KETIGA Agar Kebijakan yang dimaksud pada Diktum kedua dapat menjadi acuan bagi seluruh petugas Rumah Sakit Ginjal NY. R.A. Habibie yang melayani pasien.

KEEMPAT Keputusan ini berlaku sejak tanggal ditetapkan dan akan dievaluasi setiap 3 (tiga) tahun sekali ataupun apabila dikemudian hari ternyata terdapat kekeliruan didalam keputusan ini.

Ditetapkan di : Bandung

Pada Tanggal : 30 Januari 2020

DIREKTUR Rumah Sakit Khusus Ginjal NY. R.A. Habibie

dr. Qania Mufliani, MM

LAMPIRAN
KEPUTUSAN DIREKTUR RUMAH SAKIT
KHUSUS GINJAL NY. R.A. HABIBIE
NOMOR : .. / / IT /RSKG-SK-DIR/ 2020
TENTANG
KEAMANAN INFORMASI DAN INTEGRASI
DATA DI RUMAH SAKIT

KEAMANAN INFORMASI DAN INTEGRITAS DATA

DI RUMAH SAKIT

LATAR BELAKANG

Penerapan manajemen informasi dan komunikasi tidak dapat terlepaskan dari operasional pelayanan kesehatan di Rumah Sakit. Informasi rekam kesehatan bersifat pribadi dan rahasia sehingga harus dijaga integritas informasi dan keamanannya agar tidak disalahgunakan oleh pihak-pihak yang mempunyai berkepentingan pribadi atau golongan. Semua petugas terkait rekam medis harus tahu dan paham tentang privasi, kerahasiaan dan keamanan informasi rekam kesehatan. Semua petugas yang terkait dengan rekam medis wajib menjaga privasi, kerahasiaan dan keamanan rekam medis.

TUJUAN

1. Tujuan Umum

Untuk memberikan acuan bagi terselenggaranya penerapan dan pengoperasian sistem informasi yang aman dan terjaga integritas datanya serta sejalan dengan kebijakan keselamatan pasien di Rumah Sakit.

2. Tujuan Khusus

a. Mengurangi kesalahan pengambilan data pasien
b. Melindungi data pasien dari kebocoran & kerusakan
c. Melindungi data & integritas data pasien
d. Melindungi data & integritasnya dari virus mau pun serangan dari dalam/luar
e. Terciptanya budaya keselamatan pasien saat menggunakan sistem informasi rumah sakit
f. Terlaksananya program-program pencegahan sehingga tidak terjadi pengulangan Kejadian Yang Tidak Diharapkan (KTD) yang berhubungan dengan sistem informasi Rumah Sakit.

KEBIJAKAN UMUM

1. Kebijakan Ketepatan Identifikasi Pasien di Rumah Sakit

Secara administratif, identifikasi pasien diperlukan untuk setiap proses sebagai berikut:

a. Sebelum melakukan pendaftaran pasien rawat inap atau rawat jalan
b. Sebelum mencatat transaksi pelayanan medis
c. Sebelum mencatat transaksi pelayanan penunjang medis
d. Sebelum membuat transaksi obat dan alat kesehatan
e. Sebelum membuat transaksi pembayaran

Berikut adalah cara identifikasi pasien dengan benar:

a. Identifikasi pasien dengan benar dilakukan dengan sedikitnya dua cara identifikasi, yaitu:

   Nama Lengkap Pasien DAN Nomer Rekam Medis Pasien. ATAU Nama Lengkap Pasien DAN Tanggal Lahir Pasien.

b. Identifikasi pasien dilakukan dengan cara:
   i. Pasien Rawat Inap dan ODS (*One Day Surgery*) dengan menanyakan **Nama Lengkap Pasien** dan kemudian mencocokkan **Nama Lengkap DAN Nomer Rekam Medis** pada gelang identitas pasien dengan **Nama Lengkap DAN Nomer Rekam Medis** pada berkas rekam medis atau formulir lain yang terkait dengan proses yang sedang dilakukan.
   ii. Pasien Unit Gawat Darurat (UGD), unit Rawat Jalan dan unit Penunjang Medik lainnya dengan menanyakan **Nama Lengkap Pasien** dan kemudian mencocokkan **Nama Lengkap DAN Nomer Rekam Medis** pada kartu pasien dengan **Nama Lengkap DAN Nomer Rekam Medis** pada berkas rekam medik atau formulir lain terkait proses yang sedang dilakukan.
   iii. Bila kartu pasien tidak tersedia, maka identifikasi pasien dilakukan dengan cara menanyakan **Nama Lengkap Pasien DAN Tanggal Lahir Pasien** kemudian mencocokkannya dengan **Nama Lengkap Pasien dan Tanggal Lahir Pasien** pada berkasi rekam medik atau formulir lain terkait proses yang sedang dilakukan

c. Identifikasi pasien koma atau tanpa identitas dilakukan dengan cara:
   i. Penentuan identitasnya menggunakan simbol Tn/Mr. A atau Mrs/Ny. A dan bila jumlah pasiennya lebih dari satu orang, maka menggunakan simbol Tn/Ny. A1, B1, C1 dan seterusnya sampai dengan Z1, kemudian Tn/Ny. A2, B2, C2 dan seterusnya.
   ii. Bila pasien sudah sadar kembali dan/atau pasien sudah bisa diidentifikasi identitasnya, maka penggunaan simbol tersebut harus segera diganti dengan identitas asli pasien tersebut.

d. Identifikasi dilakukan oleh seluruh petugas di Rumah Sakit yang karena tanggung jawabnya harus melakukan hal-hal seperti pada poin di atas, misalnya dokter, perawat, petugas farmasi, petugas laboratorium, petugas radiologi, kasir, petugas pendaftaran, dll. Hal ini harus diwaspadai agar proses identifikasinya tetap dapat berjalan akurat pada setiap kondisi.

2. Kebijakan Pencatatan Transaksi dengan Benar

Saat melakukan pencatatan transaksi, perlu ketelitian dalam mencatatkan apa yang ditransaksikan. Karena kesalahan pencatatan dapat beresiko terjadi kesalahan pemberian pelayanan medis dan/atau obat yang membahayakan pasien. Untuk itu Rumah Sakit menetapkan kebijakan pencatatan transaksi dalam kaitannya dengan penanganan pasien dengan tujuan memastikan pencatatan data pelayanan medik dan obat dicatat dengan benar dan tidak terjadi kesalahan dan mampu diverifikasi dengan baik.

a. Pencatatan Transaksi yang dimaksud adalah:
   i. Pendaftaran pasien Rawat Inap, Rawat Jalan, UGD, ODS, dan Penunjang Medis di pendaftaran
   ii. Pencatatan transaksi pelayanan medis seperti visit dokter, konsultasi, tindakan, pemeriksaan, dll di poli, *nurse station*, dan kasir.
   iii. Pencatatan transaksi pemeriksaan dan tindakan di departemen penunjang medis oleh petugas departemen penunjang diagnosa.
   iv. Pencatatan resep online oleh dokter penanggung jawab pasien.
   v. Pencatatan transaksi obat/alat kesehatan di farmasi atau pun di ruang rawat.
   vi. Pencatatan jumlah hari rawat inap dan transaksi pemindahan atau pengeluaran pasien dari ruang rawat oleh perawat atau petugas administrasi.
   vii. Pencatatan transaksi pembayaran deposit dan pelunasan atau penagihan oleh petugas kasir.
   viii. Pencatatan order makanan/diet oleh perawat ruangan.
   ix. Pencatatan rujukan ke dokter spesialis lain atau order pemeriksaan ke departemen penunjang diagnosa oleh dokter, perawat atau petugas administrasi.
   x. Pencatatan data transaksi bedah di OK/VK oleh petugas OK/VK.
   xi. Pencatatan transfer pasien ke Rawat Inap, OK/VK, ICU, ODS.

b. Pencatatan transaksi yang benar meliputi:
   i. Pencatatan identitas pasien yang benar dengan proses identifikasi sesuai dengan poin 1.
   ii. Pengambilan ulang data pasien untuk transaksi lebih lanjut dengan mematuhi proses identifikasi sesuai poin 1.
   iii. Pencatatan pemeriksaan yang benar dengan memilih jenis pemeriksaan yang terdapat dalam daftar pilihan.
   iv. Pencatatan jumlah, satuan dan nominal transaksi dengan benar.
   v. Pencatatan transaksi obat/alat kesehatan dengan memilih dari daftar pilihan yang sesuai dengan nama obat/alat kesehatan, dosis atau sediaan, jumlah dan satuan.
   vi. Pencatatan transaksi pemeriksaan atau paket pemeriksaan yang tepat dengan memilih pemeriksaan dari daftar pilihan yang sesuai.

vii. Pencatatan hasil pemeriksaan yang benar dengan memperhatikan nilai hasil
viii. pemeriksaan dan satuan pemeriksaan.
ix. Pencatatan data workorder bedah dan detail data bedah dengan memilih dari
x. daftar pilihan dengan benar.
xi. Pencatatan pemindahan, pengeluaran atau pemulangan pasien dari ruang rawat dengan memperhatikan jumlah hari rawat, kondisi pasien, kelas rawat, dan laini-lain.
xii. Pencatatan rujukan yang benar dengan memperhatikan tujuan rujukan (ke dokter spesialis, penunjang diagnosa, rawat inap, ICU) dan pemeriksaan atau tindakan rujukan yang benar.
xiii. Pencatatan transaksi transfer pasien dari Rawat Jalan atau UGD ke Rawat Inap, ICU, OK/VK, ODS dengan memperhatikan departemen/ruang tujuan transfer, dokter penanggung jawab pasien, dll.

c. Pemilihan data transaksi yang benar dengan cara:
i. Saat melakukan penambahan data transaksi, terdapat pilihan pelayanan, pemeriksaan, obat/alkes atau tindakan yang sesuai dengan departemen kerja.
ii. Pemilihan dilakukan dengan tepat sesuai nama dan keterangan pengikut di nama pilihan, misalnya keterangan jenis sediaan obat.
iii. Jika transaksi yang dimaksud tidak tersedia di daftar pilihan, segera hubungi pihak terkait dalam hal ini staf IT.
iv. Memasukkan jumlah yang sesuai dengan satuan atau sediaan.
v. Memasukkan satuan transaksi.
vi. Memperhatikan nilai transaksi yang telah diatur secara *default* sesuai dengan kelas pelayanan . Jika nilai transaksi berbeda, harap segera mengklarifikasikannya ke pihak terkait dalam hal ini adalah staf IT RS.
vii. Dalam hal terjadi kesalahan pencatatan, petugas dapat mengisi formulir permohonan perubahan data yang disetujui koordinator/manajer terkait dan segera memberikan formulir tersebut ke staff IT untuk ditindaklanjuti.

3. Kebijakan Pencegahan Kebocoran Data Pasien

Saat bekerja, dokter atau petugas medis kadang kala harus meninggalkan tempat kerja untuk sebuah keperluan. Untuk menghindari bocornya data pasien kepada pihak lain yang tidak berhak yang kemudian berpotensi terhadap penyalahgunaan data tersebut atau potensi transaksi palsu, maka perlu dibuat kebijakan untuk pencegahan kebocoran data pasien.

a. Setiap komputer kerja harus memiliki proteksi password yang hanya diketahui oleh orang yang berhak.
b. Password tersebut berbeda antara satu komputer dengan komputer lain

dalam lingkungan rumah sakit.

c. Dilakukan penggantian password setiap bulan sekali oleh orang yang bertanggung jawab atas komputer tersebut.
d. Tidak memberikan password kepada orang lain yang tidak berhak.
e. Komputer diatur untuk memiliki penguncian otomatis ketika tidak ada aktivitas pada komputer tersebut selama lebih dari 5 menit. Penguncian otomatis ini dapat menggunakan fasilitas *screen saver* atau *desktop lock* yang telah tersedia di sistem operasi.
f. Ketika akan meninggalkan komputer kerja, petugas wajib *logout* dari sistem informasi RS. Atau melakukan penguncian desktop secara manual dengan fasilitas yang telah disebutkan di poin 3e.

4. Kebijakan Pencegahan Virus, Program Jahat dan Serangan Dari Luar

Komputer dan jaringan yang digunakan oleh petugas RS rentan terhadap infeksi virus komputer dan serangan dari program jahat atau pihak luar. Virus dan serangan ini selain dapat merusakkan data dan integritasnya juga berpotensi dalam pencurian data yang bisa digunakan oleh pihak lain untuk tujuan yang tidak benar. Untuk itu perlu dibuat kebijakan untuk pencegahan terhadap virus dan serangan dari program jahat atau pihak luar

a. Komputer kerja dalam lingkungan RS harus menggunakan sistem operasi yang aman dan kebal terhadap virus dan serangan dari luar. Jika tidak, maka perlu dipasang program tambahan untuk melindunginya seperti contohnya antivirus,*firewall*, dll.
b. Setiap komputer kerja perlu dilindungi oleh program antivirus yang sesuai dengan sistem operasinya.
c. Antivirus yang terpasang harus secara periodik melakukan update data definisi virusnya. Pengguna harus memastikan bahwa proses update data antivirusnya berhasil dengan baik sehingga selalu terkini.
d. Setiap komputer kerja perlu dilindungi oleh Firewall untuk membatasi akses dari luar sehingga sistem aman dari serangan dari luar. Dalam hal sistem operasi belum memiliki fitur *firewall*, maka perlu dipasang program *firewall* secara terpisah.
e. Setiap komputer kerja yang terpasang fasilitas akses jarak jauh perlu dilindungi dengan password untuk mengaksesnya. Password akses jarak jauh ini hanya boleh diketahui oleh orang yang berhak. Password ini harus diganti secara periodik, misalnya sebulan sekali.
f. Setiap kali diperlukan penyalinan file (data atau dokumen) dari pihak luar perlu dilakukan pemeriksaan (scan) dengan antivirus untuk memastikan bahwa file tersebut tidak mengandung virus dan program jahat (*malware*).
g. Tidak diperkenankan memasang program atau sistem informasi dari pihak luar sebelum mendapat ijin dari direktur dan telah diteliti potensi terjadinya masalah oleh departemen IT.

5. Kebijakan Pengiriman Data Elektronik Pasien Kepada Pihak Lain

Dalam menunjang kualitas pelayanan medis kepada pasien, proses konsul *(second opinion)* mau pun rujukan data pasien antar Rumah Sakit dapat terjadi dan tidak menutup kemungkinan terjadi pengiriman data medis pasien dalam bentuk elektronik. Namun dalam pengiriman data ke pihak luar ini, data pasien dapat disadap, salah kirim, atau salah terima yang kemudian berpotensi terhadap bocornya data pasien dan dapat terjadi penyalahgunaan data pasien. Untuk itu perlu adanya kebijakan dalam pengiriman data medis pasien kepada pihak lain.

a. Dalam pengiriman data medik pasien dalam format elektronik via email perlu
   dipastikan kebenaran alamat email tujuan. Alamat tujuan harus valid.
b. Data medik pasien harus dienkripsi (disandikan) dan dilindungi oleh password untuk
   membukanya.
c. Kode enkripsi dan password diberikan kepada pihak tujuan dengan media lain, misalnya via sms. Kode enkripsi dan password ini hanya diberikan kepada pihak yang berhak/tujuan dan pastikan supaya tidak bocor atau tersebar ke pihak lain yang tidak berhak.

6. Kebijakan Pembuatan Password

Walau pun data telah dienkripsi dan dilindungi password, namun jika password tersebut mudah ditebak oleh orang lain, maka perlindungan menjadi tidak efektif. Untuk itu diperlukan kebijakan pembuatan password di lingkungan kerja Rumah Sakit.

a. Panjang minimal password adalah 6 karakter.
b. Password merupakan kombinasi dari karakter dan nomor.
c. Password yang dipilih bukanlah kombinasi yang mudah ditebak seperti abcdef, 123456, qwerty, dll.
d. Password yang dipilih bukan bagian dari nama pengguna atau salah satu anggota keluarganya.
e. Password yang dipilih bukan merupakan kombinasi tanggal lahir pemegang password atau salah satu anggota keluarganya.
f. Password yang dipilih bukan merupakan merek atau nama produk yang umum dikenal atau yang digunakan oleh pengguna.
g. Perlu dilakukan penggantian password secara periodik minimal setiap 2 bulan.
h. Password yang telah dibuat dapat dicatat pada catatan yang aman dan tidak
   mudah ditemukan oleh orang lain, misalnya di dalam passbook.

7. Kebijakan Pemberian Hak Akses Program dan Data

Sistem Informasi Rumah Sakit yang digunakan harus mengakomodasi pemberian dan pembatasan hak akses kepada pengguna yang tepat. Kebijakan ini berguna untuk mencegah akses oleh pihak yang tidak berhak dan untuk mengurangi tingkat kesalahan pencatatan atau terjadinya penyalahgunaan program/data.

a. Setiap pengguna sistem dalam lingkungan Rumah Sakit dikelompokkan dalam group akses sistem. Contohnya adalah group akses Pendaftaran, Pembayaran, Perawat, Gizi, Laboratorium, dll.
b. Setiap group akses memiliki hak akses terhadap program tertentu yang sesuai dengan kerjanya.
c. Sebuah group akses tidak bisa mengakses program lain di luar hak aksesnya.
d. Sebuah group akses selain dibatasi program yang dapat diaksesnya juga dibatasi akses ke departemen hanya kepada departemen kerjanya saja.
e. Dalam hal dibutuhkan group akses yang spesifik hak aksesnya, maka bisa dibuatkan group akses baru dengan kemampuan akses program yang sesuai.

8. Kebijakan Pemberian Akses Data dan Program Kepada Pihak Lain

Untuk sebuah keperluan khusus, mungkin diperlukan pemberian hak akses terhadap data atau sistem informasi Rumah Sakit kepada pihak lain. Untuk mencegah terjadinya hak akses di luar kewenangan atau pun kebocoran data dan program sehingga berpotensi terhadap penyalahgunaan data atau program dan potensi perusakan data atau sistem informasi, maka perlu dibuat kebijakan untuk pemberian akses data dan program kepada pihak lain.

a. Pemberian hak akses terhadap data atau sistem informasi kepada pihak lain harus melalui persetujuan resmi dari direktur dengan mengisi formulir pemberian hak akses.
b. Pada formulir pemberian hak akses data atau sistem informasi harus lengkap berisi nama orang yang diberi hak akses, nomer telepon, alamat, email dll.
c. Formulir ini dilengkapi dengan fotokopi kartu identitas yang berlaku.
d. Formulir ini mencakup lama waktu pemberian hak akses yang diberikan
e. Formulir ini mencantumkan perjanjian kesepakatan perahasiaan data dan sistem informasi dan password sehingga jika terjadi penyalahgunaan data atau program oleh orang tersebut dapat segera diproses ke bidang hukum.
f. Formulir didisposisi kepada koordinator IT yang kemudian akan memberikan hak akses kepada orang tersebut.
g. Segala penyalahgunaan hak akses yang dilakukan oleh pihak lain harus segera diproses ke hukum.

KEBIJAKAN KHUSUS

Kebijakan khusus dimaksudkan untuk departemen IT yang akan memastikan bahwa data tersimpan dengan aman dan kebal terhadap serangan virus atau pihak luar.

1. **Kebijakan Perlindungan Server**

   Dalam operasionalnya, sistem informasi rumah sakit dijalankan di sebuah server atau group server yang harus dilindungi dari virus, program jahat (malware) dan serangan dari luar. Mengingat begitu pentingnya peran server (atau group server) ini, maka diperlukan kebijakan untuk melindungi server tersebut.

   a. Setiap server dilindungi oleh password yang secara periodik diganti.
   b. Password hanya diketahui oleh orang yang berhak. Pemberian password dapat dilakukan secara berjenjang sesuai tingkatan akses orang tersebut, misalnya untuk system administrator, database administrator, network administrator, email administrator, dll.
   c. Dilakukan pembatasan hak akses dari jarak jauh (dari luar RS) kepada orang yang berhak saja.
   d. Server memiliki duplikat (mirror) yang setiap saat dapat diaktifkan untuk menggantikan peran server utama jika terjadi kerusakan.
   e. Server memiliki fitur perlindungan yang dibutuhkan seperti firewall, antivirus, antimalware, intruder detection, dan lain-lain.
   f. Server harus selalu memiliki sub sistem yang terkini. Update harus segera dilakukan jika ada update yang tersedia oleh pembuat sistem.
   g. Pemberian hak akses kepada pihak lain hanya bisa dilakukan melalui persetujuan Direktur dengan formulir pemberian hak akses. Pemberian hak akses kepada pihak lain memiliki durasi waktu yang mana jika durasi tercapai harus segera dinonaktifkan.
   h. Server harus menggunakan jalur komunikasi jaringan yang aman dan handal dari sadapan, gangguan atau perusakan.

2. **Kebijakan Backup Database**

   Data transaksi dan medik pasien tersimpan dalam database server (atau kelompok server) sangat penting dalam operasional pelayanan medis Rumah Sakit sehingga perlu dilakukan backup database untuk mencegah dan menanggulangi jika terdapat kerusakan database.

   a. Backup database dilakukan minimal dalam 2 bentuk, yaitu backup file dan replikasi.
   b. Backup file database dijalankan secara otomatis oleh server setiap hari dalam jam tertentu di media penyimpanan yang terpisah dari server utama, misalnya di server backup (mirror) yang tersimpan di ruang/gedung terpisah.
   c. Staff IT secara manual menyimpan backup harian otomatis tersebut dalam media penyimpanan lain, misalnya CD/DVD, tape backup atau flashdisk/*solid state storage*.

d. Media penyimpanan lain tersebut harus disimpan di sebuah *safety box* yang tahan
   api dan memiliki kunci yang hanya dipegang oleh koordinator IT.
   Database server harus memiliki minimal 1 server replikasi yang secara real time akan menduplikasi perubahan data yang terjadi di server utama. Server replikasi harus disimpan di ruang/gedung terpisah dari server utama.

3. Kebijakan Penanggulangan Kerusakan Server

Dalam suatu ketika bisa terjadi kerusakan server yang mengakibatkan gangguan pelayanan medik di Rumah Sakit. Untuk itu diperlukan kebijakan penanggulangan kerusakan server.

a. Ketika terjadi kerusakan server, maka diperlukan kepimpinan koordinator/manajer IT untuk memimpin proses penanggulangan. Dalam hal koordinator/manajer IT berhalangan, maka kepimpinan dapat dipegang oleh staff senior.
b. Pemimpin penanggulangan mengumumkan terjadinya kerusakan server kepada para manajer RS.
c. Pemimpin penanggulangan mengidentifikasi masalah yang terjadi.
d. Pemimpin penanggulangan merencanakan tindakan perbaikan dan mengalokasikan sumber daya yang diperlukan.
e. Pemimpin penanggulangan memutuskan untuk memperbaiki server yang rusak atau menggunakan server cadangan (mirror atau replikasi). Memperbaiki server utama yang rusak bisa dipilih jika perbaikan yang diperlukan tidak lebih dari 2 jam.Jika opsi ini yang dipilih, maka diperlukan koordinasi dengan para manajer RS untuk penggunaan sistem manual.
f. Sistem Informasi dan database yang digunakan dipilih menggunakan posisi yang terkini, bisa dari backup file atau replikasi.
g. Ketika server utama telah diperbaiki atau jika server mirror/replikasi mengambil alih tugas server utama telah aktif, maka pemimpin penanggulangan mengumumkan ketersediaan sistem kepada para manajer Rumah Sakit. Pemimpin penanggulangan mencatat kejadian kerusakan server dan langkah penanggulangannya di berita acara.
h. Dalam hal tidak dapat ditanganinya penanggulangan kerusakan ini oleh sumber daya internal rumah sakit, maka pemimpin dapat meminta bantuan pihak luar dengan sebuah kontrak kerja sama.

DIREKTUR Rumah Sakit Khusus Ginjal NY. R.A. Habibie

dr. Qania Mufliani, MM