Universitas Esa Unggul

Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

PERTEMUAN-13

Dr. HOSIZAH, SKM, M.KM
PRODI MIK | FAKULTAS ILMU-ILMU KESEHATAN

RELIABILITAS, SEKURITAS DAN PRIVASI DALAM RKE

- Sistem Keandalan, Privasi & Keamanan merupakan standar sistem informasi, hal ini seharusnya tidak menyebabkan pentingnya mereka untuk disalahartikan, melainkan harus mencerminkan sifat dasar dan lintas fungsionalnya.
- Keandalan & Keamanan berhubungan dengan semua aspek fungsi sistem EHR, mulai dari kebijakan & prosedur yang menangani kerahasiaan dan integritas data dari hardware & software yang melindungi data dari bahaya dan memastikan kinerja sistem.

RELIABILITAS

- Dalam sistem komputer, keandalan mengacu pada kemampuan suatu sistem untuk menjalankan fungsinya tanpa kesalahan, gagal, atau masalah kinerja. Kesalahan terjadi karena masalah sistem kinerja atau kurangnya keamanan sistem.
- Masalah sistem kinerja mungkin melebihi hasil dari data dan di luar kemampuan, pemeliharaan yang buruk, kerusakan fisik (seperti seseorang menjatuhkan seluruh komputer atau sengaja memotong kabel), atau kesulitan teknis lainnya.

RELIABILITAS

- Kesalahan sangat penting dalam kesehatan karena tidak hanya dapat menghasilkan biaya tambahan (dalam hal koreksi atau kewajiban), tetapi juga dalam kematian pasien tidak selalu dapat diidentifikasi secara terus – menerus.
- Sistem pemantauan memeriksa kesalahan dan meninjau output kegiatan penting dalam mengidentifikasi dan melacak penyebab kesalahan

KEGAGALAN

- Kegagalan disebabkan oleh banyak masalah sistem kinerja atau pelanggaran masalah keamanan adalah bahwa kesalahan, tetapi bukan menghasilkan kesalahan, melainkan menyebabkan sistem untuk berhenti berfungsi sama sekali

MASALAH KINERJA

- Masalah kinerja dihasilkan oleh banyak peristiwa yang menyebakan kesalahan dan kegagalan, tetapi lebih cenderung mengalami gangguan, seperti proses repon yang lambat dalam entry data atau retrivel.
- Masalah kinerja juga dapat dikaitkan dengan ketidakcukupan dan ukuran sistem. Monitoring sistem harus mengidentifikasi kapan volume dan jumlah transaksi mulai terlalu banyak untuk kapasitas sistem.

PRIVASI DAN KEAMANAN

- Meskipun kesehatan selalu peduli dengan privasi pasien dan kerahasiaan informasi kesehatan, tetapi belum ada standar nasional HIPAA untuk memastikan perlindungan privasi yang sama diantara penyedia atau dasar keamana untuk kerahasiaan, integritas data dan ketersediaan data.
- ARRA/HITECH yang disahkan oleh kongres tahun 2009, menyerukan memperbaharui privasi HIPAA, kemanan dan penegakkan aturan.

PRIVASI DAN KEAMANAN

- Aturan privasi membahas penggunaan dan pengungkapan informasi yang dilindungi kesehatan (PHI) termasuk peggunaaan dan pengungkapan yang diperlukan.
- Pada aturan Omnibus, bagaimanapun memang membuat perubahan penggunaan dan pengungkapan informasi genetik (yang tidak boleh digunakan untuk tujuan yang dapat menimbulkan kerugian).

PRIVASI DAN KEAMANAN

- Aturan privasi HIPAA membahas hak individu untuk PHI, termasuk hak untuk memberitahukan dari praktik privasi, akses ke informasi kesehatan, dan hak untuk meminta amandeme, pembatasan dan komunikasi rahasia. Persyaratan memerlukan entitas tercakup dalam HIPAA untuk mengurangi efek berbahaya dari peggunaan pelanggaran, dan memiliki kebijakan, prosedur dan dokumentasi untuk mendukung kepatuhan.

PRIVASI DAN KEAMANAN

- Aturan privasi juga memiliki standar administrasi yang memerlukan penunjukan pejabat privasi (PO) yang dikenal sebagai petugas privasi, penyediaan pelatihan penanganan keluhan, dan penangan keluhan, dan penerapan sanksi yang sesuai terhadap anggota angkatan kerja yang gagal mematuhi persyaratan privasi.
- Perubahan signifikan yang ditegaskan oleh aturan Omnibus adalah membuat bisnis bertanggung jawab langsung pada aturan keamanan dan komponen tertentu dari aturan privasi.

PRIVASI DAN KEAMANAN

Komponen ini meliputi :

1. Penggunaan yang tidak diizinkan
2. Gagal memberikan pemberitahuan pelanggaran
3. Kegagalan untuk memberikan akses ke salinan elektronik PHI untuk entitas tertutup atau individu yang ditunjuk
4. Kegagalan untuk mengungkapkan PHI jika diminta oleh HHS, untuk menyelidiki yang bermasalah dalam HIPAA.
5. Kegagalan dalam memberikan pemberitahuan akutansi

PERATURAN SEKURITAS (KEAMANAN)

- Aturan Kemanan HIPAA bertanggung jawab termasuk standar untuk administrasi, fisik, dan teknis pengamanan, serta persyaratan u.ntuk kebijakan, prosedur, dan dokumentasi. Aturan Keamanan HIPAA berbasis risiko, berarti standar memberikan persyaratan umum untuk perlindungan keamanan, tetapi organisasi harus memutuskan, melalui analisis risiko apa dan kontrol tertentu yang mampu mereka lindungi.

PERATURAN SEKURITAS (KEAMANAN)

- Analisis risiko adalah sebuah proses dimana organisasi menganalisis kerentanan atau kelemahan dalam kontrol keamanan dan ancaman yang mungkin mengeksploitasi mereka untuk semua lokasi dimana PHI disimpan, diterima, dipelihara atau dikirimkan.
- OCR telah mengeluarkan panduan tentang persyaratan analisis risiko di bawah kekuasaan keamanan HIPAA (2010).

KONTROL KEAMANAN

- Pada tahun 2007, CMS dimulai dengan keamanan HIPAA proaktif investigasi di lokasi dan ulasan pengujian.
- Tinjauan pertama dilakukan di RS Piedmont Atlanta (Vijayan, 2007) dan mereka bersedia untuk berbagai pertanyaan pers yang diajukan kepada meraka selama peninjauan.

KONTROL KEAMANAN

Uji komprehensif, review komprehensif dan termasuk pendekatan berlapis yang disepakati ahli sangatlah penting

- Dalam pendekatan berlapis ada sebuah sistem keamanan menyeluruh
- Pendekatan berlapis untuk keaman juga mengacu pada struktur logis dan fisik dari kontrol yang dilaksanakan

CONTOH

- HIPAA, termasuk spesifikasi implementasi relatif untuk enskripsi data pada saat keadaan tenang dan untuk transmisi keamanan.
- Tanggung jawab untuk keamanan adalah bagian dari pekerjaan setiap orang tetapi organisasi juga perlu menunjuk ISO untuk memberikan pengawas
- Pengguna telah benar-benar terlatih pada keamanan dan mengingatnya secara terus-menerus