RAKONTEK SIK REGIONAL III 2017

Tanggal Publikasi : SENIN, 06 MARET 2017 00:00:00, Dibaca : 877 Kali

Batam, 23 Februari 2017 Sebagai bagian dari rangkaian pertemuan Rapat Konsolidasi Teknis Sistem Informasi Kesehatan (Rakontek SIK) 2017, Pusat Data dan Informasi menyelenggarakan Rakontek SIK Regional III di Kota Batam, Kepulauan Riau, pada tanggal 20-23 Februari 2017. Kegiatan ini dihadiri oleh 360 peserta yang berasal dari 15 provinsi dan 266 kabupaten/kota di Jawa dan Sumatera serta Kementerian Kesehatan.

Sistem Informasi Kesehatan Indonesia saat ini masih jauh dari kondisi ideal. Berbagai masalah masih dihadapi dalam pengelolaan sistem informasi kesehatan, di antaranya

adalah adanya *overlapping* dalam pengumpulan dan pengolahan data kesehatan sehingga masih terjadi pengumpulan data berulang yang memungkinkan terjadinya duplikasi data. Untuk menerapkan informasi satu pintu *(one data)* perlu dilakukan integrasi dari beberapa aplikasi yang saat ini ada. Pusat Data dan Informasi beberapa tahun ini telah mengenalkan *Health Information Exchange (HIE)* atau pertukaran informasi kesehatan. Harapannya, pada aplikasi-aplikasi yang ada di Kementerian Kesehatan, tidak terjadi tumpang tindih variabel atau indikator yang dikumpulkan. Oleh karena itu, perlu dilakukan konsolidasi terhadap sesama unit di Kementerian Kesehatan dan dengan daerah.

Secara umum, pertemuan ini bertujuan untuk melakukan koordinasi dan sinkronisasi serta harmonisasi perencanaan dan penyelenggaraan sistem informasi kesehatan baik dengan lintas unit utama maupun daerah. Namun, pada pertemuan ini dilakukan pula (1) sosialisasi terhadap beberapa kebijakan dan regulasi terkait sistem informasi yang dapat digunakan oleh daerah sebagai acuan, (2) berbagi ilmu dan pengalaman oleh petugas SIK antar daerah, (3) pengumpulan data kesehatan, (4) identifikasi permasalahan penerapan SIK di daerah, serta (5) pemberian saran/masukan terhadap penyelenggaraan SIK saat ini.

Materi pertemuan tidak hanya disampaikan oleh narasumber dari Kementerian Kesehatan, namun juga dari Lembaga Sandi Negara. Dari Kementerian Kesehatan, materi mencakup penyelenggaraan SIK, pengelolaan data dan informasi serta pengalokasian anggaran untuk mendukung penyelenggaraan SIK di daerah. Sementara, materi yang disampaikan oleh Lembaga Sandi Negara adalah yang terkait dengan keamanan informasi di era siber.

Sebagian besar pengelola data masih terfokuskan pada bagaimana data bisa dicatat dan dilaporkan sehingga informasi yang akuntabel dan tepat waktu dapat dihasilkan. Padahal, bagaimana cara menjaga keamanan agar data dan informasi tersebut juga tidak kalah penting. Di era siber dengan situasi TI yang terus berkembang ini, ada banyak kemungkinan dan peluang dilakukannya pembocoran keamanan data dan informasi. Sebagai lembaga pemerintah yang utamanya bertugas mengamankan dokumen rahasian negara, Lembaga Sandi Negara memiliki salah satu fungsi melindungi informasi publik, dan informasi kesehatan merupakan salah satu informasi publik yang harus dilindungi karena di *black marke*t data kesehatan bisa dihargai 10 kali lipat lebih mahal dari data kartu kredit.

Ada beberapa cara untuk melakukan pengamanan terhadap data dan informasi yang kita miliki. Cara pertama adalah dengan menggunakan password. Namun, karena umumnya *password* merupakan pengamanan yang paling banyak digunakan, maka *password* ini lah yang paling banyak dijadikan incaran untuk diretas. Selanjutnya, dilakukan *double password* atau *password* ganda, yaitu pin dan sidik jari. Sebagai upaya pengamanan situs, digunakan *software* keamanan SSL (dapat dilihat dari penggunaan url yang diawali dengan https). Sayangnya, *software* ini masih kita sewa dari Amerika, sehingga setiap tahun kita harus mengeluarkan biaya untuk melakukan upaya pengamanan.

Sejalan dengan semakin banyaknya pemanfaatan dan penggunakan internet digunakan dalam transaksi data dan informasi, otentifikasi elektronik sangat dibutuhkan, yaitu berupa tanda tangan digital dan sertifikat elektronik. Tanda tangan digital adalah data yang dienkripsi dan hanya dapat dibuka dengan menggunakan token. Transaksi elektronik dapat diamankan dengan dilakukan enkripsi data dan menyeting server pengirim dan penerima sehingga hanya server penerima yang dapat mengenali dan membuka data yang dikirim oleh server pengirim. Sementara sertifikat elektronik adalah identitas yang digunakan dalam kerja sama antar negara.

Pengamanan informasi dapat dimulai dari rutinitas harian dengan melakukan pengamanan dokumen, yaitu saat akan men-*copy* atau memindahkan data dari media yang bukan milik kita, pastikan bahwa *flashdisc* yang digunakan tidak berisi data penting, lebih baik lagi bila *flashdisc* dalam keadaan kosong.

Dengan kata lain, perkembangan serta pemanfaatan teknologi dan informasi tidak dapat ditahan dan dihalangi. Yang perlu dilakukan adalah melakukan pengamanan yang kuat pada jaringan, aplikasi dan informasi yang ada. Sama halnya dengan serangan terhadap sistem/aplikasi yang tidak bisa dihindarkan, yang terpenting adalah bagaimana kita mengamankan data dan sistem kita.

Berita ini dipublikasikan oleh Tim Web Pusat Data dan Informasi, Kementerian Kesehatan RI.