MODUL CLOUD PERTEMUAN 11 DAN 12

SYEFIRA SALSABILA, S.GZ, MKM

"HEALTH CARE DATA SECURITY"

Penggunaan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang potensial seperti meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan pembacaan ketersediaan fasilitas dan aksesibilitas informasi. Namun demikian, ancaman terhadap keamanan Sistem Informasi Kesehatan juga meningkat secara signifikan.

Pada dasarnya, ancaman dan tindakan yang disengaja dapat sangat merusak sistem informasi kesehatan dan akibatnya dapat mencegah profesional untuk menggunakannya di kemudian hari2. Selain itu, kurangnya perlindungan yang memadai dalam menopang aspek kerahasiaan, integritas dan ketersediaan untuk investigasi juga menjadi ancaman, terutama di domain sistem informasi kesehatan.Hal ini memerlukan pengelolaan lebih dalam keamanan informasi serta perhatian khusus dari sektor publik dan swasta.

Keamanan sistem informasi adalah segala betuk mekanisme yang harus dijalankan dalam sebuah sistem yang ditujukan agar sistem tersebut terhindar dari segala ancaman yang membahayakan keamanan data informasi dan keamanan pelaku sistem3. Ancaman mencakup berbagai jenis perilaku karyawan seperti keridaktahuan karyawan, kecerobohan, mengambil sandi karyawan lain dan memberikan *password* untuk karyawan lain. Untuk ancaman eksternal, yaitu virus dan serangan *spyware*, *hacker* dan penyusup di tempat. Selain itu, telah dikategorikan ancaman sistem informasi rumah sakit berdasarkan studi kasus dilakukan dengan menggunakan risiko yang dipilih dalam metode analisis.

Dengan melihat beberapa aspek yang menjadi ancaman bagi keamanan sistem infomasi kesehatan yang disampaikan dalam makalah-makalah yang ditinjau, beberapa hal yang perlu diperhatikan oleh pengelola sitem informasi yaitu:

1. Melakukan perlindungan yang memadai dalam menopang aspek kerahasiaan, integritas dan ketersediaan untuk investigasi. Penyelidikan lebih lanjut untuk mengidentifikasi ancaman keamanan di kesehatan sistem informasi.
2. Melakukan perlindungan yang menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman
3. Melakukan analisis resiko keamanan untuk melindungi aset informasi menjamin keamanan sistem informasi.

Cloud computing presents a new model for improving the delivery of healthcare and increasing the business flexibility of medical organizations, enabling them to operate with greater efficiency, cost-effectiveness, and agility. Use of cloud services has taken off across countless industries. Adoption of cloud computing in healthcare has taken place a little more tentatively, as providers sort out how they can benefit from cloud offerings and how much of their operations they can afford to transfer to the cloud. electronic health record (EHR), analytics and imaging systems are a few areas in which healthcare providers have found success with cloud deployments.

Information Technology plays a strong role in the health and patient care arenas with cloud computing slowly beginning to make its mark. However, despite the significant advantages for the utilization of cloud computing as part of Healthcare IT (HIT), security and privacy, reliability, integration and data portability are some of the significant challenges and barriers to implementation that are responsible for its slow adoption

Cost, efficiency and effectiveness create ongoing complexity for the health care industry. The latest new technology will fix or mitigate these problems, for the benefit of the health care system, individual patients and those paying for health care. But the regulatory system is getting in the way of this technology making this all work. If we could just let the technology work, everything would be well.

First, it was the Health Insurance Portability and Accountability Act (HIPAA) “standard transactions” rule. This idea streamlined, uniform electronic transactions, fitting all

shapes and sizes in the health care industry would create enormous efficiencies and ease transaction costs.

The latest technological opportunity comes through the use of cloud computing. As the concept of cloud computing has rapidly moved onto the scene, businesses across all industries have moved swiftly (and some would argue recklessly) to take advantage of "the cloud," often without fully realizing the hidden risks associated with this movement because of the immediate lure of visible cost savings. The health care industry (as it often is) has been slow to take advantage of the technological opportunities presented by the cloud, but the issues with cloud computing go deeper than this general technological reluctance.

Benefits of Cloud Computing for Healthcare: "Patient centricity" has become the key trend in healthcare provisioning and is leading to the steady growth in adoption of electronic medical records (EMR), electronic health records (EHR), personal health records (PHR), and technologies related to integrated care, patient safety, point-of-care access to demographic and clinical information, and clinical decision support. Availability of data, irrespective of the location of the patient and the clinician, has become the key to both patient satisfaction and improved clinical outcomes. Cloud technologies can significantly facilitate this trend.

Cloud computing offers significant benefits to the healthcare sector: doctor's clinics, hospitals, and health clinics require quick access to computing and large storage facilities which are not provided in the traditional settings. Moreover, healthcare data needs to be shared across various settings and geographies which further burden the healthcare provider and the patient causing significant delay in treatment and loss of time. Cloud caters to all these requirements thus providing the healthcare organizations an incredible opportunity to improve services to their customers, the patients, to share information more easily than ever before, and improve operational efficiency at the same time.

Privacy and Security Challenges: Data maintained in a cloud may contain personal, private or confidential information such as healthcare related information that requires the proper safeguards to prevent disclosure, compromise or misuse. Globally, concerns related to data jurisdiction, security, privacy and compliance are impacting adoption by healthcare organizations.

Data Security and Availability: Related to security is an important challenge the idea of “availability” of the data. Healthcare providers need access to patient data all the time, immediately and reliably. While the cloud often provides this, there remain concerns about accessibility of data on an automatic basis, with consistent reliability. And, where healthcare providers are concerned about this reliability, they either will refuse to use the cloud or will find a need to build redundant systems, thereby reducing or eliminating the cost benefits of the cloud.

OWASP Top 10

Software yang tidak aman telah mengancam infrastruktur keuangan, kesehatan, pertahanan, energi, dan infrastruktur kritikal lainnya. Dengan semakin kompleks dan terhubungnya infrastruktur digital kita, kesulitan mencapai keamanan aplikasi meningkat secara eksponensial. Kita tidak dapat lagi mentoleransi masalah keamanan sederhana seperti yang ditampilkan dalam OWASP Top 10.

OWASP Top 10 merupakan sebuah panduan bagi para developers dan security team mengenai kelemahan-kelemahan pada web apps yang rentan diserang dan harus segera disiasati. Berbagai kelemahan ini memudahkan penyusup untuk menanamkan malware, mencuri data, atau mengambil alih sepenuhnya situs atau komputer Anda.