MODUL III

Konsep Keamanan, Kepatuhan dan Identitas

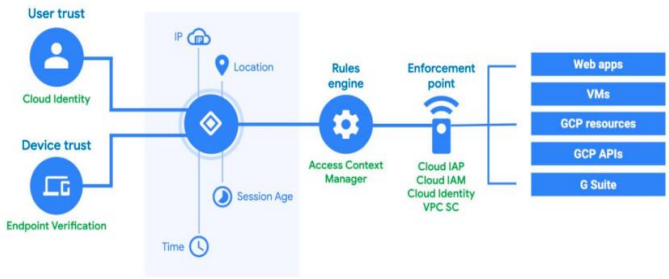
3.1.Konsep Dasar Keamanan, Kepatuhan dan Identitas

Sebuah organisasi perlu memahami bagaimana tindakan yang paling tepat untuk melindungi data yang dimiliki, bukan hanya sekedar berpikir bagaimana agar data yang ada dapat di proses, diakses, keberadaan data apakah di komputasi awan ataukah bukan. Selain itu, perlu memahami konsep dan metodologi keamanan seperti model *Zero Trust*, model tanggung jawab bersama, dan proses pertahanan yang mendalam karena perlu memahami kerangka kerja adopsi komputasi awan untuk memandu adopsi yang tersedia.

Konsep Dasar Keamanan, Kepatuhan dan Identitas

3.1.1. Metodologi Zero - Trust

Zero trust mengasumsikan bahwa semua komponen yang tersedia berada dalam sebuah jaringan yang terbuka dan beroperasi berdasarkan prinsip “tidak percaya siapapun, namun memverifikasi semuanya”. Kemampuan seorang penyerang dalam melewati kontrol akses yang sifatnya konvensional yaitu dengan tidak mempercayai integritas jaringan sebuah perusahaan sehingga pastinya keamanan akan diperkuat. Namun, dalam pengoperasiannya tidak ada yang berasumsi bahwa keamanan dengan kata sandi sudah cukup dalam memvalidasi akun pengguna tetapi dengan menambahkan otentifikasi multifaktor untuk memberikan pemeriksaan tambahan. Sehingga pengguna hanya diizinkan mengakses aplikasi atau data tertentu yang dibutuhkan.



Context-aware access high-level architecture

Metodologi Zero - Trust

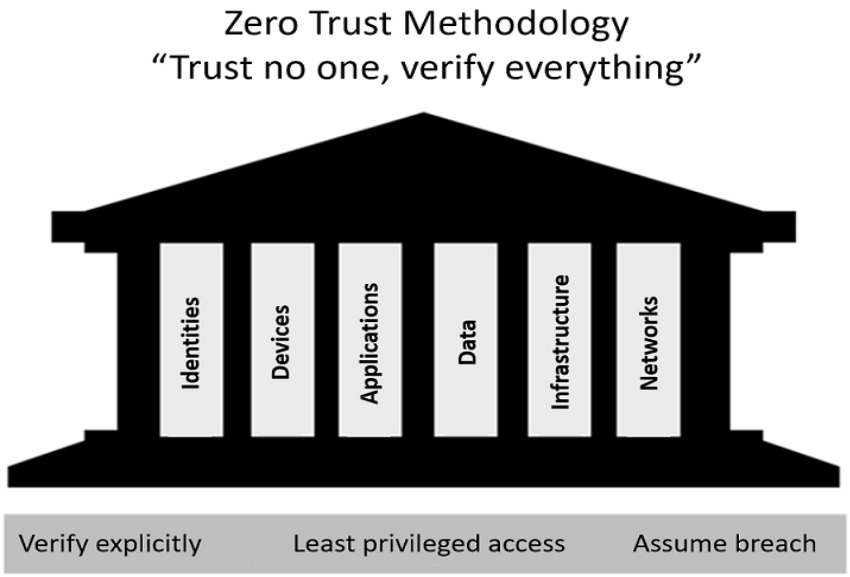
Ada sebuah model dikenal dengan istilah pendekatan tanpa kepercayaan yang digunakan untuk memverifikasi permintaan secara eksplisit menggunakan semua sinyal yang tersedia dan menggunakan prinsip akses hak istimewa paling rendah. Pendekatan tersebut berfungsi sebagai filosofi keamanan yang terintegrasi pada enam pilar dasar, yaitu :

1. Identitas, memverifikasikan semua identitas dengan otentikasi yang kuat.
2. Perangkat, mendapatkan visibilitas ke semua perangkat yang mengakses ke sebuah jaringan.
3. Aplikasi, menemukan bayangan IT dan memantau serta mengontrol akses secara analitik terhadap waktu.
4. Jaringan, mengenkripsi semua komunikasi internal yang membatasi akses dengan kebijakan serta jaringan segmen.
5. Infrastruktur, mendeteksi ancaman terhadap waktu dan secara otomatis memblokir dan menandai risiko serta mempekerjakan akses prinsip hak istimewa.
6. Data, mengklasifikasikan serta mengenkripsi data untuk menjaga privasi.

Model zero trust memiliki tiga prinsip yang dapat memandu dan mendukung penerapan keamanan, seperti verifikasi secara eksplisit yang selalu mengautentifikasi dan mengotorisasi berdasarkan titik data yang tersedia seperti identitas pengguna, lokasi, perangkat, layanan atau beban kerja, serta mengklasifikasi suatu data. Prinsip berikutnya yaitu proses akses dengan hak istimewa rendah, artinya batas akses pengguna dengan waktu yang cukup cepat, kebijakan adaptif yang berisiko, dan melindungi data secara produktivitas. Prinsip yang terakhir yaitu mengasumsikan pelanggaran, artinya melakukan segmentasi akses berdasarkan jaringan, pengguna, perangkat dan aplikasi. Penggunaan enkripsi diperlukan untuk melindungi data dan menggunakan analitik ketika ingin mendapatkan visibilitas serta mendeteksi ancaman serta proses untuk meningkatkan kualitas keamanannya. Dalam model zero trust terdapat elemen yang saling bekerja sama untuk memberikan keamanan dari awal hingga akhir. Elemen yang dimaksud terdiri dari :

1. Identifikasi, berupa pengguna, layanan atau perangkat. Apabila suatu identitas pengguna mengakses sumber daya tertentu pastinya memerlukan verifikasi dengan otentifikasi yang kuat serta mengikuti prinsip – prinsip akses hak istimewa.
2. Perangkat, membuat permukaan penyerangan yang sangat besar dengan cara proses data yang mengalir dari suatu perangkat ke beban kerja lokal dan komputasi awan. Pemantauan yang dilakukan di suatu perangkat akan digunakan untuk proses kepatuhan sebagai salah satu aspek keamanan.
3. Aplikasi, menemukan semua aplikasi yang digunakan atau disebut *Shadow IT* karena tidak semua aplikasi dapat dikelola secara terpusat sehingga pillar ini hanya mencakup beberapa pengelolaan izin dan akses.

4. Klasifikasi Data, memberi label dan enkripsi berdasarkan atribut. Upaya keamanan yang dapat terlaksana seperti melindungi data, memastikan perangkat telah di nonaktifkan, memastikan data tetap aman saat meninggalkan perangkat.
5. Infrastruktur, meningkatkan keamanan dalam menilai versi, konfigurasi serta akses mendeteksi serangan dan anomali. Sehingga memungkinkan terjadinya pemblokiran otomatis atau menandai perilaku yang berisiko dan tetap mengambil tindakan perlindungan.
6. Jaringan tersegmentasi, berupa segmentasi yang terdiri dari segmentasi mikro dalam jaringan dengan perlindungan ancaman waktu secara utuh, enkripsi . Selain itu, perlindungan ancaman dibutuhkan dari proses awal hingga ke proses tahap selanjutnya untuk melakukan pemantauan.



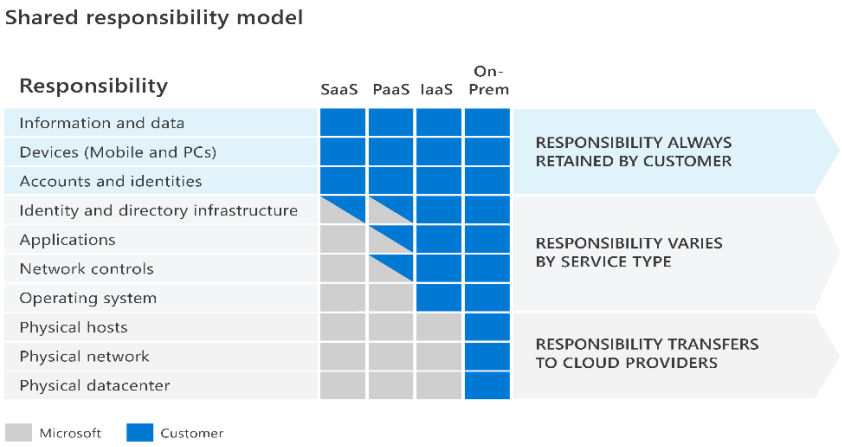
Metodologi Zero - Trust

Keenam pilar dasar tersebut bekerja sama dengan model Zero Trust dalam menegakkan kebijakan keamanan organisasi di dunia Internet.

3.1.2. Model Tanggung Jawab Bersama

Model ini dapat melakukan pengidentifikasian tugas keamanan yang dikerjakan oleh penyedia komputasi awan dan para pengguna. Ketika sebuah organisasi menggunakan perangkat keras dan lunak maka organisasi tersebut perlu bertanggung jawab untuk menerapkan keamanan dan kepatuhan secara 100% penuh. Dengan bantuan layanan yang berbasis komputasi awan, maka tanggung jawab tersebut terbagi menjadi dua bagian, diantaranya yaitu pelanggan dan penyedia komputasi awan. Tanggung jawab itu sangat bervariasi bentuknya dan dapat di spesifikasikan berdasarkan beban kerjanya seperti perangkat lunak sebagai layanan, platform sebagai layanan, infrastruktur sebagai layanan, serta pusat data lokalnya. Model ini membuat semua pengguna maupun yang terlibat di dalam suatu organisasi memahami arti tanggung jawab yang sebenarnya. Ketika data sebuah organisasi di pindahkan ke komputasi awan maka sebagian besar juga

tanggung jawab akan dipindahkan atau dialihkan ke bagian penyedia komputasi awan dan sisanya ke organisasi pelanggan. Di bawah ini tersedia sebuah gambar yang dapat mengilustrasikan area yang bertanggung jawab antara pelanggan dan penyedia komputasi awan berdasarkan tempat penyimpanan datanya.



Model Tanggung **Jawab Bersama**

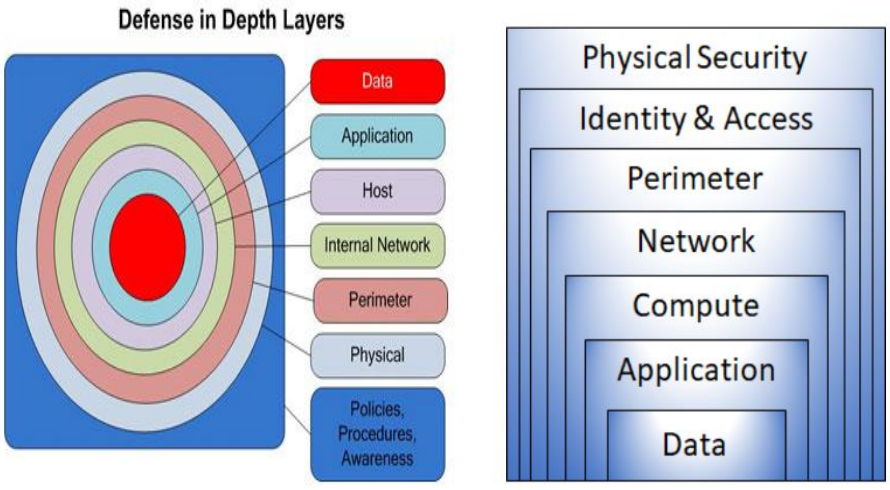
Sebuah pusat data lokal akan bertanggung jawab terhadap beberapa tugas komponennya seperti keamanan fisik hingga beberapa enkripsi data yang sangat sensitif. Sebuah infrastruktur layanan membutuhkan beberapa pengelolaan untuk melayani sebuah pelanggan komputasi awan. Sebagai pelanggan komputasi awan tidak bertanggung jawab atas sebuah komponen fisik berupa komputer dan jaringan atau keamanan fisik pusat data. Akan tetapi, pelanggan komputasi awan harus bertanggung jawab terhadap komponen perangkat lunak seperti sistem operasi, pengontrolan jaringan, aplikasi dan perlindungan data. Platform sebagai layanan menyediakan sebuah ruang lingkup untuk membangun, menyebarkan dan menguji aplikasi yang dibuat dengan tujuan untuk membantu ketika proses pembuatan aplikasi dengan cepat. Perangkat lunak sebagai layanan berhak dikelola oleh semua penyedia komputasi awan tanpa terkecuali. Contoh perangkat lunak sebagai layanan yaitu Microsoft 365, skype dan dymanis CRM online. Sehingga penyedia komputasi awan hanya bertanggung jawab dalam mengelola semuanya kecuali data, perangkat, dan identitas. Tanggung jawab yang selalu dipegang oleh sebuah organisasi pelanggan meliputi informasi dan data, perangkat, serta akun dan identitas. Sehingga manfaat dari model tersebut yaitu menyatakan bahwa model tersebut bertanggung jawab bersama dalam pengorganisasian tanggung jawab sebagai pengguna pengorganisasian schedule.

3.1.3. Proses Pertahanan yang Mendalam

Sebuah pertahanan yang mendalam pastinya menggunakan pendekatan yang berlapis – lapis agar dapat menjaga suatu data dari penyerang yang semakin datang menyerang daripada mengandalkan suatu perimeter. Strategi penggunaan proses pertahanan yang mendalam yaitu menggunakan serangkaian mekanisme agar mampu memperlambat kemajuan serangan. Karena

setiap lapisan mampu memberikan perlindungan dengan cara apabila ada pengguna yang salah melakukan proses koneksi dan terdapat kesalahan maka sistem akan menilai bahwa pengguna tersebut bukanlah pengguna aslinya melainkan penyerang. Sama halnya dengan apabila satu lapisan saja dilanggar maka lapisan berikutnya akan mencegah penyerang untuk mendapatkan akses yang tidak valid ke dalam suatu data. Ada beberapa contoh lapisan keamanan seperti berikut,

1. Keamanan fisik, membatasi akses ke pusat data karena hanya untuk personal yang berwenang.
2. Kontrol keamanan identitas dan juga akses, mengotentifikasi multi – faktor atau mengontrol akses ke infrastruktur juga kontrol perubahan.
3. Keamanan perimeter, melakukan perlindungan penolakan layanan yang terdistribusi agar dapat memfilter serangan berskala besar sebelum menyebabkan penolakan layanan bagi pengguna.
4. Keamanan jaringan, melakukan segmentasi jaringan serta kontrol akses jaringan untuk membatasi komunikasi antar sumber daya yang digunakan.
5. Menghitung keamanan lapisan, mengamankan akses ke mesin virtual yang ada di penyimpanan komputer atau di komputasi awal agar dapat menutup port tertentu lainnya.
6. Keamanan lapisan aplikasi, memastikan bahwa aplikasi yang digunakan aman dan bebas dari kerentanan keamanan.
7. Keamanan lapisan data termasuk kontrol untuk mengelola akses ke data bisnis untuk mengelola akses ke data bisnis dan pelanggan juga melakukan enkripsi dalam melindungi setiap data.



Proses Pertahanan **yang Mendalam**

Kerahasiaan, integritas dan ketersediaan atau disebut CIA dalam pelafalan bahasa inggris adalah cara untuk memikirkan sebuah pertukaran keamanan. Sebuah kerahasiaan pastinya akan

mengacu pada sebuah kebutuhan yang ingin dijaga kerahasiaannya secara sensitif seperti informasi mengenai pelanggan, kata sandi atau juga dapat berupa data keuangan. Kita dapat melakukan data enkripsi dalam menjaga kerahasiaan namun perlu juga dalam mengunci enkripsi. Karena kerahasiaan adalah bagian keamanan yang paling terlihat dan secara jelas melihat bagaimana pentingnya dan bermanfaatnya sebuah kunci, kata sandi, dan rahasia lainnya. Sebuah integritas akan mengacu pada cara menjaga data atau pesan agar tetap benar diimplementasikan. Ketika mengirim pesan email, dipastikan bahwa pesan yang diterima nantinya akan sama dengan data yang dikirim oleh pengirim. Enkripsi data dalam sebuah proses penjagaannya perlu ad acara mendekripsikannya agar sama halnya sebelum kita melakukan dienkripsi. Karena integritas memiliki keyakinan bahwa data yang tersedia oleh kita tidak terdapat kerusakan dan tidak ada proses perubahan oleh siapapun. Sedangkan ketersediaan mengacu pada cara membuat sebuah data yang tersedia bagi seorang pengguna yang membutuhkan. Penting bagi sebuah organisasi untuk menjaga keamanan data pelanggan, tetapi di waktu yang bersamaan pula harus tersedia bagi karyawan yang berhubungan dengan pelanggan. karena karyawan tetap memerlukan akses ke data yang didekripsi.

3.1.4. Ancaman Secara Umum

Seperti yang diketahui bahwa ancaman sebagai tindakan kekerasan yang dapat melibatkan satu atau lebih orang sehingga menyebabkan pihak yang terlibat mengalami kerugian. Berbagai ancaman yang dilakukan oleh penyerang atau pelaku pastinya memiliki tujuan tertentu seperti mencuri data sebuah organisasi, memeras uang bahkan bisa saja penyerang tersebut mengganggu operasi yang sedang dikerjakan.

Ancaman Secara **Umum**

a. Pelanggaran data

Dapat dikatakan pelanggaran data apabila memiliki suatu data yang dicuri dan data tersebut merupakan milik pribadi. Data pribadi artinya setiap informasi yang terkait dengan individu dapat digunakan dalam melakukan pengidentifikasian secara langsung maupun tidak

langsung. Ancaman tersebut dapat mengakibatkan malware, phishing, dan SQL yang diinjeksi untuk mencuri sandi atau sebuah detail tentang data terkait tersebut.

b. Serangan kamus (Dictionary Attack)

Serangan ini merupakan serangan terhadap identitas berupa mencuri identitas. Dengan mencoba sejumlah besar kata sandi yang diketahui atau secara acak ke salah satu tempat mengakses akun tertentu. Setiap kata sandi tersebut dengan otomatisnya akan menguji apakah benar saling terkait dengan nama pengguna ataukah tidak. Serangan ini dikenal juga sebagai serangan brute force.

c. Ransomware

Malware merupakan salah satu perangkat lunak yang digunakan oleh penjahat dunia internet untuk melakukan tindakan yang membahayakan. Malware dapat memberi akses yang tidak membutuhkan verifikasi kepada penyerang sehingga memungkinkan penyerang dapat melakukan aksi untuk mengambil pengelolaan sistem sumber daya sebuah organisasi atau seorang dan bisa saja mereka mengunci komputer sehingga tidak dapat diakses sehingga mereka meminta tebusan. Ransomware termasuk salah satu jenis malware yang mengenkripsi sebuah file dan folder dalam mencegah pengaksesan ke beberapa file yang penting. Penyerang yang mendistribusikan malware sering kali dimotivasi oleh uang dan akan menggunakan komputer yang terinfeksi untuk melancarkan serangan seperti mengumpulkan informasi yang dapat dijual, menjual akses ke sumber daya komputasi serta memeras pembayaran dari korban.

d. Serangan yang mengganggu

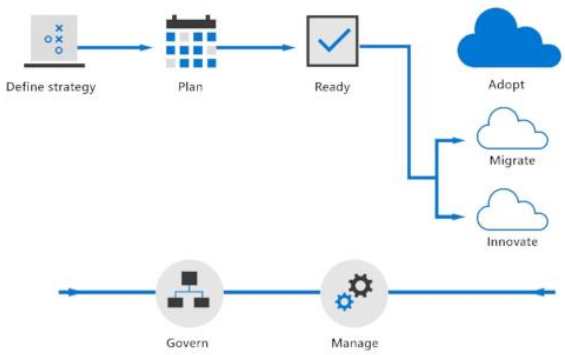
Serangan ini akan mencoba menghabiskan sumber daya suatu aplikasi sehingga membuat aplikasi tidak dapat diakses oleh pengguna yang seharusnya atau pengguna asli. Serangan ini lebih disebut serangan *Distributed Denial of Service* (DDoS) yang dapat menargetkan titik akhir yang dapat dijangkau oleh publik melalui internet.

Ancaman umum lainnya dapat berupa penambang koin, trojan, worm, juga rootkit. Rootkit tersebut mencegat dan mengubah proses standar sistem operasi dengan menginfeksi perangkat sehingga pengguna tidak dapat mempercayai informasi yang dilaporkan oleh perangkat terhadap akun yang dimilikinya. Trojan akan berpura – pura menjadi perangkat lunak yang asli dan saat pengguna akan menginstal suatu program yang bentuknya seperti yang diiklankan disitulah tindakan jahat dilancarkan seperti mencuri informasi. Artinya bahwa trojan itu harus di unduh terlebih dahulu secara manual dan dapat atau sering menggunakan nama file yang sama dengan aplikasi aslinya sehingga pengguna akan terkena perangkap untuk mengunduh trojan tersebut. Worm akan menginfeksi perangkat dengan mengeksploitasi kerentanan dalam aplikasi yang sedang berjalan sehingga dapat menyebar ke perangkat lain pada jaringan yang sama. Artinya, worm dapat menyalin dirinya sendiri dan dapat menyebar melalui jaringan dengan

memanfaatkan kerentanan tersebut. Penyebaran dilakukan berbagai tempat seperti email, pesan teks, file program, situs jejaring sosial, dan bisa juga drive. Kerentanan adalah salah satu kelemahan pada suatu perangkat lunak sehinggan digunakan oleh malware untuk masuk ke perangkat pengguna. Malware dapat mengeksploitasi kerentanan tersebut untuk melewati perlindungan keamanan komputer pengguna dan menginfeksinya.

3.1.5 Kerangka Kerja Adopsi Komputasi Awan

Microsoft Cloud Adoption Framework for Azure terdiri dari panduan implementasi, dokumen, praktik yang terbaik, dan juga alat yang dapat dirancang untuk membantu penerapan strategi bisnis di komputasi awan. Ini memberikan metodologi yang terbukti dan konsisten untuk menerapkan teknologi komputasi awan sebagai perusahaan dalam mengubah proses digital di dalam sistem perusahaan atau organisasi tersebut. Microsoft Cloud Adoption Framework for Azure telah terbukti dirancang untuk membantu membuat dan menerapkan strategi bisnis dan teknologi. Kerangka kerja dimulai dengan menentukan tujuan bisnis yang dikembangkan sehingga organisasi yang ada dapat mengidentifikasi peluang pertumbuhan dan cara mewujudkannya menggunakan teknologi komputasi awan. Perlu juga mempersiapkan organisasi untuk komputasi awan yang mencakup penyelarasan serta merasionalisasikan perkembangan digital saat ini serta mengatasi kesenjangan keterampilan dalam pemasukan teknologi baru. Setelah sistem organisasi siap untuk mengadopsi komputasi awan, maka dapat memigrasikan aplikasi dan memodernkannya serta dapat membangun solusi inovatif baru menggunakan teknlogi berbasis komputasi awan tersebut. Akhirnya, membangun lingkungan komputasi awan yang terkelola dengan baik dan menciptakan solusi yang berjalan secara optimal. Hal yang perlu diingat adalah proses yang terjadi berulang secara terus menerus karena sistem suatu organisasi perlu ditinjau setiap tahapnya. Adapun siklusnya dapat di lihat seperti di bawah ini:



Kerangka Kerja **Adopsi Komputasi Awan**

a. Strategi, menentukan pembenaran bisnis juga hasil adopsi yang diharapkan.
b. Rencana, menyelaraskan rencana adopsi yang dapat ditindaklanjuti dengan hasil bisnis.
c. Siap, menyiapkan lingkungan komputasi awan untuk perubahan yang direncanakan.

d. Mengadopsi
   - Memigrasikan dan memodernisasi beban kerja yang ada.
   - Berinovasi untuk mengembangkan solusi komputasi awan native atau hybrid baru.

e. Mengatur lingkungan dan beban kerja

f. Mengelola manajemen operasi untuk solusi komputasi awan dan hybrid

3.2 Kepatuhan dan Identitas di Bidang Kesehatan

Menurut HHS (Health and Human Services), HIT "Melibatkan pertukaran informasi kesehatan dalam lingkungan elektronik. Penggunaan IT kesehatan secara luas dalam industri perawatan akan meningkatkan kualitasnya, mencegah kesalahan medis, mengurangi biaya perawatan kesehatan, meningkatkan efisiensi administrasi, mengurangi dokumen dan memperluas akses ke perawatan kesehatan yang terjangkau." Selain HIT yang digunakan secara langsung untuk memberikan layanan perawatan pasien, organisasi kesehatan juga menggunakan HIT untuk fungsi manajemen dan dukungan bisnis. Manajemen catatan perawatan kesehatan termasuk bagian penting dari sistem perawatan karena industri berusaha untuk mengefisiensi dan melakukan otomatisasi. Program manajemen catatan kesehatan yang efektif akan mendukung kepatuhan terhadap berbagai persyaratan hukum dan peraturan. Walaupun setiap organisasi perlu mengembangkan program yang memenuhi kebutuhan spesifiknya ada dua hal yang perlu diketahui yaitu elemen sebagai pembuat dan pemelihara catatan termasuk kualitas dan kontrol akses, manajemen juga distribusi. Spesifikasi yang lainnya adalah pemusnahan yang tepat dari catatan perawatan kesehatan. Informasi catatan perawatan kesehatan harus dikelola dan dijaga dengan baik dari awal hingga akhir serta sepanjang waktu di antaranya. Pada pemukaannya, suatu kebijakan, prosedur, standar atau pedoman terdapat perbedaan yang jelas dan organisasi harus memahami seluk – beluk serta mengelola hubungan di antara alat tata kelola dalam memastikan program privasi dan keamanan yang sukses dalam organisasi perawatan kesehatan.

Kepatuhan dan Identitas di Bidang Kesehatan

Gambar tersebut terdapat hubungan antara setiap dokumen tata kelola yang berbeda misalnya kebijakan dan prosedur. Kita perlu memahami secara spesifiknya masing – masing, yaitu :

a. Kebijakan, dokumen yang sifatnya formal tingkat tinggi yang secara singkat dapat menyatakan sebuah perspektif organisasi tentang topik tertentu. Bentuknya ditulis pada tingkat tinggi maka akan berfokus pada tujuan organisasi, daripada panduan khusus tentang cara mencapai tujuan tersebut.
b. Prosedur, langkah – langkah berurutan terperinci yang didokumentasikan dan menginformasikan karyawan rumah sakit tentang cara melakukan tindakan tertentu. Karena kebijakan ditulis pada tingkat tinggi dan hanya menyatakan apa yang ingin dicapai oleh organisasi, prosedur diperlukan untuk memberi tahu karyawan bagaimana secara spesifik mencapai tujuan organisasi.
c. Standar, seperangkat spesifikasi yang harus diikuti oleh karyawan layanan kesehatan atau organisasi dan biasanya membahas sistem atau konfigurasi teknis. Standar memungkinkan sebuah organisasi untuk memiliki konsistensi. Memiliki konsistensi organisasi mendukung kebijakan dan memastikan bahwa tujuan privasi dan keamanan tercapai secara seragam di dalam organisasi. Standar tidak opsional dan diperlukan di seluruh organisasi.
d. Pedoman, rekomendasi atau saran terdokumentasi yang menawarkan panduan khusus topik berdasarkan praktik terbaik industri. Sebagian besar organisasi kesehatan memberikan pedoman kepada karyawan untuk membantu mereka membuat pilihan yang masuk akal dan membimbing mereka menuju keputusan dan menghasilkan hasil yang selaras dengan praktik terbaik industri.

Setiap organisasi harus memutuskan kerangka kerja mana yang paling sesuai dengan persyaratan bisnis dan peraturan khusus mereka. Tata kelola informasi dapat diartikan sebagai struktur (kerangka kerja) yang terdiri dari kebijakan, proses, prosedur, perilaku dan teknologi yang dirancang untuk membantu mengelola informasi sepanjang siklus hidupnya dengan cara yang konsisten. Struktur tata kelola memberi organisasi kemampuan untuk mengelola informasi dengan cara membantu memenuhi tujuan bisnisnya sampai meminimalkan risiko dan mempertahankan kepatuhan terhadap berbagai undang – undang tempat organisasi menjalankan bisnis.

3.2.1. Microsoft Cloud for Healthcare

Microsoft Cloud for Healthcare memberi organisasi layanan kesehatan alat untuk membantu dalam pengelolaan data kesehatan dalam skala besar. Cloud for healthcare membantu organisasi layar kesehatan, meningkatkan pengalaman pasien, mengoordinasikan perawatan, dan mendorong efisiensi operasional, membantu mendukung keamanan, kepatuhan dan interoperabilitas data kesehatan. Kesehatan dalam masa transisi, industri perawatan kesehatan yang telah di bebani oleh tren yang sudah berlangsung lama, seperti populasi yang menua, kelelahan penyedia, dan ketidakpuasan pasien. Sejak Covid -19, organisasi layanan kesehatan telah memikirkan norma – norma yang ditetapkan dan praktik terbaik dalam pengoperasiannya.

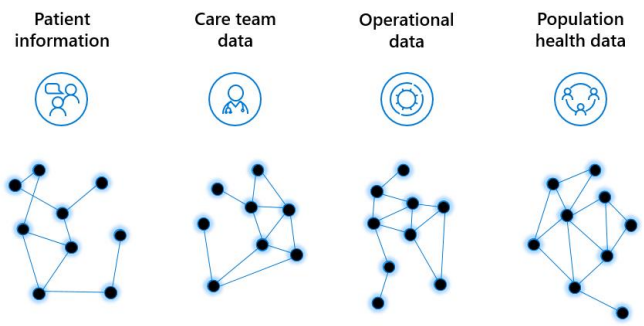
Sedangkan teknologi baru saat ini menjanjikan manfaat klinis dan operasional yang signifikan bagi organisasi layanan kesehatan, Covid – 19 telah mengubahnya dari yang bentuknya biasa saja.

Microsoft Cloud for **Healthcare**

Seperti yang ada pada gambar bahwa industri perawatan kesehatan mengalami transisi di bidang – bidang seperti kesehatan virtual, interoperabilitas, hasil kesehatan, serta tekanan keamanan,

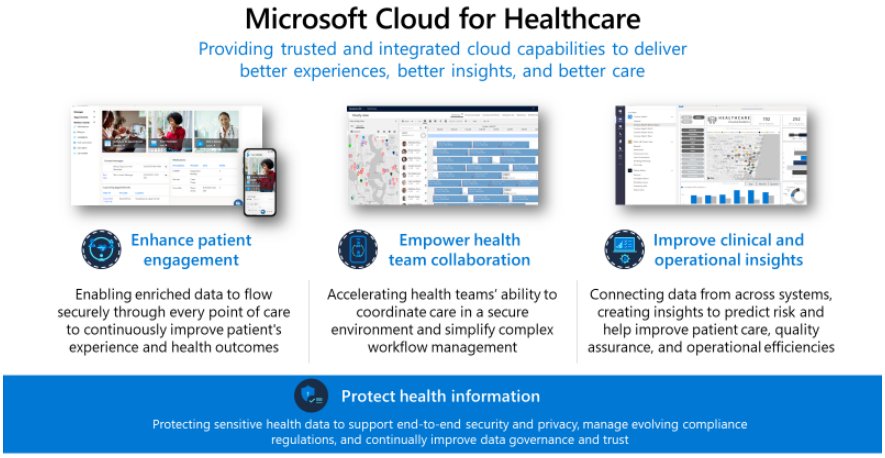
a. Kesehatan virtual, banyak pasien yang mencari peluang baru untuk menggunakan teknologi saat mengelola kesehatan mereka. Sebagai konsumen, pasien terbiasa mengelola aspek lain dari kehidupan mereka, seperti keuangan dan belanja online.
b. Interoperabiltas, meningkatkan keterlibatan pasien jarak jauh yang membutuhkan pertukaran data secara terintegrasi dan lancar untuk memastikan bahwa penyedia dapat mengakses wawasan pasien utama.
c. Hasil kesehatan, dengan volume data yang besar namun tidak terstruktur maka penyedia harus menghabiskan banyak waktu untuk mencoba mengumpulkan wawasan dari data tersebut. Faktor ini ada sebagai penghalang utama untuk meningkatkan data klinis, operasional, dan keuangan.
d. Tekanan keamanan, apabila organisasi perawatan kesehatan tidak dapat menggunakan data mereka secara efisien maka volume data yang besar menempatkan mereka pada risiko keamanan yang meningkat.

Organisasi perawatan kesehatan modern memiliki data yang berasal dari berbagai sumber. Pasien memasukkan informasi pribadi mereka saat pertama kali menghubungi penyedia perawatan primer yang kemudian menambahkan informasi tersebut dengan data klinis tentang kesehatan pasien. Penyedia layanan kesehatan juga dapat membandingkan data pasien dengan data kesehatan populasi untuk memahami tren yang luas mengenai pengaruh populasi pasien. Tujuan utama organisasi layanan kesehatan adalah untuk melayani pasien dan memberikan hasil perawatan terbaik, mereka juga harus mengelola data operasional untuk memelihara fasilitas mereka dan memastikan memberikan perawatan yang efisien.



Microsoft Cloud for **Healthcare**

Microsoft cloud for healtcare menyediakan kemampuan yang terintegrasi dan tepercaya. Kemampuan ini menyatukan data terstruktur dan tidak terstruktur untuk mengungkapkan wawasan yang dapat ditindaklanjuti dari analitik data cerdas dan mendorong efisiensi dengan mengotomatiskan alur kinerja bernilai tinggi.



Microsoft Cloud for **Healthcare**

Kemampuan ini mendukung tiga skenario prioritas yang disorot oleh Microsoft Cloud for Healthcare dengan cara yaitu :

1. Meningkatkan keterlibatan pasien, memungkinkan data pasien mengalir dengan aman di seluruh rangkaian perawatan, menciptakan pengalaman pasien secara individual dan menghadirkan alat kesehatan virtual dalam memfasilitas komunikasi antara penyedia dan pasien.
2. Memberdayakan kolaborasi tim kesehatan, mempercepat kemampuan tim kesehatan untuk mengordinasikan perawatan, berkolaborasi dalam pandangan pasien yang sama dan terpadu serta memantau pasien di lokasi terpencilnya sekalipun.
3. Meningkatkan wawasan klinis dan operasional, menyatukan data dan menerapkan analitik canggih dan kecerdasan buatan untuk mengungkapkan wawasan yang dapat ditindaklanjuti guna membantu membuat keputusan klinis dan operasional yang lebih baik dan cerdas.

Microsoft ini dibangun untuk melindungi informasi kesehatan dalam mendukung keamanan dan privasi secara menyeluruh, mengelola peraturan kepatuhan yang terus berkembang dan meningkatkan tata kelola serta kepercayaan data.

3.2.2. Kemampuan Layanan Kesehatan Unggulan

Terdapat sembilan kemampuan yang diaktifkan melalui tiga skenario yang dijelaskan di pembahasan sebelumnya dan berpusat pada penyedia. Setiap kemampuan dapat dikomposisi dengan artian bahwa penerapannya dilakukan satu per satu atau dalam kelompok. Pengguna juga dapat menggunakan investasi tersebut yang ada dalam teknologi Microsoft komputasi awan dengan menerapkan kemampuan ini ke solusi yang sudah diterapkan ke lingkungan. Kesembilan kemampuan tersebut yaitu :

1. Perawatan yang dipersonalisasi, membangun hubungan melalui peningkatan pengalaman yang dipersonalisasi untuk setiap pasien.
2. Wawasan pasien, mengubah data menjadi wawasan preskriptif.
3. Kesehatan virtual, menyediakan cara baru untuk pemeliharaan melalui teks bot, suara, video dan obrolan.
4. Kolaborasi tim perawatan, mengoptimalkan sumber daya dan menyelesaikan masalah secara kolektif.
5. Koordinasi perawatan, mengembangkan sistem keterlibatan dengan alur kerja yang cerdas.
6. Pemantauan pasien berkelanjutan, menggabungkan Internet of Medical Things (IoMT) dan analitik untuk mengoptimalkan perawatan.
7. Interoperabilitas, membuat sistem keterlibatan layanan kesehatan baru dengan menghubungkan data dari beberapa kumpulan data.
8. Analisis operasional, mendapatkan wawasan yang dapat ditindaklanjuti untuk mengoptimalkan operasi.
9. Analisis klinis, mengakses dan membantu pembagian data yang dapat ditindaklanjuti dengan aman untuk membantu meningkatkan perawatan pasien.

Kemampuan ini telah dibangun dengan hasil yang diinginkan dalam memberikan pengalaman pasien yang lebih baik, wawasan yang lebih baik mendorong perubahan positif dan perawatan yang lebih baik secara keseluruhan di seluruh rangkaian perawatan. Microsoft Cloud for Healthcare akan mendukung percepatan transformasi kesehatan ke masa depan dengan kemampuan komputasi awan yang terpercaya untuk pelanggan dan mitra mencakup kebutuhan paling penting bagi organisasi perawatan kesehatan.

DAFTAR PUSTAKA

Describe security concepts and methodologies - Learn | Microsoft Docs

Zero Trust Guidance Center | Microsoft Docs

Shared responsibility in the cloud - Microsoft Azure | Microsoft Docs

Common Data Model - Learn | Microsoft Docs

Microsoft Cloud for Healthcare overview - Learn | Microsoft Docs