# Lab - Rekomendasikan Langkah-Langkah Keamanan untuk Memenuhi Persyaratan Kepatuhan

## Tujuan

Bagian 1: Selidiki persyaratan kepatuhan

Bagian 2: Rekomendasikan solusi kepatuhan

### Latar belakang

Kepatuhan terhadap standar keamanan dan privasi yang relevan merupakan tantangan bagi sebagian besar bisnis. Kepatuhan sering kali rumit dan taruhannya tinggi. Bisnis sering kali menyerahkan sebagian besar beban kepatuhan kepada perusahaan yang mengkhususkan diri dalam menyediakan solusi yang telah terbukti memenuhi persyaratan kepatuhan dan memenuhi audit kepatuhan.

Di lab ini, Anda akan menyelidiki persyaratan kepatuhan dan merekomendasikan langkah-langkah untuk memenuhi persyaratan HIPAA. Health Insurance Portability and Accountability Act (HIPAA) adalah serangkaian peraturan yang dibuat di Amerika Serikat untuk melindungi privasi dan hak-hak pasien layanan kesehatan. Peraturan ini mengatur bagaimana informasi layanan kesehatan pasien dapat dibagikan. Peraturan ini menetapkan persyaratan terperinci yang dirancang untuk melindungi privasi dan keamanan pasien.

Semua penyedia layanan kesehatan di Amerika Serikat, dari kantor terkecil hingga rumah sakit terbesar, harus mematuhi HIPAA. Banyak penyedia layanan telah memasuki pasar untuk membantu penyedia layanan kesehatan dalam mencapai kepatuhan HIPAA.

#### Skenario

Dr. Anthony Larouche, seorang dokter gigi, telah bekerja di sebuah kantor gigi besar bersama dokter gigi lainnya. Ia telah memutuskan untuk membuka kantornya sendiri. Semua sistem TI yang terkait dengan kantor tersebut ditangani oleh staf kantornya. Ia hanya tahu sedikit tentang jaringan komputer dan keamanan jaringan. Ia telah mempekerjakan perusahaan Anda sebagai konsultan untuk membantunya mematuhi persyaratan keamanan teknis HIPAA.

Anda telah diminta untuk membuat daftar persyaratan khusus yang akan memenuhi Pengamanan Teknis berdasarkan Aturan Keamanan dalam peraturan kepatuhan HIPAA.

# Sumber Daya yang Diperlukan

• Komputer atau perangkat lain dengan koneksi internet

### Instruksi

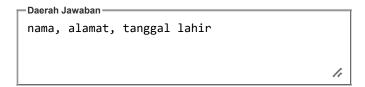
# Bagian 1: Selidiki persyaratan kepatuhan

Pada bagian ini, Anda akan meninjau persyaratan untuk mematuhi spesifikasi keamanan HIPAA. Peraturan HIPAA terdiri dari dua aturan, Aturan Privasi dan Aturan Keamanan. Kami akan fokus pada Aturan Keamanan, yang terdiri dari perlindungan, standar, dan spesifikasi implementasi. Ada lima standar keamanan dalam perlindungan teknis. Beberapa standar memiliki beberapa spesifikasi implementasi terkait. Beberapa standar tidak memiliki spesifikasi implementasi.

#### Langkah 1: Pahami Perlindungan HIPAA

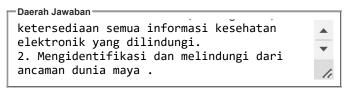
Telusuri web untuk mempelajari lebih lanjut tentang Pengamanan Aturan Keamanan HIPAA. Penelusuran yang baik untuk tinjauan umum adalah **site:compliancy-group.com aturan keamanan hipaa**. Jawab pertanyaan berikut.

Apa tiga contoh informasi kesehatan yang dilindungi?



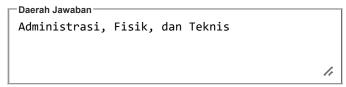
Tampilkan Jawaban

Rangkum empat aturan umum yang harus dipatuhi oleh semua organisasi perawatan kesehatan terkait Aturan Keamanan.



Tampilkan Jawaban

Apa saja tiga jenis perlindungan yang membentuk aturan keamanan HIPAA?



Tampilkan Jawaban

### Langkah 2: Tinjau dokumen Safeguard Teknis

- Silakan merujuk ke <u>dokumen</u> ini untuk klarifikasi mengenai Standar Keamanan Teknis 164.312 (a) (e)(2)(ii) dan penanganan informasi kesehatan elektronik yang dilindungi (EPHI). Konsultasikan sumber internet lainnya untuk klarifikasi tambahan. Tinjau isi dokumen dengan cepat.
- b. Lengkapi tabel di bawah ini dengan nama standar dan spesifikasi implementasi untuk standar tersebut, jika berlaku. Dua dari standar tersebut tidak memiliki spesifikasi implementasi.

Pengamanan Teknis				
Bagian	Standar	Spesifikasi Implementasi		
164.312(a)(1)	Daerah Jawaban  Kontrol Akses	Daerah Jawaban  - Identifikasi Pengguna Unik - Prosedur Akses Darurat - Logoff Otomatis - Enkripsi dan Dekripsi		
164.312(b)	Daerah Jawaban  Kontrol Audit	Daerah Jawaban Tidak tersedia		

Pengamanan Teknis				
164.312(c)(1)	Daerah Jawaban Integritas	- Mekanisme Autentikasi Informasi Kesehatan Elektronik yang Dilindungi		
164.312(d)	Daerah Jawaban Autentikasi Orang atau Entitas	Daerah Jawaban Tidak tersedia		
164.312(e)(1)	Daerah Jawaban  Keamanan Transmisi	Daerah Jawaban - Kontrol Integritas - Enkripsi		

Klik Tampilkan Jawaban pada tabel contoh jawaban.

Tampilkan Jawaban

### Bagian 2: Rekomendasikan solusi kepatuhan.

Spesifikasi keamanan teknis HIPAA harus menyarankan langkah-langkah keamanan yang akan meningkatkan atau memenuhi kepatuhan terhadap setiap persyaratan. Lengkapi tabel di bawah ini dengan rekomendasi Anda. Gunakan pengetahuan yang telah Anda peroleh dalam kursus sejauh ini dan lakukan pencarian internet tambahan. Anda akan menemukan bahwa ada banyak solusi yang tersedia dari perusahaan yang memenuhi setiap standar HIPAA.

Standar	Nama	Kontrol
164.312(a) (1)	Kontrol Akses	
164.312(a) (2)(i)	Identifikasi pengguna yang unik	Semua pengguna harus memiliki nama pengguna yang unik tidak hanya untuk login tetapi juga untuk mengidentifikasi siapa yang telah membuat mengedit atau mengakses FPHT.
164.312(a) (2)(ii)	Prosedur akses darurat	Penyimpanan HDD yang dicerminkan untuk rekaman, pencadangan, penggunaan cloud yang aman untuk penyimpanan dan pengambilan data.
164.312(a) (2)(iii)	Daerah Jawaban Keluar otomatis	Semua komputer harus diatur dengan kebijakan keamanan untuk logout setelah periode tidak aktif. Konfigurasikan aplikasi yang relevan untuk secara otomatis logout pengguna setelah periode tidak aktif juga.
164.312(a) (2)(iv)	Enskripsi dan Deskripsi	Identifikasi informasi yang akan dienkripsi, enkripsi HDD server, baik dalam perangkat lunak atau dengan drive enkripsi otomatis.
164.312(b)	Daerah Jawaban  Kontrol Audit	Terapkan akuntansi AAA dan pelacakan versi dokumen.
164.312(c) (1)	Integritas	
164.312(c) (2)	Mekanisme untuk mengotentikasi informasi kesehatan elektronik yang dilindungi (EPHI)	Terapkan pemantauan integritas file (FIM)
164.312(d)	Daerah Jawaban Autentikasi Orang atau Entitas	Otentikasi multifaktor (MFA), pertanyaan untuk pengaturan ulang kata sandi, otentikasi biometrik
164.312(e) (1)	Keamanan Transmisi	
164.312(e) (2)(i)	Daerah Jawaban  Kontrol integritas	keamanan komunikasi hashing pada dokumen yang dikirim, penghapusan email dan dokumen EPHI lainnya secara aman
164.312(e) (2)(ii)	Enkripsi	terenkripsi, HTTPS, menghapus EPHI dari email yang tidak terenkripsi seperti penerusan dan tanggapan.

Klik **Tampilkan Jawaban** pada tabel contoh jawaban.

Tampilkan Jawaban

# Pertanyaan Refleksi

1. Ada banyak kerangka kerja kepatuhan yang memberlakukan persyaratan pada keamanan jaringan. Relevansi kerangka kerja ini bergantung pada jenis bisnis dan aktivitas bisnis yang dilakukan. PCI-DSS adalah kerangka kerja kepatuhan untuk bisnis yang menerima pembayaran melalui kartu kredit. Telusuri web untuk **tujuan pengendalian PCI-DSS**. Setiap tujuan memiliki satu atau beberapa persyaratan. Dari penelusuran Anda, lengkapi tabel di bawah ini:

Tujuan PCI-DSS	Persyaratan PCI-DSS
Membangun dan memelihara jaringan yang aman.	- Instal dan kelola konfigurasi firewall untuk melindungi data pemegang kartu Jangan gunakan kata sandi sistem dan parameter keamanan lainnya yang disediakan vendor.
Daerah Jawaban  Lindungi data pemegang kartu.	- Lindungi data pemegang kartu yang tersimpan Enkripsi transmisi data pemegang kartu melalui jaringan publik yang terbuka.
Pertahankan program manajemen kerentanan.	- Gunakan dan perbarui perangkat lunak anti- virus secara teratur Mengembangkan dan memelihara sistem dan aplikasi yang aman.
Terapkan tindakan kontrol akses yang kuat.	- Batasi akses ke data pemegang kartu berdasarkan kebutuhan bisnis Tetapkan ID unik untuk setiap orang yang memiliki akses komputer Batasi akses fisik ke data pemegang kartu.
Pantau dan uji jaringan secara teratur.	- Melacak dan memantau semua akses ke sumber daya jaringan dan data pemegang kartu. - Uji sistem dan proses keamanan secara teratur.
Pertahankan kebijakan keamanan informasi.	- Pertahankan kebijakan yang membahas keamanan informasi untuk semua personel.

Klik Tampilkan Jawaban pada tabel contoh jawaban.

Tampilkan Jawaban

2. Bagaimana persyaratan kepatuhan ini dibandingkan dengan persyaratan HIPAA yang Anda berikan di atas?

Daerah Jawaban

Keduanya sangat mirip. Sebagian besar merupakan
persyaratan keamanan yang umum dan sudah dikenal.

Tampilkan Jawaban

3. Kerangka kerja kepatuhan seperti HIPAA dan PCI-DSS tidak hanya berlaku untuk organisasi besar, tetapi juga organisasi kecil. Misalnya, semua profesional medis harus mematuhi HIPAA. Semua bisnis yang menerima kartu kredit harus

mematuhi PCI-DSS. Bahkan, praktik medis yang menerima kartu kredit harus mematuhi keduanya. Dari pengalaman Anda meneliti di lab ini, apa saja tantangan utama kepatuhan organisasi yang lebih kecil menurut Anda?

- Daerah Jawaban

Organisasi kecil menghadapi tantangan signifikan dalam mematuhi kerangka kerja kepatuhan seperti HIPAA dan PCI-DSS. Salah satu tantangan utama adalah penilaian kepatuhan, di mana mereka tidak hanya perlu menerapkan langkahlangkah yang diperlukan tetapi juga membuktikan kepatuhan tersebut melalui audit keamanan dan penilaian kerentanan. Selain itu, keterbatasan sumber daya, baik dari segi finansial maupun personel, dapat menyulitkan mereka untuk memenuhi standar kepatuhan yang memerlukan investasi dalam teknologi dan pelatihan. Selain itu, kepatuhan berkelanjutan menjadi tantangan karena organisasi kecil harus terus memantau dan memperbarui kebijakan sesuai dengan perubahan regulasi dan teknologi.

Tampilkan Jawaban

Akhir dakum

Tampilkan Semua Jawaban

Hapus Respons Saya

© 2017 - 2022 Cisco dan/atau afiliasinya. Semua hak dilindungi undang-undang. Cisco Public