Tools Ringkasan Standar Aturan Keamanan HIPAA

Aris Susanto, A.Md.Perkes., S.T., M.MRS.

IDENTITAS

Nama Lengkap Asesor *

Jenis Kelamin *

- ○ Laki-laki
- ○ Perempuan

Pendidikan Terakhir *

Silahkan Pilih

Nomor HP/WA *

Email *

example@example.com

Nama Instansi yang dinilai *

Provinsi Instansi *

Silahkan Pilih

Kota/Kabupaten Instansi *

Contoh: Kota Cimahi, Kab. Bandung, Kota Bandung

Tanggal Asesmen *

Day Month Year

PENGAMANAN ADMINISTRATIF

Proses Manajemen Keamanan

CFR 164.308(a)(1)

Menerapkan kebijakan dan prosedur untuk mencegah, mendeteksi, menahan, dan mengoreksi pelanggaran keamanan.

Analisis Risiko (R) *

- ○ Ada
- ○ Tidak Ada

Lakukan penilaian yang akurat dan menyeluruh terhadap potensi risiko dan kerentanan terhadap kerahasiaan, integritas, dan ketersediaan informasi kesehatan elektronik yang dilindungi yang dimiliki oleh entitas yang dilindungi atau rekanan bisnis.

Manajemen Risiko (R) *

- ○ Ada
- ○ Tidak Ada

Terapkan langkah-langkah keamanan yang memadai untuk mengurangi risiko dan kerentanan ke tingkat yang wajar dan sesuai untuk mematuhi § 164.306(a)

Kebijakan sanksi (R) *

- ○ Ada
- ○ Tidak Ada

Terapkan sanksi yang sesuai terhadap anggota tenaga kerja yang gagal mematuhi kebijakan dan prosedur keamanan entitas yang tercakup atau rekanan bisnis

Tinjauan aktivitas sistem informasi (R) *

- ○ Ada
- ○ Tidak Ada

Terapkan prosedur untuk meninjau catatan aktivitas sistem informasi secara berkala, seperti log audit, laporan akses, dan laporan pelacakan insiden keamanan.

Tanggung Jawab Keamanan yang Ditetapkan

CFR 164.308(a)(2)

Identifikasi pejabat keamanan yang bertanggung jawab atas pengembangan dan penerapan kebijakan serta prosedur yang diwajibkan oleh subbagian ini untuk entitas yang tercakup atau rekanan bisnis.

Tanggung jawab keamanan yang ditetapkan (R) *

- ○ Ada
- ○ Tidak Ada

Identifikasi pejabat keamanan yang bertanggung jawab atas pengembangan dan penerapan kebijakan serta prosedur yang diwajibkan oleh subbagian ini untuk entitas yang tercakup atau rekanan bisnis.

Keamanan Tenaga Kerja

CFR 164.308(a)(3)

Menerapkan kebijakan dan prosedur untuk memastikan bahwa semua anggota tenaga kerjanya memiliki akses yang tepat terhadap informasi kesehatan elektronik yang dilindungi, sebagaimana diatur dalam paragraf (a)(4) bagian ini, dan untuk mencegah anggota tenaga kerja yang tidak memiliki akses berdasarkan paragraf (a)(4) bagian ini memperoleh akses ke informasi kesehatan elektronik yang dilindungi.

Otorisasi dan/atau pengawasan (A) *

- ○ Tidak Ada
- ○ Lain

Terapkan prosedur untuk otorisasi dan/atau pengawasan anggota tenaga kerja yang bekerja dengan informasi kesehatan elektronik yang dilindungi atau di lokasi tempat informasi tersebut dapat diakses.

Prosedur izin tenaga kerja (A) *

- ○ Tidak Ada
- ○ Lain

Terapkan prosedur untuk menentukan bahwa akses anggota tenaga kerja ke informasi kesehatan elektronik yang dilindungi sudah tepat.

Prosedur penghentian (A) *

- ○ Tidak Ada
- ○ Lain

Terapkan prosedur untuk menghentikan akses ke informasi kesehatan elektronik yang dilindungi ketika masa kerja, atau pengaturan lain dengan, anggota tenaga kerja berakhir atau sebagaimana diwajibkan oleh penentuan yang dibuat sebagaimana ditentukan dalam paragraf (a)(3)(ii)(B) dari bagian ini.

Manajemen Akses Informasi

CFR 164.308(a)(4)

Terapkan kebijakan dan prosedur untuk mengizinkan akses ke informasi kesehatan elektronik yang dilindungi yang konsisten dengan persyaratan yang berlaku pada subbagian E bagian ini.

Mengisolasi fungsi lembaga kliring perawatan kesehatan/clearinghouse* (R)

- ◯ Ada
- ◯ Tidak Ada

Jika lembaga kliring perawatan kesehatan merupakan bagian dari organisasi yang lebih besar, lembaga kliring tersebut harus menerapkan kebijakan dan prosedur yang melindungi informasi kesehatan elektronik yang dilindungi dari lembaga kliring tersebut dari akses yang tidak sah oleh organisasi yang lebih besar.

*Dalam konteks HIPAA (*Health Insurance Portability and Accountability Act*), *clearinghouse* mengacu pada entitas yang berfungsi sebagai perantara dalam pemrosesan klaim medis dan transaksi keuangan elektronik. *Clearinghouse* bertanggung jawab untuk mengonversi data dari satu format ke format lain yang sesuai dengan standar transaksi HIPAA.

Otorisasi Akses (A) *

- ◯ Tidak Ada
- ◯ Lain _____

Terapkan kebijakan dan prosedur untuk memberikan akses ke informasi kesehatan elektronik yang dilindungi, misalnya, melalui akses ke stasiun kerja, transaksi, program, proses, atau mekanisme lainnya.

Pembentukan dan modifikasi akses (A) *

- ◯ Tidak Ada
- ◯ Lain _____

Terapkan kebijakan dan prosedur yang, berdasarkan kebijakan otorisasi akses entitas yang tercakup atau rekan bisnis, menetapkan, mendokumentasikan, meninjau, dan memodifikasi hak akses pengguna ke stasiun kerja, transaksi, program, atau proses.

Kesadaran dan Pelatihan Keamanan

CFR 164.308(a)(5)

Menerapkan program kesadaran dan pelatihan keamanan untuk semua anggota tenaga kerjanya (termasuk manajemen)

Spesifikasi Implementasi Keamanan

	Tidak Ada	Lain (uraikan jika ada)
Pengingat Keamanan (A)	○	
Perlindungan dari Perangkat Lunak Berbahaya (A)	○	
Otorisasi Akses (A)	○	
Pembentukan dan Modifikasi Akses (A)	○	

Prosedur Insiden Keamanan

CFR 164.308(a)(6)

Respon dan Pelaporan (R) *

- ○ Ada
- ○ Tidak Ada

Mengidentifikasi dan menanggapi insiden keamanan yang diduga atau diketahui; mengurangi, sejauh yang dapat dilakukan, dampak buruk dari insiden keamanan yang diketahui oleh entitas yang tercakup atau rekan bisnis; dan mendokumentasikan insiden keamanan dan hasilnya.

Rencana Kontijensi

CFR 164.308(a)(7)

Tetapkan (dan terapkan sesuai kebutuhan) kebijakan dan prosedur untuk menanggapi keadaan darurat atau kejadian lain (misalnya, kebakaran, vandalisme, kegagalan sistem, dan bencana alam) yang merusak sistem yang berisi informasi kesehatan elektronik yang dilindungi.

Spesifikasi Implementasi Keamanan

	Tidak Ada	Lain (uraikan jika ada)
Rencana Pencadangan Data (R)	○	
Rencana Pemulihan Bencana (R)	○	
Rencana Operasi Mode Darurat (R)	○	
Prosedur Pengujian dan Revisi (A)	○	
Aplikasi dan Analisis Kekritisan Data (A)	○	

Evaluasi

CFR 164.308(a)(8)

Evaluasi teknis dan non teknis secara berkala *

○ Ada
○ Tidak Ada

Lakukan evaluasi teknis dan nonteknis secara berkala, yang awalnya didasarkan pada standar yang diterapkan berdasarkan peraturan ini dan, selanjutnya, sebagai respons terhadap perubahan lingkungan atau operasional yang memengaruhi keamanan informasi kesehatan elektronik yang dilindungi, yang menetapkan sejauh mana kebijakan dan prosedur keamanan entitas yang tercakup atau rekanan bisnis memenuhi persyaratan subbagian ini.

PENGAMANAN FISIK

Entitas yang tercakup atau rekanan bisnis harus, sesuai dengan § 164.306

Kontrol Akses Fasilitas

	Tidak Ada	Lain (uriakan jika ada)
Operasi Kontijensi (A)	○	
Rencana Keamanan Fasilitas (A)	○	
Prosedur Kontrol Akses dan Validasi (A)	○	
Catatan Pemeliharaan (A)	○	

Terapkan kebijakan dan prosedur yang menentukan fungsi yang tepat untuk dilakukan, cara fungsi tersebut dilakukan, dan atribut fisik lingkungan sekitar stasiun kerja atau kelas workstation tertentu yang dapat mengakses informasi kesehatan elektronik yang dilindungi. Terapkan perlindungan fisik untuk semua workstation yang mengakses informasi kesehatan elektronik yang dilindungi, untuk membatasi akses ke pengguna yang berwenang.

Workstation

	Ada	Tidak Ada
Penggunaan workstation (R)	○	○
Keamanan workstation (R)	○	○

Kontrol Perangkat dan Media

	Tidak Ada	Lain (uraikan jika Ada)
Pembuangan (R)	○	
Penggunaan Kembali Media (R)	○	
Akuntabilitas (A)	○	
Pencadangan dan penyimpanan data (A)	○	

PENGAMANAN TEKNIS

Kontrol Akses

	Tidak Ada	Lain (uraikan jika ada)
Identifikasi Pengguna Unik (R)	○	
Prosedur Akses Darurat (R)	○	
Logout otomatis (A)	○	
Eknkripsi dan Dekripsi (A)	○	

Lain-lain

	Tidak Ada	Lain (uraikan jika ada)
Kontrol Audit (R)	○	
Integritas (A)	○	
Autentikasi Orang atau Entitas (R)	○	
Keamanan Transmisi (A)	○	