IBM Watson Health Core

Syarat-syarat Penggunaan ("ToU") terdiri atas Syarat-syarat Penggunaan IBM – Syarat-syarat Tawaran Spesifik SaaS ("Syarat-syarat Tawaran Spesifik SaaS") ini dan sebuah dokumen berjudul Syarat-syarat Penggunaan IBM – Syarat-syarat Umum ("Syarat-syarat Umum") yang tersedia di URL berikut: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Apabila terdapat ketidaksesuaian, Syarat-syarat Tawaran Spesifik SaaS akan berlaku di atas Syarat-syarat Umum. Dengan memesan, mengakses, atau menggunakan SaaS IBM, Klien menyetujui ToU.

ToU diatur oleh Perjanjian Keuntungan Paspor Internasional IBM, Perjanjian Ekspres Keuntungan Paspor Internasional IBM, atau Perjanjian Internasional IBM untuk Tawaran SaaS IBM Terpilih, sebagaimana yang berlaku ("Perjanjian") dan bersama dengan ToU merupakan perjanjian yang lengkap.

1. SaaS IBM

Tawaran SaaS IBM berikut dicakup oleh Syarat-syarat Tawaran Spesifik SaaS ini:

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. Metrik Biaya

SaaS IBM dijual berdasarkan salah satu metrik(-metrik) biaya berikut sebagaimana yang ditetapkan dalam Dokumen Transaksi:

a. **Akses** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Akses adalah hak untuk menggunakan SaaS IBM. Klien harus memperoleh kepemilikan Akses tunggal untuk menggunakan SaaS IBM selama periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

b. **Individu** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Individu adalah benda tunggal atau seorang manusia. Kepemilikan yang memadai harus diperoleh untuk mencakup setiap Individu yang diproses oleh atau dikelola oleh SaaS IBM selama periode pengukuran yang ditetapkan dalam PoE atau Dokumen Transaksi Klien.

   Untuk tujuan SaaS IBM ini, suatu Individu termasuk seseorang, perangkat atau aplikasi mobile yang datanya dikelola oleh SaaS IBM.

c. **Mesin Virtual** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Mesin Virtual adalah akses ke suatu konfigurasi spesifik dari SaaS IBM. Kepemilikan yang memadai harus diperoleh untuk setiap Mesin Virtual SaaS IBM yang tersedia untuk akses dan penggunaan selama periode pengukuran yang ditetapkan dalam PoE atau Dokumen Transaksi Klien.

3. Biaya dan Penagihan

Jumlah yang harus dibayarkan untuk SaaS IBM ditetapkan dalam Dokumen Transaksi.

3.1 Biaya Pertengahan Bulan (*Partial Month Charges*)

Biaya pertengahan bulan sebagaimana yang ditetapkan dalam Dokumen Transaksi dapat dinilai secara pro-rata.

3.2 Biaya untuk Kelebihan Penggunaan

Apabila penggunaan yang sebenarnya oleh Klien atas SaaS IBM selama periode pengukuran melampaui kepemilikan yang dinyatakan dalam PoE, maka Klien akan dikenai biaya untuk kelebihan penggunaan tersebut sebagaimana yang tercantum dalam Dokumen Transaksi.

4. Jangka Waktu dan Opsi Pembaruan

Jangka waktu SaaS IBM dimulai pada tanggal ketika IBM memberi tahu Klien mengenai akses mereka ke lingkungan pengoperasian Perintis (*Pilot operating*) SaaS IBM, sebagaimana yang didokumentasikan dalam Dokumen Pemesanan. Periode langganan untuk kepemilikan Individu dimulai ketika IBM memberi

tahu Klien mengenai akses mereka ke lingkungan pengoperasian Produksi. Dokumen Pemesanan akan menetapkan apakah SaaS IBM memperbarui secara otomatis, berlanjut berdasarkan penggunaan berkelanjutan, atau berakhir pada akhir jangka waktu.

Untuk pembaruan otomatis, kecuali apabila Klien memberikan pemberitahuan tertulis untuk tidak memperbarui setidaknya 90 hari sebelum tanggal habis masa berlakunya jangka waktu, SaaS IBM akan secara otomatis memperbarui untuk jangka waktu yang ditetapkan dalam PoE.

Untuk penggunaan berkelanjutan, SaaS IBM akan terus tersedia dengan basis per bulan hingga Klien memberikan pemberitahuan tertulis 90 hari sebelumnya mengenai pengakhiran. SaaS IBM akan tetap tersedia hingga akhir bulan kalender setelah periode 90 hari tersebut.

5. Dukungan Teknis

IBM akan menyediakan Buku Petunjuk Dukungan Perangkat Lunak sebagai Layanan IBM yang memberikan informasi kontak dukungan teknis, waktu pemeliharaan, serta informasi dan proses lainnya. Informasi kontak dukungan teknis dan rincian lainnya mengenai pengoperasian dukungan dapat ditemukan di: Buku Petunjuk Dukungan SaaS IBM: https://support.ibmcloud.com.

Permintaan dukungan teknis dan konfigurasi sederhana untuk SaaS IBM diberikan melalui pengajuan elektronik. Dukungan teknis ditawarkan dengan SaaS IBM dan tidak tersedia sebagai suatu tawaran terpisah.

Informasi Pribadi (PI) termasuk Informasi Kesehatan yang Dilindungi (PHI) dan informasi pribadi sensitif (SPI) apa pun tidak dapat dimasukkan dalam dokumentasi atau informasi apa pun ketika melaporkan insiden masalah.

6. Definisi

Peraturan Perundang-undangan yang Berlaku – berarti setiap peraturan perundang-undangan, undang-undang atau pengesahan legislatif, peraturan, regulasi, arahan, perintah, dekrit, atau persyaratan lainnya yang dikeluarkan oleh otoritas pemerintah atau standar industri yang diakui secara umum yang berlaku pada kinerja Syarat-syarat Penggunaan

API – berarti antarmuka program aplikasi, yang merupakan kumpulan rutin, protokol, dan peralatan untuk pembuatan aplikasi perangkat lunak. API menentukan cara komponen perangkat lunak berinteraksi dan API digunakan ketika memprogram komponen antarmuka pengguna grafis (GUI).

Administrator yang Sah – adalah setiap karyawan Klien, kontraktor Klien yang disetujui, individu, atau grup yang bertanggung jawab atas pengelolaan pemeliharaan dan operasi platform yang dapat diandalkan. Tanggung jawab dapat mencakup konfigurasi, dukungan, serta pengelolaan pengguna dan akun. Administrator juga bisa seorang investigator klinis yang bertanggung jawab untuk mengatur penelitian dalam sistem Watson Health.

Individu yang Sah – adalah setiap orang, aplikasi mobile atau perangkat yang telah diotentikasi yang telah diberi akses guna mengakses hak-hak untuk mengirimkan data ke Watson Health Core. Hal ini dapat mencakup Klien; atau peserta penelitian, pelanggan, atau pasien Klien.

Peraturan perundang-undangan Data yang Berlaku Klien – berarti Peraturan Perundang-undangan Data yang berlaku untuk kinerja kewajiban Klien berdasarkan Perjanjian, Dokumen Terkait, dan Uraian Layanan yang berlaku, Dokumen Pemesanan serta Pernyataan Kerja antara para Pihak.

Data Klien – berarti input data apa pun dalam SaaS IBM oleh atau untuk Klien, baik data milik Klien atau data yang dimasukan oleh atau atas nama pelanggan Klien maupun pihak ketiga mana pun, dan termasuk data apa pun dari perangkat kesehatan kebugaran pihak ketiga.

Peraturan Perundang-undangan Data – berarti setiap Peraturan Perundang-undangan yang Berlaku yang berkaitan dengan perlindungan, kerahasiaan, atau keamanan data.

Subjek Data – berarti individu yang teridentifikasi atau dapat diidentifikasi yang terkait dengan Data Pribadi.

Pusat Data yang Ditunjuk – berarti pusat(-pusat) data yang ditetapkan untuk pusat data utama dan pemulihan bencana dalam Dokumen Transaksi yang menjalankan mesin virtual SaaS IBM Klien, apabila berlaku.

Data Kesehatan – berarti data atau informasi apa pun, termasuk gambar, yang merupakan Informasi Pribadi yang berkaitan dengan kesehatan.

Data Kesehatan yang Diaktifkan – berarti, terkait dengan SaaS IBM, kemampuan SaaS IBM untuk memenuhi standar kerahasiaan dan keamanan, peraturan perundang-undangan, dan regulasi yang berlaku di Yurisdiksi Dalam Cakupan untuk Data Kesehatan termasuk spesifikasi implementasi yang tercantum dalam Ayat 164, Subayat A dan C, pada regulasi yang mengimplementasikan HIPAA (sebagaimana yang dimodifikasi oleh Undang-undang HITECH) dan Peraturan Perundang-undangan yang Berlaku lainnya untuk Data Kesehatan, namun tidak berarti bahwa IBM bertindak dalam kapasitas Asosiasi Bisnis atau Pengendali Data.

HIPAA – berarti Health Insurance Portability and Accountability *Act* tahun 1996, sebagaimana yang diamandemen, termasuk Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act tahun 2009 ("Undang-undang HITECH"), regulasi tertentu yang diresmikan berdasarkan HIPAA oleh Departemen Kesehatan dan Layanan Masyarakat Amerika Serikat di 45 C.F.R. Ayat 160 dan 164 dan regulasi tertentu yang diresmikan menurut Undang-undang HITECH.

Peraturan Perundang-undangan Data yang Berlaku IBM – berarti Peraturan Perundang-undangan Data yang berlaku untuk kinerja kewajiban IBM berdasarkan Perjanjian, Dokumen Terkait, dan Uraian Layanan yang berlaku, Dokumen Pemesanan serta Pernyataan Kerja antara para pihak.

Personel IBM – berarti (a) IBM, Afiliasinya, dan subkontraktornya, dan terkait setiap pihak yang disebutkan di atas, karyawan mereka; dan (b) pemasok pihak ketiga mana pun; dalam setiap kasus yang menjalankan layanan atas nama IBM menurut Perjanjian dan Dokumen Terkait yang berlaku atau jika tidak, yang diberi akses ke Data Pribadi Klien oleh IBM.

Negara-negara Dalam Cakupan – berarti 28 Negara Anggota Uni Eropa dan Swiss, serta negara-negara yang dapat ditambahkan oleh IBM ke daftar ini dari waktu ke waktu.

Data Pribadi atau **Informasi Pribadi** – berarti informasi dalam media atau format apa pun, termasuk catatan elektronik dan tercetak, yang berkaitan dengan individu teridentifikasi atau yang dapat diidentifikasi, seorang "individu yang dapat diidentifikasi" merupakan seseorang yang dapat diidentifikasi, secara langsung maupun tidak langsung, khususnya melalui rujukan ke nomor identifikasi atau ke satu atau beberapa faktor spesifik dari identitas fisik, fisiologis, mental, ekonomi, budaya atau sosialnya.

Proses dan variasi darinya, seperti **pemrosesan** (baik dalam huruf besar atau tidak) – berarti setiap operasi atau kumpulan operasi yang dijalankan pada data, baik secara otomatis ataupun tidak, seperti pengumpulan, pencatatan, organisasi, penyimpanan, adaptasi atau perubahan, pengambilan kembali, konsultasi, penggunaan, pengungkapan melalui transmisi, penyebaran informasi, atau jika tidak, penyediaan, penjajaran atau penggabungan, pemblokiran, penghapusan atau pemusnahan.

Data yang Diproses – berarti setiap data, informasi atau materi rahasia atau kepemilikan, termasuk Data Kesehatan dan Data Pribadi, yang diproses oleh IBM menurut Perjanjian, Dokumen Terkait, dan/atau Uraian Layanan, Dokumen Pemesanan dan/atau Pernyataan Kerja.

Insiden Keamanan – memiliki arti yang tercantum dalam SBCA.

7. Manajemen Akun

SaaS IBM dapat diakses oleh pengguna yang sah Klien (hanya "**Administrator yang Sah**" atau "**Individu yang Sah**"). Klien akan mengendalikan akun yang disahkan untuk mengakses SaaS IBM, yang dapat mencakup aplikasi, personel Klien, penyedia dan kontraktor layanan pihak ketiga Klien yang sah, dan bertanggung jawab sepenuhnya atas (i) pengendalian semua pengguna yang sah, termasuk tanpa batasan, verifikasi identitas setiap pengguna yang sah; dan (ii) memastikan bahwa hanya pengguna yang sah yang mengakses SaaS IBM.

Individu yang Sah yang merupakan pelanggan, pasien atau peserta penelitian dari Klien dapat diberi akses hanya untuk tujuan pengunggahan data ke SaaS IBM, di mana dalam kasus ini, Individu yang Sah tidak akan memiliki akses lain ke SaaS IBM.

8. Kerahasiaan

8.1 Persyaratan Umum

Sebagaimana antara para Pihak, Klien adalah pengontrol tunggal atas semua Data Pribadi Klien, dan Klien menunjuk IBM sebagai prosesor data. Sesuai dengan Peraturan Perundang-undangan Data yang Berlaku, Klien memiliki hak untuk menginstruksikan IBM sehubungan dengan pemrosesan Data Pribadi Klien oleh IBM.

Apabila IBM memproses Data Pribadi Klien, IBM akan:

a. mematuhi semua Peraturan Perundang-undangan Data yang Berlaku IBM; dan

b. tidak mencampur Data Pribadi Klien dengan data dari sumber lain kecuali:

- sebagaimana yang diperlukan untuk menyediakan SaaS IBM dan bukan untuk tujuan lain apa pun, kecuali apabila diinstruksikan secara spesifik oleh Klien untuk melakukan hal tersebut; atau
- sesuai dengan syarat-syarat dari Syarat-syarat Penggunaan ini dan Apendiks SBCA.

Apabila IBM memproses Data Pribadi Klien, Klien akan:

a. mematuhi semua Peraturan Perundang-undangan Data yang Berlaku Klien;

b. bertanggung jawab atas semua komunikasi oleh Klien dengan Afilisasi, pasien, pengguna akhir, Subjek Data Klien dan/atau pihak ketiga Klien lainnya;

c. mengadakan perjanjian pemrosesan data dengan pengontrolnya yang diperlukan guna mengizinkan IBM sebagai prosesor data dan subprosesornya untuk memproses setiap Data Pribadi Klien; dan

d. bertindak sebagai pihak penghubung tunggal untuk IBM dan bertanggung jawab sepenuhnya untuk koordinasi internal, peninjauan, dan pengajuan instruksi atau permintaan Afiliasi Klien yang merupakan pengontrol lain atas IBM. IBM akan dibebaskan dari kewajibannya untuk menginformasikan atau memberi tahu Afiliasi Klien mana pun yang merupakan pengontrol ketika IBM telah memberikan informasi atau pemberitahuan tersebut kepada Klien. IBM berhak untuk menolak instruksi apa pun yang diberikan secara langsung oleh Afiliasi Klien mana pun yang merupakan pengontrol dari pihak yang bukan Klien.

Tidak ada pihak yang akan diwajibkan untuk bertindak dengan cara yang melanggar Peraturan Perundang-undangan Data yang Berlaku milik pihak tersebut.

8.2 Hak-hak Data Klien

Klien menyatakan dan menjamin bahwa pihaknya (a) memiliki data yang akan dimasukkan ke dalam SaaS IBM, atau (b) telah memperoleh, dan bertanggung jawab atas pemeliharaaan, semua hak-hak, izin, persetujuan dan otorisasi yang diperlukan untuk memberikan IBM hak untuk mengakses, menggunakan, dan mengungkapkan Data Klien sesuai dengan syarat-syarat yang tercantum dalam Syarat-syarat Penggunaan ini atau Perjanjian atau lainnya yang diperlukan bagi IBM untuk menyediakan SaaS IBM. Klien menyatakan dan menjamin lebih lanjut bahwa Data Klien hanya akan (a) berkaitan dengan individu yang berada di Amerika Serikat dan kemudian hanya akan dimasukkan ke dalam SaaS IBM di pusat data Amerika Serikat atau (b) berkaitan dengan individu yang berada di satu atau beberapa Negara-negara Dalam Cakupan dan kemudian hanya akan dimasukkan ke dalam SaaS IBM di Pusat(-pusat) Data yang Ditunjuk.

8.3 Layanan Data dan Tanggung Jawab

a. Klien menyetujui bahwa Klien hanya akan menjalankan analitik atau meminta IBM untuk menjalankan analitik pada Data Klien sehubungan dengan aktivitas yang merupakan "operasi pelayanan kesehatan" atau "penelitian" Klien sebagimana masing-masing ditentukan berdasarkan HIPAA dan/atau syarat-syarat serupa berdasarkan Peraturan Perundang-undangan Data yang Berlaku dan bahwa Klien akan menggunakan Data Klien atau mengarahkan IBM untuk menggunakan Data Klien hanya sehubungan dengan semua persyaratan yang sesuai (yaitu keputusan Dewan Peninjau Institusi (*Institutional Review Board*) atau pengabaian apabila diperlukan) berdasarkan Syarat-syarat Penggunaan ini atau Peraturan Perundang-undangan Data yang Berlaku Klien lain apa pun.

b. Klien bertanggung jawab sepenuhnya untuk memperoleh setiap dan semua registrasi, persetujuan, otorisasi, dan izin sebagaimana yang diperlukan oleh Peraturan Perundang-undangan yang Berlaku Klien di setiap Negara Dalam Cakupan yang berlaku, termasuk, tanpa batasan, HIPAA serta peraturan perundang-undangan kerahasiaan dan keamanan data, aturan, dan regulasi agar Data Klien dimasukkan ke SaaS IBM serta digunakan dan diungkapkan sebagaimana yang dimaksudkan berdasarkan Syarat-syarat Penggunaan ini dan Perjanjian oleh Klien serta oleh IBM dan subkontraktor IBM yang diizinkan. IBM tidak akan bertanggung jawab atas pemantauan ketika registrasi, persetujuan, otorisasi dan izin tersebut diterima atau diperlukan.

c. Klien bertanggung jawab sepenuhnya untuk memastikan bahwa semua Data Klien yang dimasukkan ke dalam SaaS IBM terbatas pada data yang berkaitan dengan individu yang berada di Amerika Serikat atau di suatu Negara Dalam Cakupan yang berlaku.

d. IBM akan memiliki pusat dukungan dengan personel yang dilatih mengenai HIPAA dan Peraturan Perundang-undangan Data yang Berlaku IBM lainnya mengenai data dari negara-negara Dalam Cakupan.

8.4 Tindakan Keamanan dan Insiden Keamanan

a. IBM akan mengimplementasikan, memelihara dan mematuhi langkah-langkah organisasional dan teknis (termasuk proses dan prosedur organisasional, serta termasuk setiap kewajiban kemananan spesifik yang ditetapkan atau direferensikan dalam Syarat-syarat Penggunaan ini dan SBCA untuk melindungi Data Pribadi Klien dari penggunaan atau akses yang tidak sah, kehilangan yang tidak disengaja, kerusakan, modifikasi, pemusnahan, pencurian atau pengungkapan yang tidak sah.

b. Apabila IBM menyadari Insiden Keamanan (sebagaimana yang didefinisikan oleh SBCA) yang melibatkan Data yang Diproses milik Klien, IBM akan menginformasikan kepada Klien sesuai dengan syarat-syarat SBCA dan Peraturan Perundang-undangan Data yang Berlaku IBM dan pemberitahuan tersebut akan mencakup informasi mengenai setiap pengaruh yang diketahui pada Klien atau Subjek Data apa pun (apabila ada) yang terpengaruh oleh Insiden Keamanan tersebut dan tindakan perbaikan yang dilaksanakan atau diajukan untuk dilaksanakan oleh IBM.

8.5 Penerimaan Pertanyaan dan Keluhan

IBM akan segera memberi tahu Klien secara tertulis dan, sejauh diizinkan oleh Peraturan Perundang-undangan Data yang Berlaku IBM, tidak lebih dari lima (5) hari kerja setelah Petugas IBM Watson Health Data Privacy menerima pertanyaan apa pun, komunikasi atau keluhan apa pun yang diterima oleh IBM yang berkaitan dengan Data Pribadi Klien dari:

a. setiap Subjek Data yang berkaitan dengan Data Pribadi mengenai Subjek Data tersebut yang Diproses oleh IBM. Klien akan menanggapi setiap permintaan dari Subjek Data tersebut dan IBM akan mematuhinya dengan instruksi yang wajar dari Klien untuk membantu Klien menanggapi permintaan tersebut. Apabila disyaratkan oleh Peraturan Perundang-undangan yang Berlaku IBM, IBM dapat menanggapi secara langsung permintaan tersebut, dengan ketentuan bahwa IBM memberi tahu Klien terlebih dahulu mengenai setiap tanggapan tersebut dan berkoordinasi secara wajar dengan Klien terkait bentuk dan konten tanggapan tersebut, apabila diizinkan oleh Peraturan Perundang-undangan yang Berlaku IBM atau sebaliknya apabila memungkinkan;

b. setiap otoritas hukum atau pengaturan, yang berkaitan dengan Pemrosesan setiap Data Pribadi Klien oleh IBM, dengan ketentuan bahwa IBM dapat menanggapi permintaan tersebut yang diterima dari agensi pemerintahan dengan surat perintah (*subpoena*) atau dokumen hukum serupa yang meminta pengungkapan oleh IBM atau sebaliknya diperlukan oleh Peraturan Perundang-undangan Data yang Berlaku, dengan ketentuan bahwa IBM memberi tahu Klien sebelumnya mengenai setiap pengungkapan tersebut dan berkoordinasi secara wajar dengan Klien mengenai bentuk dan konten tanggapan tersebut, apabila diizinkan oleh hukum atau sebaliknya apabila memungkinkan.

8.6 Pemrosesan Data Pribadi Klien

IBM akan membatasi pengungkapan Data Pribadi Klien kepada Personel IBM yang mungkin diperlukan untuk membantu IBM dalam memberikan Layanan.

IBM akan mematuhi setiap permintaan yang wajar dari Klien yang mewajibkan IBM untuk mengamendemen, memperbaiki, menghapus atau memblokir Data Pribadi Klien sesuai dengan Peraturan Perundang-undangan yang Berlaku.

Sesuai permintaan oleh salah satu Pihak, IBM, Klien atau Afiliasi mereka akan mengadakan perjanjian standar yang diwajibkan oleh hukum untuk melindungi Data Pribadi Klien. Para Pihak menyetujui (dan akan membuat masing-masing Afiliasi mereka menyetujui) bahwa perjanjian tersebut akan tunduk pada batasan dan pengecualian tanggung jawab dalam Perjanjian ini untuk tujuan klaim di antara para Pihak. Para Pihak akan bekerja sama dalam mengadakan (atau membuat Afiliasi Pihak tersebut mengadakan) dan mematuhi syarat-syarat atau perjanjian lebih lanjut yang disetujui bersama sebagaimana yang dapat diperlukan oleh Peraturan Perundang-undangan Data yang Berlaku.

8.7 Pengembalian Data Pribadi Klien

Pada pengakhiran atau habisnya masa berlaku Perjanjian, IBM akan, dan akan meminta semua Personel IBM untuk, berhenti menggunakan atau memproses Informasi Kepemilikan Klien apa pun dan Data Pribadi Klien apa pun dan akan, sesuai dengan opsi dan permintaan Klien:

a. segera mengembalikan dalam suatu format atau media penyimpanan yang dapat diminta oleh Klien secara wajar, semua Informasi Kepemilikan Klien dan Data Pribadi Klien yang disimpan secara elektronik oleh IBM dan setelah konfirmasi Klien atas penerimaan, penghapusan, pemusnahan, atau jika tidak, menjadikan Informasi Kepemilikan Klien dan Data Pribadi Klien tidak dapat dibaca atau tidak dapat dipahami secara permanen, termasuk salinan dan cadangan. IBM dapat membebankan biaya untuk biaya media penyimpanan dan aktivitas tertentu yang dijalankan sesuai dengan permintaan Klien (seperti pengiriman Informasi Kepemilikan Klien dan Data Pribadi Klien dalam format yang spesifik atau pemusnahan Informasi Kepemilikan Klien dan Data Pribadi Klien dengan cara tertentu); dan

b. Secara langsung menghapus, memusnahkan, atau dengan cara lain menjadikan Informasi Kepemilikan Klien dan Data Pribadi Klien tidak dapat dibaca atau tidak dapat dipahami secara permanen, termasuk salinan dan cadangan.

8.8 Perjanjian Asosiasi Bisnis

Apabila sesuai dan diperlukan oleh HIPAA, IBM dan Klien akan mengadakan Perjanjian Asosiasi Bisnis (*Business Associate Agreement* - "BAA"), yang akan mengatur kewajiban IBM sebagai Asosiasi Bisnis Klien dalam penyediaan SaaS IBM. Tanpa membatasi kewajiban tegas IBM berdasarkan Perjanjian dan BAA apabila berlaku, Klien menyatakan dan menyetujui bahwa Klien bertanggung jawab untuk menentukan keberlakuan, dan mematuhi, semua Peraturan Perundang-undangan yang Berlaku dan persyaratan pemberian lisensi yang berlaku untuk penggunaan Klien atau aktivitas lain sehubungan dengan (termasuk penggunaan atau aktivitas lainnya oleh Pengguna yang Sah) SaaS IBM.

8.9 Adendum Pemrosesan Data Uni Eropa

Apabila Klien memerintahkan IBM untuk memproses Data Pribadi Uni Eropa, IBM dan Klien akan mengadakan Adendum Pemrosesan Data termasuk, jika sesuai, Klausul Model Uni Eropa, dengan klausul pilihan yang dihapus.

9. Syarat-syarat Tambahan Tawaran SaaS IBM

9.1 Keamanan

SaaS IBM ini mematuhi prinsip-prinsip kerahasiaan dan keamanan data IBM untuk SaaS IBM yang tersedia di http://www.ibm.com/cloud/data-security dan syarat-syarat tambahan yang tercantum di bawah dan dalam Apendiks Keamanan dan Kesinambungan Bisnis dari Syarat-syarat Penggunaan ini. Perubahan apa pun pada prinsip-prinsip kerahasiaan dan keamanan data IBM tidak akan menurunkan keamanan SaaS IBM.

IBM Watson Health Core mengimplementasikan kebijakan, standar dan proses keamanan berdasarkan kerangka kerja ISO 27001 sebagaimana yang diuraikan lebih lanjut dalam Uraian Keamanan. Di antara kemampuan keamanannya, solusi mengimplementasikan hal berikut ini:

a. Zona Pengoperasian Aman

   IBM Watson Health Core mengimplementasikan pertahanan dengan strategi mendalam, memanfaatkan beberapa zona keamanan untuk mengelola titik integrasi *cloud* seperti onboarding data dan pengembangan aplikasi kustom.

b. Enkripsi

   Semua Data Klien dienkripsi dalam keadaan istirahat (*at rest*) dan bergerak (*in flight*). Semua data yang berpindah (*data in transit*) ke dan dari IBM Watson Health Core dienkripsi. Layanan bersama menyediakan manajemen kode enkripsi. Klien bertanggung jawab atas semua konektivitas dan kualitas jaringan antara Layanan IBM Watson Health dan server proksi Klien.

c. Pemantauan Peristiwa Keamanan

   IBM menggunakan platform intelejensi keamanannya untuk manajemen informasi dan peristiwa keamanan, manajemen catatan, forensik insiden, deteksi ancaman, dan manajemen kerentanan.

d. Manajemen Identitas

- Watson Health Core mendukung penyedia identitas standar terbuka untuk pasien dan populasi pengguna berskala besar dengan menggunakan OpenID Connect.
- Untuk populasi pengguna di mana IBM merupakan penyedia identitas, Watson Health Core memanfaatkan layanan direktori yang sesuai dan kemampuan manajemen identitas untuk menangani otentikasi.

e. Otentikasi Ketat dan Akses Berbasis Peran

- Watson Health Core mendukung otentikasi melalui SAML sebagai mekanisme bagi Klien untuk mengintegrasikan Single Sign On (SSO) atau layanan direktori mereka.
- Watson Health Core menggunakan solusi manajemen akses dan komponen terkait untuk mengelola kebijakan keamanan, apabila diperlukan.
- Watson Health Core mendukung otentikasi dua faktor berbasis perangkat lunak.
- Watson Health Core memberikan kontrol akses berbasis peran dasar, sebagaimana yang diperlukan; Watson Health Core mendukung konfigurasi penelitian, profil pengguna, peran, dan grup pengguna melalui antarmuka pemrograman aplikasi program ("API") yang mengaktifkan peran berbasis akses.

9.2 Cookies

Klien menyadari dan menyetujui bahwa IBM dapat, sebagai bagian dari dukungan dan operasi normal atas SaaS IBM, mengumpulkan informasi pribadi dari Klien (karyawan dan kontraktor Anda) yang berkaitan dengan penggunaan SaaS IBM melalui pelacakan dan teknologi lainnya. IBM melakukan hal tersebut untuk mengumpulkan statistik penggunaan dan informasi mengenai keefektifan SaaS IBM kami untuk tujuan memperbaiki pengalaman pengguna dan/atau menyesuaikan interaksi dengan Klien. Klien mengonfirmasikan bahwa pihaknya akan atau telah memperoleh persetujuan untuk mengizinkan IBM memproses informasi pribadi yang dikumpulkan untuk tujuan di atas dalam IBM, perusahaan-perusahaan IBM lainnya dan subkontraktor mereka di mana pun kami dan subkontraktor kami melakukan bisnis sesuai dengan hukum yang berlaku. IBM akan mematuhi permintaan dari karyawan dan kontraktor Klien untuk mengakses, memperbarui, memperbaiki atau menghapus informasi pribadi mereka yang dikumpulkan.

9.3 Lokasi Manfaat yang Diperoleh

Apabila berlaku, pajak akan didasarkan pada lokasi(-lokasi) yang diidentifikasi oleh Klien sebagai penerima manfaat dari SaaS IBM. IBM akan menerapkan pajak berdasarkan alamat bisnis yang dicantumkan pada saat memesan SaaS IBM sebagai lokasi manfaat utama kecuali apabila Klien memberikan informasi tambahan kepada IBM. Klien bertanggung jawab untuk tetap memperbarui informasi tersebut dan menyampaikan setiap perubahan kepada IBM.

9.4 Pengiriman Berkelanjutan

Klien berhak atas kemampuan dan peningkatan yang dibuat untuk solusi dan penyebaran oleh IBM dengan model pengiriman *cloud* berkelanjutan.

9.5 Pencadangan dan Restorasi

IBM Watson Health Core memberikan cadangan Data Klien di lingkungan produksi (termasuk tempat penyimpanan Data Lake dan Data Reservoir untuk keadaan baik yang terakhir diketahui dengan tujuan pemulihan layanan dalam peristiwa kegagalan sistem.

9.6 Ketersediaan Tinggi

Komponen IBM Watson Health Core di lingkungan produksi diimplementasikan dalam konfigurasi ketersediaan tinggi, dengan server basis data yang dikluster untuk redundansi guna memberikan distribusi beban kerja dan menghapus titik kegagalan tunggal.

9.7 Pemulihan Bencana

Pendekatan IBM untuk pemulihan bencana terdiri atas beberapa pusat data di area geografi yang tersebar untuk mencapai sasaran kesinambunganbisnisnya sebagai berikut untuk lingkungan Produksi-nya:

- RTO – dalam waktu 36 jam setelah pernyataan bencana
- RPO – tidak lebih dari 24 jam sejak hilangnya konten Klien

9.8 Peralatan Pengukuran

SaaS IBM menggunakan solusi pemantauan sintetik untuk memantau, mengukur dan melaporkan ketersediaan atau ketidaktersediaan terhadap tingkat layanan yang ditetapkan. Solusi ini menyimulasikan dan melacak tanggapan pengguna dan pengalaman pengguna di tingkat global – baik untuk ketersedian statis dan transaksi.

SaaS IBM juga menggunakan sistem pemantauan internal untuk metrik, peristiwa, dan peringatan di semua solusi.

9.9 Publisitas

Klien menyetujui bahwa IBM dapat merujuk Klien sebagai pelanggan SaaS IBM dalam komunikasi pemasaran atau publisitas.

Apendiks A

1. IBM Watson Health Core

IBM Watson Health Core merupakan platform sebagai layanan (*platform as a service* - "PaaS") yang Diaktifkan oleh Data Kesehatan, platform pengembangan, dan subsistem operasional untuk penyimpanan, perbaikan, dan pemrosesan Informasi Kesehatan yang Dilindungi (*Protected Health Information* - "PHI"), sebagaimana yang ditentukan oleh HIPAA dan Data Kesehatan lainnya sesuai dengan Peraturan Perundang-undangan Data yang Berlaku IBM yang berada di pusat data yang dikontrol atau dimiliki oleh IBM. Klien harus memperoleh kepemilikan yang sesuai untuk IBM Watson Health Core dan IBM Watson Health Core Access untuk mengaktifkan fitur dan kemampuan yang diuraikan di bawah ini.

1.1 Watson Health Core Operating Environments

Kepemilikan Watson Health Core mencakup tiga lingkungan pengoperasian *cloud* yang diaktifkan Data Kesehatan yang dirancang untuk mengizinkan Klien memproses Data Kesehatan:

- Percobaan

  Memberikan lingkungan pengujian di mana Klien dapat mengembangkan dan menguji aplikasi yang dibangun dengan menggunakan SaaS IBM. Lingkungan percobaan mengimplementasikan semua kontrol keamanan HIPAA kecuali untuk Pemulihan Bencana, ketersediaan tinggi dan cadangan sistem catatan.

- Lingkungan Produksi

  Memberikan lingkungan berskala penuh di mana Klien dapat menyebarkan beban kerja Data Kesehatan. Lingkungan produksi merupakan lingkungan muatan yang diseimbangkan dengan ketersediaan tinggi dan dapat gagal di lokasi Pemulihan Bencana.

- Pemulihan Bencana

  Memberikan tiruan serupa dengan lingkungan Produksi; dan berlokasi di lokasi pusat data yang terpisah.

1.2 Pengembangan Aplikasi

IBM Watson Health Core mengaktifkan pengembangan aplikasi dan pengumpulan data aman dari perangkat Klien atau perangkat pengguna yang sah Klien. API memberikan antarmuka program dan dokumentasi yang pengguna yang sah Klien, termasuk penyedia layanan pihak ketiga Klien, dapat menggunakannya untuk mengembangkan aplikasi dan bertukar data dengan SaaS IBM. Penggunaan API oleh Klien atau pengembangnya tunduk pada kepatuhan dengan Persyaratan Pengembang API.

- REST API

  Watson Health Core memberikan serangkaian REST API dan layanan untuk platform Watson Health Core. Kemampuan API mencakup, namun tidak terbatas pada, mekanisme untuk mengakses penyimpanan data, layanan kurasi data, manajemen pengguna, dan catatan audit.

- Apple HealthKit dan Apple ResearchKit

  Watson Health Core mendukung integrasi dengan kerangka kerja API Apple ResearchKit untuk pembelajaran penelitian berbasis iOS, dan dengan Apple HealthKit untuk mendapatkan data kesehatan.

1.3 Tata Kelola Data

- Manajemen Persetujuan

  Watson Health Core memberikan kerangka kerja untuk mendapatkan persetujuan yang diberikan oleh pasien atau peserta penelitian dan dapat menyimpan dengan aman catatan persetujuan terpisah dari muatan data ketika individu mendaftar melalui aplikasi Klien yang diaktifkan persetujuan.

- Penyamaran Data

  Watson Health Core memberikan kemampuan untuk memisahkan pengenal nama dari muatan data terstruktur. Watson Health Core menerima data di *cloud* melalui API program. API memungkinkan pemisahan pasien atau pengenal nama individu dari keseluruhan muatan data, untuk disimpan di penyimpanan data terenkripsi yang terpisah. Muatan data ditetapkan sebagai suatu token anonim yang dapat digunakan umtuk pelacakan sumber (*provenance tracking*) di masa mendatang.

1.4 Layanan Data Kesehatan

Watson Health Core memberikan pengumpulan, penyimpanan, sinkronisasi data, termasuk Data Kesehatan eksogen dan Informasi Pribadi lainnya, baik terstrukur maupun tidak terstruktur.

- Pengambilan Data

  Watson Health Core memberikan kemampuan untuk mengambil data dari aplikasi atau perangkat pasien melalui API program. Watson Health Core memberikan hak kepada setiap Individu yang Sah Klien untuk mengunggah hingga 25 MB data ke Health Core setiap tahun dari jangka waktu kontrak. Layanan mengakomodasi hingga 10 unggahan per Individu per hari.

- Data Lake Operasional

  Data pasien atau Klien Mentah disimpan di Watson Health Core dalam bentuk asalnya hingga dibutuhkan untuk analitik dan pemodelan.

- Muatan Perubahan Ekstrak (*Extract Transform Load* - "ETL")

  Data diubah menjadi format yang dinormalisasikan dalam subsistem operasional. Suatu standar industri berdasarkan Kabel Layanan Perusahaan (*Enterprise Service Bus*) untuk pelayanan kesehatan memudahkan izin untuk integrasi antar aplikasi dan protokol Klien yang berbeda.

- Data Reservoir

  Setelah dikurasi, data dipindahkan ke Data Reservoir. Watson Health Core menggunakan aspek-aspek IBM Unified Data Model for Healthcare untuk menormalkan data kesehatan bisnis dan teknis untuk penggunaan dalam analitik.

- Indeks Orang Utama

  Watson Health memberikan peralatan Manajemen Data Utama dengan tujuan untuk mengkonsolidasikan data dari berbagai sumber untuk membuat Catatan Orang Memanjang (*Longitudinal Person Record* - "LPR").

2. Fitur Opsional

2.1 IBM Watson Health Core Terminology Service

Layanan add-on ini memudahkan integrasi data dan keberoperasian antara sistem kesehatan yang berbeda, yang memberikan penggunaan istilah klinis yang konsisten di semua aplikasi Watson Health Cloud. Layanan ini memberikan platform fungsional untuk semua tugas yang melibatkan istilah-istilah, sistem kode, dan konten terstruktur, seperti:

- pembuatan sistem kode baru;
- penerjemahan sistem kode internasional; dan
- pemetaan antara daftar kode lokal dan standar internasional.

Apendiks B

IBM memberikan perjanjian tingkat layanan ("SLA") ketersediaan berikut untuk SaaS IBM sebagaimana yang ditetapkan dalam PoE. SLA bukan merupakan suatu jaminan. SLA tersedia hanya untuk Klien dan berlaku hanya untuk penggunaan di lingkungan produksi.

1. Kredit yang Tersedia

Potongan harga ketersediaan hanya berlaku untuk biaya langganan atas kepemilikan Individu.

Klien harus mencatatkan tiket dukungan Tingkat Permasalahan 1 dengan bagian bantuan (*help desk*) dukungan teknis IBM dalam waktu 24 jam sejak pertama kali menyadari bahwa suatu peristiwa telah berdampak pada ketersediaan SaaS IBM. Klien harus membantu IBM secara wajar dengan setiap diagnosis dan penyelesaian masalah.

Klaim tiket dukungan atas kegagalan untuk memenuhi suatu SLA harus diajukan dalam waktu tiga hari kerja setelah akhir bulan masa kontrak. Kompensasi untuk klaim SLA yang sah akan menjadi kredit terhadap tagihan yang akan datang untuk SaaS IBM berdasarkan durasi waktu saat pemrosesan sistem produksi untuk SaaS IBM tidak tersedia ("Waktu Henti"). Waktu Henti dihitung dari waktu Klien melaporkan peristiwa tersebut hingga waktu SaaS IBM dipulihkan dan tidak termasuk waktu yang berkaitan dengan penghentian untuk pemeliharaan yang terjadwal atau telah diumumkan; sebab-sebab di luar kendali IBM; masalah dengan rancangan atau instruksi, konten atau teknologi Klien atau pihak ketiga; konfigurasi sistem dan platform yang tidak didukung atau kesalahan Klien lainnya; atau insiden keamanan yang disebabkan oleh Klien atau pengujian keamanan Klien. IBM akan memberlakukan kompensasi yang berlaku yang paling tinggi berdasarkan ketersediaan kumulatif SaaS IBM selama masing-masing bulan masa kontrak, sebagaimana yang ditunjukkan dalam tabel di bawah. Total kompensasi berkaitan dengan bulan masa kontrak mana pun tidak dapat melampaui 20 persen dari satu per dua belas (1/12) dari biaya tahunan untuk SaaS IBM.

2. Tingkat Layanan

Ketersediaan SaaS IBM selama suatu bulan masa kontrak

Ketersediaan selama suatu bulan masa kontrak	**Kompensasi (% biaya langganan Individu bulanan* untuk bulan masa kontrak yang merupakan pokok klaim)**
< 99,95%	10%
< 99,0%	20%

* Jika SaaS IBM diperoleh dari Mitra Bisnis IBM, biaya langganan bulanan akan dihitung sesuai daftar harga yang berlaku pada saat itu untuk SaaS IBM yang berlaku selama bulan masa kontrak yang merupakan pokok klaim yang didiskon sebesar 50%. IBM akan menyediakan suatu potongan harga secara langsung untuk Klien.

Ketersediaan yang dinyatakan sebagai persentase dihitung dengan cara: total jumlah menit dalam suatu bulan masa kontrak, dikurangi total jumlah menit Waktu Henti dalam suatu bulan masa kontrak, dibagi dengan total jumlah menit dalam bulan masa kontrak.

Contoh: 108 menit total Waktu Henti selama bulan masa kontrak

43.200 total menit dalam suatu bulan masa kontrak selama 30 hari - 108 menit Waktu Henti = 43,092 menit _____ 43.200 total menit	= 10% kredit yang Tersedia untuk 99.75% ketersediaan selama bulan masa kontrak

3. Pengecualian

SLA ini tidak berlaku untuk hal-hal berikut:

- Selain pemantauan server, SLA tidak berlaku untuk mesin virtual yang diselenggarakan untuk mendukung aplikasi kustom atau Klien.
- Apabila Klien telah melanggar kewajiban materiil apa pun berdasarkan kewajiban perjanjian saat ini.

Apendiks C

Apendiks Keamanan dan Kesinambungan Bisnis ini ("SBCA" ini) mencantumkan persyaratan dan kewajiban tertentu bagi IBM dalam menyediakan SaaS IBM untuk Klien. Persyaratan dan kewajiban yang tercantum dalam dokumen ini adalah tambahan untuk persyaratan dan kewajiban yang tercantum di uraian prinsip-prinsip untuk keamanan data untuk SaaS IBM yang tersedia di http://www.ibm.com/cloud/data-security. Istilah-istilah dalam huruf besar yang tidak didefisinikan di sini akan memiliki makna yang tercantum dalam Perjanjian atau Syarat-syarat Penggunaan.

1. Program Keamanan Informasi

IBM memiliki kebijakan, standar, dan proses keamanan internal berdasarkan kerangka kerja dan area kontrol ISO 27001. Selain tata kelola Organisasi Keamanan Perusahaan IBM (*IBM Corporate Security Organization*), kebijakan, standar, dan proses tersebut tunduk pada audit internal secara rutin.

IBM mempertahankan suatu program keamanan informasi untuk perlindungan organisasional, operasional, administratif, fisik, dan teknis yang melakukan tata kelola pemrosesan, penyimpanan, dan transmisi konten Klien yang setidaknya sesuai dengan persyaratan SBCA ini.

IBM akan membagi dengan Klien, sesuai dengan permintaan Klien, informasi mengenai program keamanan informasi IBM Watson Health sehingga Klien dapat menentukan secara wajar kesinambungan kesesuaian, kecukupan, dan keefektifannya. Program keamanan informasi IBM Watson Health akan diperbarui dari waktu ke waktu agar tetap terbarukan dengan praktik industri yang diterima secara umum dan Peraturan Perundang-undangan yang Berlaku IBM.

2. Pengendalian Akses

IBM akan mengungkapkan konten Klien hanya kepada karyawan, subkontraktor atau pihak ketiganya yang memiliki kebutuhan bisnis yang sah untuk mengakses konten Klien tersebut dengan tujuan untuk membantu IBM melaksanakan kewajibannya kepada Klien atau orang lain sebagaimana yang diperlukan untuk menyediakan SaaS IBM sesuai dengan Peraturan Perundang-undangan yang Berlaku, Perjanjian atau Dokumen Terkait, sebagaimana berlaku. Apabila IBM merupakan Asosiasi Bisnis Klien, IBM dan Klien akan mengungkapkan Informasi Kesehatan Pribadi hanya sesuai dengan syarat-syarat Perjanjian Asosiasi Bisnis yang berlaku antara para Pihak.

IBM memiliki proses pengelolaan akses pengguna internal dan formal di mana akses pengguna diminta, disetujui setelah verifikasi identitas, dan diberikan secara formal berdasarkan kebutuhan untuk mengetahui, dengan memanfaatkan konsep hak terendah. Akses ke konten Klien akan dibatasi hanya untuk pengguna aktif dan akun pengguna aktif. IBM memiliki proses formal untuk validasi ulang akses internal berkala atas akun pengguna aktif.

IBM menggunakan protokol otentikasi pengguna yang aman, termasuk menetapkan identifikasi khusus dan kata sandi yang kuat untuk akun pengguna aktif pada sistem yang digunakan untuk memberikan layanan kepada Klien sesuai dengan standar dan kebijakan keamanan perusahaan IBM:

a. Kata sandi tidak akan berupa kata sandi default yang disuplai oleh vendor dan akan disimpan di lokasi dan/atau dalam format yang tidak mengurangi keamanan data yang dijaga.

b. Tampilan dan pencetakan kata sandi harus disamarkan, disembunyikan atau jika tidak, dikaburkan sehingga pihak-pihak yang tidak sah tidak dapat mengobservasi atau memulihkan kata sandi sesudahnya. Kata sandi tidak dapat dicatat atau ditahan saat kata sandi tersebut dimasukkan. Kata sandi pengguna tidak dapat disimpan dalam teks yang jelas.

c. Kata sandi untuk setiap teknologi yang berisi SaaS IBM dipilih untuk mengurangi risiko terkait dengan kerentanan panjang kata sandi yang diketahui dan harus didokumentasikan.

d. Ketika penggunaan ID internal, istimewa, dan fungsional bersama diperlukan untuk alasan operasional, IBM mengelola ID bersama, fungsional, dan/atau Sistem yang membutuhkan pemeriksaan kata sandi untuk memelihara akuntabilitas individu.

Batas waktu ketidakaktifan ditetapkan untuk semua sistem dan aplikasi yang menyimpan konten Klien.

Apabila diperlukan, akses jarak jauh ke jaringan, sistem dan aplikasi IBM yang menyimpan konten Klien akan dibuat berdasarkan permintaan Klien dan persetujuan formal IBM, serta semua koneksi jarak jauh

tersebut akan diamankan dengan menggunakan protokol otentikasi dan enkripsi yang ketat. Aktivitas akses jarak jauh akan dicatat dan dipantau.

Apabila penyampaian SaaS IBM memerlukan IBM untuk mengakses sistem apa pun dalam jaringan internal Klien secara jarak jauh, semua akses jarak jauh tersebut akan dijalankan hanya dengan menggunakan sistem dan protokol akses jarak jauh aman Klien dan menggunakan kredensial akses yang diberikan kepada IBM oleh Klien. Akses jarak jauh ke jaringan Klien akan dibuat hanya sesuai permintaan IBM dan disetujui oleh Klien, dan sesuai dengan kebijakan Klien saat itu, yang akan diberikan kepada IBM di muka. Penggunaan jaringan internal Klien oleh IBM akan tunduk pada penggunaan IT dan kebijakan keamanan Klien yang akan diberikan kepada IBM di muka.

IBM mengimplementasikan pemisahan kewajiban untuk administrasi keamanan, peninjauan akses, dan investigasi pelanggaran keamanan.

Penyimpanan, penyelenggaraan, dan pemrosesan konten Klien spesifik untuk Klien secara logika terpisah dari klien lain yang dilayani oleh IBM. Dalam mesin virtual di mana area kerja penyimpanan, penyelenggaraan, dan pemrosesan bersama disahkan oleh Klien, IBM akan memiliki prosedur dan perlindungan keamanan yang sesuai dengan persyaratan yang tercantum dalam SBCA ini yang dirancang untuk mencegah pengungkapan yang tidak sah atas konten Klien tersebut.

IBM mengimplementasikan kebijakan meja bersih/layar bersih untuk memastikan bahwa konten Klien selalu diawasi di tempat umum mana pun setiap saat.

3. Transfer dan Enkripsi

IBM akan menjalankan tindakan pencegahan pentransmisian konten Klien yang sesuai (dengan faksimile, *email*, kurir, dll.) untuk memastikan bahwa informasi kontak yang benar digunakan untuk penerima dan membuat pengaturan awal dengan penerima yang dimaksud untuk mengamankan penerimaan informasi tersebut.

IBM menggunakan, dan akan memerintahkan Personel IBM untuk selalu menggunakan, formulir enkripsi yang sesuai atau teknologi yang aman lainnya sehubungan dengan pemrosesan konten Klien, termasuk yang berhubungan dengan setiap transfer, komunikasi, akses jarak jauh atau penyimpanan (termasuk penyimpanan cadangan) konten Klien. Sebagai contoh, IBM akan mengenkripsi, dengan menggunakan enkripsi berstandar industri yang sesuai, semua catatan dan file yang berisi konten Klien:

a. yang disimpan di laptop, perangkat portable atau media elektronik portabel IBM termasuk perekam cadangan ketika dalam perjalanan ke fasilitas penyimpanan di luar situs;

b. yang disimpan atau dipindahkan oleh IBM ke luar fasilitas dan kantor IBM atau Klien yang diamankan secara fisik, tidak termasuk dokumen kertas dalam bentuk cetak;

c. ketika melakukan perjalanan melewati jaringan publik oleh IBM;

d. ketika sedang ditransfer dari sistem IBM kepada Klien;

e. ketika ditransmisikan secara nirkabel oleh IBM; dan

f. yang disimpan oleh IBM di server dan basis data.

4. Keamanan Jaringan

IBM menggunakan versi perangkat lunak keamanan sistem terbaru yang wajar seperti *firewall*, *proxy*, *firewall* dan antarmuka aplikasi web. Perangkat lunak tersebut harus mencakup perlindungan *malware* dan definisi virus dan *patch* yang cukup baru. Sesuai dengan standar perusahaan, perangkat lunak antivirus akan dipasang di tempat kerja, server, dan titik akhir terkait yang dapat dikerjakan secara teknis dan perangkat lunak dikelola untuk kebijakan perusahaan dengan solusi manajemen internal.

IBM memantau SaaS IBM untuk mendeteksi dan mengidentifikasi insiden keamanan secepat mungkin. IBM akan mengelola, setidaknya, peralatan dan pencegahan deteksi intrusi standar industri, pemantauan dan proses tanggapan dengan cara yang dirancang untuk mengidentifikasi kerentanan dan risiko internal maupun eksternal yang dapat menyebabkan pengungkapan, penyalahgunaan, alterasi, atau pemusnahan konten Klien atau sistem informasi yang tidak sah yang digunakan untuk menyampaikan layanan kepada Klien.

IBM berlangganan layanan inteligensi kerentanan atau penasihat keamanan informasi dan sumber yang sesuai lainnya yang memberikan informasi saat ini mengenai kerentanan sistem. IBM menjalankan penilaian dan perbaikan kerentanan berkala pada jaringannya.

IBM memantau SaaS IBM untuk mendeteksi, mengidentifikasi, mengetahui, dan menyelesaikan Insiden Keamanan.

IBM memvalidasi ketersediaan, integritas dan keefektifan infrastruktur keamanan jaringan di mana SaaS IBM tersedia melalui proses manajemen rilis.

5. Manajemen Insiden dan Pemberitahuan

Tim IBM Watson Health bekerja bersama dengan tim IBM Cybersecurity Incident Response, suatu tim global yang mengelola penerimaan, investigasi dan koordinasi internal mengenai insiden keamanan yang berkaitan dengan tawaran IBM, dan untuk mengimplementasikan langkah-langkah pencegahan yang diperlukan untuk mengurangi masalah keamanan yang berkaitan dengan perangkat lunak. "Insiden Keamanan" adalah akses, penggunaan, penyingkapan, modifikasi, atau gangguan pada operasi sistem atau data yang tidak sah yang berhasil di suatu sistem informasi yang digunakan oleh IBM untuk menyediakan SaaS IBM. Apabila Insiden Keamanan ditemukan (melalui pemindaian rutin, peringatan, peristiwa ambang batas dll.), IBM akan menginformasikan dan memberi tahu Klien:

a. mengenai setiap Insiden Keamanan yang dikonfirmasi yang melibatkan konten Klien sesegera mungkin dan tidak lebih dari 2 hari kerja setelah investigasi dan konfirmasi Insiden Keamanan tersebut;

b. dengan segera memenuhi setiap permintaan untuk akses ke, atau informasi mengenai, konten Klien apa pun dari kantor pemerintahan mana pun (termasuk agen perlindungan data atau agensi penegak hukum mana pun) kecuali apabila dilarang oleh hukum atau perintah yang relevan; dan

c. kecuali sebagaimana yang diizinkan dalam pasal yang berjudul Pengendalian Akses pada SBCA ini, sebelum setiap pengungkapan atau transfer, atau akses ke, konten Klien kepada atau oleh pihak ketiga.

6. Pencatatan

IBM mempertahankan, sesuai dengan kebiasaan umum dan kebijakan IBM serta kebiasaan umum industri yang diterima secara umum, pemantauan sistem yang wajar untuk penggunaan yang tidak sah atas atau akses ke Data yang Diproses Klien. Pelanggaran logon aktual atau percobaan serta pelanggaran akses akan dicatat.

IBM memelihara catatan semua permintaan akses dan catatan aktivitas akses untuk semua sistem yang menyimpan, mengakses, memproses dan mentransmisikan Data Kesehatan dan Klien selama diperlukan oleh HIPAA dan Peraturan Perundang-undangan Data yang Berlaku IBM.

Catatan dan laporan mencakup, sedikitnya: (i) semua percobaan login, baik yang berhasil maupun tidak, termasuk informasi pengidentifikasian yang wajar; (ii) semua perubahan konfigurasi sistem dan jaringan, termasuk pemasangan aplikasi, perubahan manajemen pengguna, dan pemberitahuan untuk izin akses file; (iii) percobaan akses sumber, baik yang berhasil maupun tidak, termasuk percobaan untuk mengakses file, jaringan bersama, catatan, atau sumber lainnya apa pun; dan (iv) unduhan data, termasuk tipe konten data dan protokol akses yang digunakan untuk mengunduh.

7. Pengembangan Aplikasi Perangkat Lunak dan Manajemen Perubahan

IBM mematuhi pengembangan aplikasi aman dan kebiasaan umum pengkodean yang melindungi integritas aplikasi produksi dan kode sumber terkait dari modifikasi yang tidak sah dan tidak teruji.

IBM mematuhi proses manajemen perubahan yang mencakup (a) pencatatan dan persetujuan perubahan formal, dan prosedur penangguhan; dan (b) pengujian yang sesuai atas perubahan tersebut, termasuk pengujian penerimaan pengguna apabila sesuai, serta pengujian keamanan.

IBM mematuhi proses manajemen tambalan (*patch*) yang mencakup tambalan (*patch*) pengujian sebelum pemasangan pada semua sistem yang digunakan untuk menyimpan, mengakses dan mentransmisikan konten Klien atau digunakan untuk menyampaikan layanan, termasuk SaaS IBM, kepada Klien.

IBM mensyaratkan bahwa administrator sistem memelihara informasi yang terbaru, akurat dan lengkap mengenai konfigurasi semua sistem imformasi yang digunakan untuk menyimpan, mengakses, dan mentransmisikan konten Klien.

8. Keamanan Lingkungan dan Fisik

Platform IBM Watson Health Core disebarkan pada infrastruktur dataIBM SoftLayer. IBM SoftLayer memelihara keamanan lingkungan dan fisik, kontrol akses, kontrol dan proses untuk melindungi data Klien dari pelanggaran atau pengaruh manusia, lingkungan, dan teknis.

Akses umum ke fasilitas di mana SaaS IBM diselenggarakan dikontrol oleh penggunaan sistem akses kartu. Kamera *closed circuit television* (CCTV) dipasang di seluruh situs dan dipantau oleh personel keamanan. Pintu akses terpilih diberi alarm dan personel keamanan memantau alarm ini.

Akses ke area terkontrol terbatas melalui penggunaan akses kartu dan/atau verifikasi biometrik tambahan. Semua individu tanpa akses yang sah ke area terkontrol harus mendaftar dan dikawal oleh individu dengan akses area terkontrol yang disetujui. Semua pintu keluar darurat area terkontrol memiliki alarm bunyi dan personel keamanan memantau alarm ini. Verifikasi berkala bahwa alarm berfungsi dijalankan, didokumentasikan, dan disimpan. Hak akses ke area terkontrol divalidasi kembali secara penuh empat kali dalam satu tahun. Akses ke area terkontrol dicabut setelah pengakhiran ketenagakerjaan.

Fasilitas dilindungi dari faktor lingkungan seperti kebakaran, air, dan panas dengan alarm kebakaran, pemadam kebakaran, alarm asap, serta sistem pemadaman dan penahan kebakaran. Fasilitas dilindungi dari gangguan atau kegagalan daya melalui sistem Suplai Daya Bebas Gangguan (*Uninterruptible Power Supply* - "UPS") dan generator cadangan yang dipelihara dan diuji secara berkala.

Laporan dan informasi kepatuhan IBM SoftLayer dapat ditemukan di: http://www.softlayer.com/compliance.

9. Kesinambungan Operasi Bisnis

IBM memiliki rencana kesinambungan bisnis dan pemulihan bencana yang dirancang untuk memelihara tingkat layanan yang konsisten dengan kewajibannya berdasarkan Perjanjian. Rencana kesinambungan bisnis dan pemulihan bencana tersebut akan diperbarui dan diuji secara berkala (setidaknya sekali dalam setahun). IBM akan mengimplementasikan semua perubahan yang wajar untuk rencana kesinambungan bisnis dan pemulihan bencana yang diperlukan agar tetap mematuhi praktik industri yang diterima secara umum, dalam setiap kasus tanpa gangguan yang tidak wajar terhadap SaaS IBM atau lingkungan produksi yang digunakan oleh Klien.

Apabila bencana muncul dan mengakibatkan SaaS IBM tidak tersedia untuk Klien, IBM akan segera memberi tahu Klien dan mengaktifkan rencana kesinambungan bisnis dan/atau pemulihan bencana. Ketika bencana dinyatakan, sasaran kesinambungan bisnis SaaS IBM adalah untuk memulihkan akses Klien ke SaaS IBM sebagai berikut: Dalam peristiwa terjadinya penghentian sumber daya, Sasaran Waktu Pemulihan (*Recovery Time Objective* - "RTO") untuk memulihkan lingkungan produksi IBM Watson Health adalah dalam 36 jam sejak pernyataan bencana. Sasaran Titik Pemulihan (*Recovery Point Objective* - "RPO") tidak lebih dari 24 jam sejak hilangnya konten Klien dalam lingkungan produksi. Sasaran kesinambungan bisnis solusi Watson Health spesifik dapat bervariasi.

Pendekatan IBM untuk pemulihan bencana terdiri atas beberapa pusat data di area geografi yang tersebar.

Semua pusat data IBM SoftLayer memelihara beberapa umpan daya, tautan fiber, generator terdedikasi, dan cadangan baterai. Pusat data disusun dari peralatan dan perangkat keras industri terdepan yang memberikan tingkat kinerja, keandalan, dan interoperabilitas tertinggi. Semua komponen pusat data untuk mencakup, daya n+1 redundansi dan sumber pendinginan sebagai contoh, diperiksa untuk memelihara kestabilan di dalam pusat data.

10. Kepatuhan

Praktik keamanan IBM didasarkan pada ISO 27001-27002. Praktik ini memberikan struktur kontrol untuk, namun tidak terbatas pada, Analisis Risiko, Keamanan Fisik, Perencanaan Darurat, Investigasi, Perlindungan Informasi, Edukasi, Perlindungan Data, dan Operasi.

IBM meninjau aktivitas yang berkaitan dengan keamanan dan kerahasiaan untuk mematuhi praktik keamanan IBM.

IBM mematuhi Peraturan Perundang-undangan Data yang Berlaku IBM dalam Yurisdiksi Dalam Cakupan.

Penanganan yang tepat atas informasi rahasia Klien juga diperlukan berdasarkan Pedoman Perilaku Bisnis IBM di mana semua karyawan harus meninjau (dan membuktikan secara resmi peninjauan mereka) secara tahunan.

11. Lain-lain

IBM akan memastikan bahwa perjanjiannya dengan semua subkontraktor dan/atau pihak ketiga yang terlibat dalam penyampaian SaaS IBM memiliki syarat-syarat yang setidaknya melindungi konten Klien sama baiknya dengan syarat-syarat dalam SBCA ini, dan setiap Dokumen Terkait yang berlaku, masing-masing sejauh syarat-syarat tersebut berlaku pada layanan yang dijalankan oleh subkontraktor dan/atau pihak ketiga tersebut.

This document is made in the English and Indonesian languages. To the extent permitted by the prevailing law, the English language of this document will prevail in the case of any inconsistencies or differences of interpretation with the Indonesian language text of this document.

Dokumen ini dibuat dalam bahasa Indonesia dan bahasa Inggris. Sepanjang diperbolehkan oleh hukum yang berlaku, dalam hal terdapat ketidaksesuaian atau perbedaan penafsiran dengan teks bahasa Indonesia dari dokumen ini, maka teks dalam bahasa Inggris yang akan berlaku.