IBM Kullanım Koşulları –
Hizmet Olarak Sunulan Yazılımlara Özgü Olanak Koşulları

IBM Watson Health Core

Kullanım Koşulları, bu IBM Kullanım Koşulları – Hizmet Olarak Sunulan Yazılımlara Özgü Olanak Koşullarından ("Hizmet Olarak Sunulan Yazılımlara Özgü Olanak Koşulları") ve aşağıdaki URL adresinde bulunan IBM Kullanım Koşulları - Genel Koşullardan ("Genel Koşullar") oluşur: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Çelişki durumunda, Hizmet Olarak Sunulan Yazılımlara Özgü Olanak Koşulları, Genel Koşullara göre öncelikli olarak uygulanır. Müşteri, IBM Hizmet Olarak Sunulan Yazılımlarına erişerek ya da IBM Hizmet Olarak Sunulan Yazılımlarını kullanarak veya sipariş ederek bu Kullanım Koşullarını kabul etmiş olur.

Kullanım Koşulları, uygulanabilir olduğu şekilde, IBM Uluslararası Passport Advantage Sözleşmesine, IBM Uluslararası Passport Advantage Express Sözleşmesine veya Seçilmiş IBM Hizmet Olarak Sunulan Yazılımları İçin IBM Uluslararası Sözleşmesine ("Sözleşme") tabidir ve Kullanım Koşulları, bunlar ile birlikte taraflar arasındaki sözleşmenin tamamını oluşturur.

1. IBM Hizmet Olarak Sunulan Yazılımları

Aşağıdaki IBM Hizmet Olarak Sunulan Yazılımları, Hizmet Olarak Sunulan Yazılımlara Özgü Olanak Koşulları kapsamında yer alır:

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

2. Ücret Ölçüleri

IBM Hizmet Olarak Sunulan Yazılımları, İşlem Belgesinde belirtilen şekilde aşağıdaki ücret ölçülerinden biri kapsamında satılır:

a. **Erişim** – IBM Hizmet Olarak Sunulan Yazılımlarının edinilebileceği bir ölçü birimidir. Erişim, IBM Hizmet Olarak Sunulan Yazılımlarını kullanmaya ilişkin haklardır. Müşterinin, Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca IBM Hizmet Olarak Sunulan Yazılımlarını kullanabilmesi için tek bir Erişim yetkisi edinmesi gerekir.

b. **Tekil Öğe** – IBM Hizmet Olarak Sunulan Yazılımlarının edinilebileceği bir ölçü birimidir. Tekil Öğe, tek nesne veya kişi olabilir. Müşteri, Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca IBM Hizmet Olarak Sunulan Yazılımı tarafından işlenen veya yönetilen her Tekil Öğeyi kapsam dahiline alabilmek için yeterli sayıda yetki edinmelidir.

   Bu IBM Hizmet Olarak Sunulan Yazılımının amaçları doğrultusunda, Tekil Öğe, verileri IBM Hizmet Olarak Sunulan Yazılımı tarafından yönetilen bir kişi, aygıt veya mobil uygulamayı içerir.

c. **Eşgörünüm**, IBM Hizmet Olarak Sunulan Yazılımlarının edinilebileceği bir ölçü birimidir. Bir Eşgörünüm IBM Hizmet Olarak Sunulan Yazılımlarının belirli bir yapılandırmasına erişimdir. Müşterinin Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi sırasında erişime ve kullanıma açılan her IBM Hizmet Olarak Sunulan Yazılımları Eşgörünümü için yeterli sayıda yetki edinilmiş olmalıdır.

3. Ücretler ve Faturalama

IBM Hizmet Olarak Sunulan Yazılımı için ödenecek tutar bir İşlem Belgesinde belirtilir.

3.1 Kısmi Aylık Ücretler

Bir kısmi aylık ücret, İşlem Belgesinde belirtilmiş olduğu şekilde, oranlanmış olarak değerlendirilebilir.

3.2 Limit Aşımı Ücretleri

Ölçüm süresi boyunca Müşterinin IBM Hizmet Olarak Sunulan Yazılımlarını gerçek kullanımı Yetki Belgesinde belirtilen yetkiyi aşarsa, İşlem Belgesinde belirtilen şekilde, Müşteri limit aşımı miktarı için faturalandırılacaktır.

4. Süre ve Yenileme Seçenekleri

IBM Hizmet Olarak Sunulan Yazılımlarının süresi, Sipariş Belgesinde belgelenmiş olduğu şekilde, Müşterinin IBM Hizmet Olarak Sunulan Yazılımlarının Pilot işletim ortamına erişiminin etkinleştirildiğinin IBM tarafından Müşteriye bildirildiği tarihte başlar. Tekil Öğelerin yetkilerine yönelik abonelik süresi, IBM'in Üretim işletim ortamına erişimini Müşteriye bildirdiğinde başlar. Sipariş Belgesinde IBM Hizmet Olarak Sunulan Yazılımlarının, otomatik olarak mı yenileneceği, sürekli kullanım esasına göre mi sürdürüleceği, yoksa belirlenen sürenin sonunda sona mı ereceği belirtilir.

Otomatik yenileme için: müşteri, sürenin sona erme tarihinden en az doksan (90) gün önce yazılı olarak olanağı kullanımını yenilemeyeceğini bildirmediği sürece, IBM Hizmet Olarak Sunulan Yazılımları, Yetki Belgesinde belirtilen süreye uygun olarak kendiliğinden yenilenir.

Sürekli kullanım için: müşteri, sürenin sona erme tarihinden doksan (90) gün önce yazılı olarak olanağı kullanımını sona erdireceğine ilişkin bildirim gönderinceye kadar, IBM Hizmet Olarak Sunulan Yazılımları aylık kullanım esasına göre kullanılmaya devam eder. IBM Hizmet Olarak Sunulan Yazılımları, doksan günlük bu bildirim süresinin sona ermesini izleyen takvim ayının sonuna kadar kullanılmaya devam edilebilir.

5. Teknik Destek

IBM, teknik destek iletişim bilgilerini, bakım sürelerini ve diğer bilgi ve süreçleri içeren IBM Hizmet Olarak Sunulan Yazılımları Destek El Kitabı'nı sağlayacaktır. Teknik destek iletişim bilgilerine ve destek operasyonları ile ilgili diğer bilgilere şu adresten ulaşılabilir: https://support.ibmcloud.com.

IBM Hizmet Olarak Sunulan Yazılımlarına yönelik teknik destek ve basit yapılandırma istekleri, elektronik iletim yoluyla sağlanır. Teknik Destek, IBM Hizmet Olarak Sunulan Yazılımları ile birlikte sunulur ve ayrı bir olanak olarak sağlanmaz.

Bir sorun veya olay bildirilirken herhangi bir belgeye veya bilgiye yasal düzenlemeye tabi sağlık verileri ve özel nitelikli kişisel veriler dahil hiçbir Kişisel Veri dahil edilmemelidir.

6. Tanımlar

Geçerli Yasalar – Bir devlet makamı tarafından düzenlenmiş herhangi bir yasa, tüzük veya yürürlüğe konulan yasa, kural, yönetmelik, direktif, emir, kararname veya diğer gereksinim ya da bu Kullanım Koşullarının uygulanması için geçerli olan, herhangi bir genel kabul görmüş sektör standardını ifade eder.

Uygulama Programı Arabirimi – yazılım uygulamalarının oluşturulması için bir dizi yordam, protokol ve aracı ifade edecektir. Uygulama Programı Arabirimi, yazılım bileşenlerinin nasıl etkileşim kurması gerektiğini belirtir. Uygulama Programı Arabirimleri, grafik kullanıcı arabirimi bileşenlerinin programlanması sırasında kullanılır.

Yetkili Yönetici – platformun güvenilir şekilde çalışmasını ve bakımını yönetmekten sorumlu herhangi bir Müşteri çalışanı, onaylı Müşteri yüklenicisi, kişi veya gruptur. Sorumluluklar; yapılandırma, destek, kullanıcı ve hesap yönetimini içerebilir. Yönetici, Watson Health sisteminde bir çalışma oluşturmaktan sorumlu bir klinik araştırmacı da olabilir.

Yetkili Tekil Öğe – Watson Health Core olanağına veri göndermek için erişim haklarına erişim verilmiş herhangi bir yetkili kişi, mobil uygulama veya aygıttır. Buna Müşteri, çalışma katılımcıları, müşteriler veya Müşterinin hastaları dahil olabilir.

Müşterinin Geçerli Veri Koruma Yasaları – Müşterinin Taraflar arasındaki Sözleşme, İlgili Belgeler, geçerli Hizmet Tanımları, Sipariş Belgeleri ve Hizmet Bildirimleri kapsamında Müşterinin yükümlülüklerinin yerine getirilmesi için geçerli olan Veri Koruma Yasalarını ifade eder.

Müşteri Verileri – bir üçüncü kişinin sağlık aygıtından alınan herhangi bir veri dahil, ister Müşterinin kendi verileri ister Müşterinin müşterisi ya da üçüncü bir kişi adına veya onun tarafından girilen veriler olsun, Müşteri tarafından veya Müşteri için IBM Hizmet Olarak Sunulan Yazılımlarında yer alan herhangi bir veri girdisini ifade eder.

Veri Koruma Yasaları – veri koruma, gizlilik veya güvenlik ile ilgili herhangi bir Geçerli Yasayı ifade eder.

İlgili kişi – Kişisel Verilerin ilgili olduğu tanımlanmış veya tanımlanabilir kişiyi ifade eder.

Belirlenmiş Veri Merkezi – Müşterinin IBM Hizmet Olarak Sunulan Yazılımlarının eşgörünümünü uygun olduğu durumda çalıştıran, İşlem Belgesinde birincil ve olağanüstü durum kurtarma verileri için belirtilmiş veri merkez(ler)ini ifade eder.

Sağlık Verileri – görüntüler dahil, sağlıkla ilgili Kişisel Veri niteliğindeki herhangi bir veriyi veya bilgiyi ifade eder.

Etkinleştirilen Sağlık Verileri, – IBM Hizmet Olarak Sunulan Yazılımları ile ilgili olarak, IBM Hizmet Olarak Sunulan Yazılımlarının, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasasını (HIPAA) (HITECH Yasası ile değiştirildiği şekliyle) uygulayan yönetmeliklerde Bölüm 164, Alt Bölüm A ve C'de belirtilen uygulama belirtimleri dahil olmak üzere, Sağlık Verileri için Kapsam Dahilindeki Yetkili Mahkemelerde geçerli güvenlik ve gizlilik standartlarına, yasalarına ve yönetmeliklerine ve Sağlık Verileriyle ilgili diğer Geçerli Yasalara uyma yeteneğini ifade eder. Ancak bu, IBM'in bir İş Ortağı veya Veri Sorumlusu olarak hareket ettiği anlamına gelmez.

HIPAA – 2009 Yılı Amerikan Kurtarma ve Yeniden Yatırım Yasasının Ekonomik Klinik Sağlık için Sağlık Bilgi Teknolojileri Yasası ("HITECH Act") ve Amerika Birleşik Devletleri Sağlık ve İnsan Hizmetleri tarafından 45 sayılı Federal Düzenlemeler Yasası, Bölüm 160 ve 164'te Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası kapsamında yayınlanan belirli yönetmelikler ve Ekonomik Klinik Sağlık için Sağlık Bilgi Teknolojileri Yasasına uygun olarak yayınlanan belirli yönetmelikler ile değiştirildiği şekliyle, 1996 yılı Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasasını ifade eder.

IBM'in Geçerli Veri Koruma Yasaları – Müşterinin Taraflar arasındaki Sözleşme, İlgili Belgeler ve geçerli Hizmet Tanımları, Sipariş Belgeleri ve Hizmet Bildirimleri kapsamında IBM'in yükümlülüklerinin yerine getirilmesi için geçerli olan Veri Koruma Yasalarını ifade eder.

IBM Personeli – (a) IBM, IBM'in Bağlı Kuruluşları ve IBM'in alt yüklenicileri ve bunların her birinin çalışanını; ve (b) herhangi bir üçüncü kişi yükleniciyi ifade eder; her iki durumda da bunlar, Sözleşmeye ve geçerli İlgili Belgelere uygun şekilde IBM adına hizmetleri yerine getiren veya IBM'in, Müşterinin Kişisel Verilerine erişimi yetkilendirdiği kişilerdir.

Kapsam Dahilindeki Ülkeler – 28 Avrupa Birliği Üye Devleti'ni, İsviçre'yi ve IBM'in zaman zaman bu listeye ekleyebileceği ülkeleri ifade eder.

Kişisel Veriler veya **Kişisel Veriler** – tanımlanmış veya tanımlanabilir bir kişi ile ilgili olan, elektronik ve kağıt kayıtları dahil, herhangi bir ortamda veya biçimde olan bilgileri ifade eder; "tanımlanabilir bir kişi", özellikle kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya birden fazla etkene atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen kişidir.

İşlem ve onun **işleme** gibi değişkenleri (büyük veya küçük harfle) - otomatik yöntemlerle olsun veya olmasın veriler üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, depolama, uyarlama veya değiştirme, alma, danışma, kullanma, iletim yoluyla ifşa, yayma veya başka şekilde sağlama, uyumlu hale getirme veya birleştirme, engelleme, silme veya imha etme gibi bir dizi operasyonu veya herhangi bir operasyonu ifade eder.

İşlenmiş Veri – Sözleşme, İlgili Belge ve/veya Hizmet Tanımı, Sipariş Belgesi ve Hizmet Bildirimine uygun şekilde IBM tarafından işlenen Sağlık Verileri ve Kişisel Veriler dahil, herhangi bir veri, gizli veya özel bilgiyi ifade eder.

Güvenlik Olayı – Güvenlik ve İş Sürekliliği Ekinde (SBCA) belirtilen anlamı taşır.

7. Hesap Yönetimi

IBM Hizmet Olarak Sunulan Yazılımına, yalnızca Müşterinin yetkili kullanıcıları **Yetkili Yöneticiler**" veya "**Yetkili Tekil Öğeler**") erişebilir. Müşteri, IBM Hizmet Olarak Sunulan Yazılımlarına erişmek için yetkilendirilmiş hesapları denetleyecektir. Bunlar; yetkili uygulamalar, Müşteri personeli, Müşterinin üçüncü kişi hizmet sağlayıcıları ve yüklenicilerini içerebilir. Müşteri, (i) herhangi bir yetkili kullanıcının kimliğini doğrulamak dahil ancak bununla sınırlı olmamak üzere tüm yetkili kullanıcılarını denetlemekten ve (ii) yalnızca yetkili kullanıcıların, IBM Hizmet Olarak Sunulan Yazılımlarına erişmesini sağlamaktan tek başına sorumludur.

Müşteriler, hastalar veya Müşterinin çalışma katılımcıları olan Yetkili Kişilere, yalnızca IBM Hizmet Olarak Sunulan Yazılımlarına veri yükleme amacıyla erişim tanınabilir. Bu durumda, söz konusu Yetkili Kişilerin IBM Hizmet Olarak Sunulan Yazılımlarına başka bir erişimi olmayacaktır.

8. Gizlilik ilkeleri

8.1 Genel Gereksinimler

Taraflar arasında olduğu gibi, Müşteri, tüm Müşteri Kişisel Verilerinin tek veri sorumlusudur ve Müşteri, IBM'i veri işleyen olarak görevlendirir. Geçerli Veri Koruma Yasaları uyarınca, Müşteri, IBM'in Müşteri Kişisel Verilerini işlemesiyle bağlantılı olarak IBM'e yönerge verme hakkına sahiptir.

IBM, Müşteri Kişisel Verilerini işlediği ölçüde,

a. IBM'in tüm Geçerli Veri Koruma Yasalarına uyacak; ve

b. Müşteri Kişisel Verilerini, aşağıdaki durumlar dışında, diğer kaynaklardan alınan veriler ile karıştırmayacaktır:

- Müşteri tarafından aksi yönde özellikle yönerge verilmedikçe, başka bir amaç için değil, IBM Hizmet Olarak Sunulan Yazılımlarını sağlamak için gerektiği şekilde: veya
- Bu Kullanım Koşullarının ve Güvenlik ve İş Sürekliliği Ekinin koşullarına uygun olarak.

Müşteri, Müşteri Kişisel Verilerini işlediği ölçüde,

a. Müşterinin tüm Geçerli Veri Koruma Yasalarına uyacak;

b. Müşterinin Bağlı Kuruluşları, hastaları, son kullanıcıları, İlgili Kişileri ve/veya diğer Müşteri üçüncü kişileri ile Müşteri arasındaki tüm iletişimlerden sorumlu olacaktır;

c. Veri işleyen olarak IBM'in ve onun alt işleyenlerinin herhangi bir Müşteri Kişisel Verisini işlemesine olanak tanıyan veri sorumlularıyla veri işleme sözleşmeleri imzalayacaktır; ve

d. IBM'in tek iletişim noktası işlevi görecek ve IBM'in diğer veri sorumluları olan Müşteri Bağlı Kuruluşlarının yönergelerinin veya isteklerinin dahili olarak koordine edilmesinden, incelenmesinden ve sunulmasından tek başına sorumlu olacaktır. IBM, veri sorumlusu atayan herhangi bir Müşteri Bağlı Kuruluşuyla ilgili bilgiyi veya bildirimi Müşteriye sağladığında, IBM söz konusu bilgiyi veya bildirimi sağlama yükümlülüğünden kurtulacaktır. IBM, Müşteri olmayan bir veri sorumlusu atayan bir Müşteri Bağlı Kuruluşu tarafından doğrudan sağlanan herhangi bir yönergeyi reddetme hakkına sahiptir.

Taraflardan hiçbiri, diğer tarafın Geçerli Veri Koruma Yasalarını ihlal etmesini gerektirmeyecektir.

8.2 Müşteri Verilerine İlişkin Haklar

Müşteri, (a) IBM Hizmet Olarak Sunulan Yazılımlarına gireceği verilerin sahibi olduğunu veya (b) bu Kullanım Koşullarında veya Sözleşmede belirtilen koşullara uygun şekilde veya IBM'in IBM Hizmet Olarak Sunulan Yazılımlarını başka şekilde sağlaması için gerektiği şekilde, IBM'e Müşteri Verilerine erişmek ve bunları kullanmak ve ifşa etmek için gereken tüm hakları, izinleri, rızaları ve yetkileri edindiğini ve tüm bunların korunmasından sorumlu olduğunu beyan ve garanti eder. Müşteri, Müşteri verilerinin yalnızca (a) Amerika Birleşik Devletleri'nde mukim kişilerle ilgili olacağını ve dolayısıyla yalnızca ABD'de bulunan veri merkezinde yer alan IBM Hizmet Olarak Sunulan Yazılımlara girişinin yapılacağını veya (b) yalnızca bir veya birden fazla Kapsam Dahilindeki ülkede mukim kişilerle ilgili olacağını ve dolayısıyla yalnızca Belirlenmiş Veri Merkez(ler)inde yer alan IBM Hizmet Olarak Sunulan Yazılımlara girişinin yapılacağını beyan ve garanti eder.

8.3 Veri Hizmetleri ve Sorumlulukları

a. Müşteri, i) her biri Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası ve/veya diğer Geçerli Veri Koruma Yasalarına ilişkin benzer koşullar kapsamında tanımlandığı şekilde, Müşterinin "sağlık hizmetleri operasyonları" veya "araştırmayı" oluşturan etkinliklerle bağlantılı olarak, yalnızca Müşteri Verileri üzerinde analitik gerçekleştirmeyi veya IBM'den bunu yapmasını istemeyi; ve ii) Müşterinin, yalnızca bu ve diğer herhangi bir Müşterinin Geçerli Veri Koruma Yasası kapsamındaki tüm ilgili gereksinimlere (örn: gerektiğinde Kurumsal İnceleme Kurulunun belirlemesi veya feragatı) uygun olarak, Müşteri Verilerini kullanmayı veya IBM'e Müşteri Verilerini kullanması konusunda yönerge vermeyi kabul eder.

b. Müşteri, Müşteri Verilerinin Müşteri, IBM ve IBM'in izin verilen alt yüklenicileri tarafından bu Kullanım Koşulları ve Sözleşme kapsamında tasarlandığı şekilde, IBM Hizmet Olarak Sunulan Yazılımlarına girilmesi, kullanılması ve ifşa edilmesi amacıyla, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası ve diğer tüm geçerli veri gizliliği ve güvenlik yasaları, kuralları ve yönetmelikleri dahil ancak bunlarla sınırlı olmamak üzere, geçerli her Kapsam Dahilindeki Ülkedeki Müşteri Geçerli Yasalarının gerektirdiği tüm ruhsatları, rızaları, yetkileri ve izinleri almaktan tek başına sorumludur. IBM'in, söz konusu ruhsatlar, rızalar, yetkiler ve izinlerin alınması veya gerekli olması durumunda izlemeye ilişkin hiçbir sorumluluğu olmayacaktır.

c. Müşteri, IBM Hizmet Olarak Sunulan Yazılımlarına girilen tüm Müşteri verilerinin, Amerika Birleşik Devletleri'nde veya geçerli bir Kapsam Dahilindeki Ülkede mukim kişilerle ilgili verilerle sınırlı olmasını sağlamaktan tek başına sorumludur.

d. IBM, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası ve Kapsam Dahilindeki Ülkelerden alınan verilerle ilgili IBM'in diğer Geçerli Veri Koruma Yasaları konusunda eğitilmiş personelin bulunduğu destek merkezlerine sahiptir.

8.4 Güvenlik Önlemleri ve Güvelik Olayları

a. IBM, Müşteri Kişisel Verilerini yetkisiz kullanım veya erişim, yanlışlıkla kaybetme, hasar, değişiklik, imha, çalınma veya yetkisiz ifşadan korumak amacıyla, bu Kullanım Koşullarında ve Güvenlik ve İş Sürekliliği Ekinde belirtilen veya bunlar içinde atıfta bulunulan herhangi bir belirli güvenlik yükümlülüğü ve kurumsal süreç ve prosedürler dahil olmak üzere, teknik ve kurumsal önlemleri uygulayacak, sürdürecek ve bunlara uyacaktır.

b. IBM'in Müşterinin İşlenmiş Verilerinin dahil olduğu bir Güvenlik Olayından haberdar olması durumunda (Güvenlik ve İş Sürekliliği Eki tarafından tanımlandığı şekilde), IBM, Müşteriyi Güvenlik ve İş Sürekliliği Ekine ve IBM'in Geçerli Veri Koruma Yasalarına uygun şekilde bilgilendirecektir. Söz konusu bilgilendirme, ilgili Güvenlik Olayından etkilenen (varsa) herhangi bir İlgili Kişinin veya Müşterinin üzerindeki bilinen herhangi bir etkiyle ilgili bilgileri ve ayrıca, IBM tarafından alınan veya önerilen düzeltici eylemi içerecektir.

8.5 Sorguların ve Şikayetlerin Alınması

IBM, IBM Watson Sağlık Verisi Gizliliği Görevlisinin, Müşteri Kişisel Verileriyle ilgili olarak IBM'in aşağıda belirtilenlerden aldığı herhangi bir sorgu, iletişim veya şikayeti aldıktan sonra en geç beş (5) gün içinde, IBM Geçerli Veri Koruma Yasalarının izin verdiği ölçüde, Müşteriyi derhal yazılı olarak bilgilendirecektir:

a. IBM tarafından işlenen İlgili Kişi hakkında Kişisel Verilerle ilgili herhangi bir İlgili Kişiden. Müşteri, İlgili Kişilerden gelen bu tür isteklere yanıt verecektir ve IBM, Müşterinin söz konusu isteklere yanıt vermesine yardımcı olma konusunda Müşterinin makul yönergelerine uyacaktır. IBM'in Geçerli Yasalarının gerektirmesi durumunda, IBM, bu tür bir yanıtı önceden Müşteriye bildirmesi ve ilgili yanıtın biçimi ve içeriği ile ilgili olarak Müşteri ile makul şekilde koordinasyon sağlaması kaydıyla, IBM'in Geçerli Yasalarının izin vermesi halinde veya mümkün olan başka şekilde ilgili isteklere doğrudan yanıt verebilir;

b. i) IBM'in ilgili talepleri, bir devlet kurumundan IBM tarafından ifşayı gerektiren bir mahkeme celbi veya benzer bir yasal belge ile veya Geçerli Veri Koruma Yasasının gerektirdiği başka şekilde aldığı ilgili taleplere doğrudan yanıt verebilmesi ii) yasaların izin verdiği veya başka şekilde mümkün olduğu ölçüde, IBM'in Müşteriyi söz konusu ifşayla ilgili olarak önceden bilgilendirmesi ve ilgili yanıtın biçimi ve içeriği ile ilgili olarak Müşteri ile makul şekilde koordinasyon sağlaması kaydıyla, herhangi bir Müşteri Kişisel Verisinin IBM tarafından işlenmesiyle ilgili herhangi bir hukuki veya yasal düzenleme makamı.

8.6 Müşteri Kişisel Verilerinin İşlenmesi

IBM, Müşteri Kişisel Verilerinin ifşasını, Hizmetleri sağlamada yardımcı olmasının gerekebileceği ilgili IBM personeli ile sınırlandıracaktır.

IBM, IBM'in Müşteri Kişisel Verilerini, Geçerli Yasaya uygun şekilde değiştirmesini, düzeltmesini, silmesini veya engellemesini gerektiren, Müşteriden alınmış herhangi bir makul isteğe uyacaktır.

Taraflardan herhangi birinin talebi üzerine, IBM, Müşteri veya onların bağlı kuruluşları, Müşteri Kişisel Verilerinin korunması için yasanın gerektirdiği standart sözleşmeleri imzalayacaktır. Taraflar, söz konusu sözleşmelerin, Taraflar arasındaki iddiaların amacı doğrultusunda, bu Sözleşmede yer alan sınırlamalar ve sorumluluk sınırlarına tabi olacağını kabul ederler (ve ilgili bağlı kuruluşlarının kabul etmesini sağlayacaklardır). Taraflar, Geçerli Veri Koruma Yasalarının gerektirebileceği şekilde, karşılıklı olarak kabul edilen koşulları veya sözleşmeleri düzenlemek (veya söz konusu Tarafın ilgili Bağlı Kuruluşlarının bunları düzenlemesini sağlamak) ve bunlara uymak üzere işbirliği yapacaktır.

8.7 Müşteri Kişisel Verilerinin İadesi

Sözleşmenin sona ermesi veya sona erdirilmesi üzerine IBM, herhangi bir Müşterinin Özel Bilgilerini ve Müşterinin Kişisel Verilerini kullanmaya veya işlemeye son verecek ve tüm IBM Personelinin de son vermesini sağlayacaktır, ayrıca Müşterinin tercihi ve talebi üzerine, aşağıda belirtilenleri gerçekleştirecektir:

a. i) IBM'in elektronik olarak kaydettiği tüm Müşterinin Özel Bilgilerini ve Müşteri Kişisel Verilerini, Müşterinin makul olarak isteyebileceği biçimde ve depolama ortamında derhal iade edecektir; ve ii) Müşterinin alındığına dair teyidi üzerine, kopyaları ve yedekleri dahil, Müşterinin Özel Bilgilerini ve Müşterinin Kişisel Verilerini silecek, imha edecek veya başka şekilde kalıcı olarak okunamaz veya

deşifre edilemez hale getirecektir. IBM, Müşterinin talebi üzerine gerçekleştirilen belirli etkinlikler (örneğin, Müşterinin Özel Bilgilerinin ve Müşterinin Kişisel Verilerinin belirli bir biçimde teslim edilmesi veya belirli şekilde imha edilmesi) ve depolama alanı maliyeti için ücret talep edebilir.

b. kopyaları ve yedekleri dahil, Müşterinin Özel Bilgilerini ve Müşterinin Kişisel Verilerini silecek, imha edecek veya başka şekilde kalıcı olarak okunamaz veya deşifre edilemez hale getirecektir.

8.8 İş Ortaklığı Sözleşmesi

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasasının gerektirdiği ve uygun olduğu ölçüde, IBM ve Müşteri, bir İş Ortaklığı Sözleşmesi imzalayacaktır. Bu sözleşme, IBM Hizmet Olarak Sunulan Yazılımlarının sağlanmasında, IBM'in Müşterinin İş Ortağı olarak yükümlülüklerini düzenleyecektir. IBM'in Sözleşme ve geçerliyse, İş Ortaklığı Sözleşmesi kapsamındaki açık yükümlülüklerine sınırlama getirmeden, Müşteri; IBM Hizmet Olarak Sunulan Yazılımlarıyla ilgili olarak Müşterinin kullanımı veya diğer etkinlikleri (Yetkili Kullanıcıların kullanımı veya diğer etkinlikleri dahil) için geçerli olan tüm Geçerli Yasaların ve lisanslama gereksinimlerinin geçerliliğini belirlemekten ve bunlara uymaktan sorumlu olduğunu kabul eder.

8.9 Avrupa Birliği Veri İşleme Eki

Müşterinin IBM'e Avrupa Birliği Kişisel Verilerini işleme talimatı vermesi durumunda, IBM ve Müşteri, isteğe bağlı maddeleri çıkararak, uygun şekilde, AB Model Maddeleri dahil, Veri İşleme Eklemesini düzenleyecektir.

9. IBM Hizmet Olarak Sunulan Yazılımları Olanağına İlişkin Ek Koşullar

9.1 Güvenlik

Bu IBM Hizmet Olarak Sunulan Yazılımı, IBM'in http://www.ibm.com/cloud/data-security adresinde sağlanan IBM Hizmet Olarak Sunulan Yazılımlarına ilişkin veri güvenliği ve gizliliği ilkelerine ve bu Kullanım Koşullarının Güvenlik ve İş Sürekliliği Ekinde ve aşağıda belirtilen tüm ek koşullara uygundur. IBM'in veri güvenliği ve gizliliği ilkelerinde yapılacak hiçbir değişiklik, IBM Hizmet Olarak Sunulan Yazılımlarının güvenliğini azaltmayacaktır.

IBM Watson Health Core, güvenlik ilkelerini, standartları ve süreçleri, ISO 27001 çerçevesine dayalı olarak, Hizmet Tanımında daha ayrıntılı olarak açıklandığı şekilde uygular. Çözüm, güvenlik yetenekleri arasında aşağıda belirtilenleri uygular:

a. Güvenli İşletim Bölgeleri

   IBM Watson Health Core, veri taşıma ve özel uygulama geliştirme gibi bulut bütünleştirme noktalarını yönetmek için birden fazla güvenlik alanını kullanarak, kapsamlı bir savunma stratejisi uygular.

b. Şifreleme

   Tüm Müşteri Verileri, atıl durumda veya kullanılmaktayken şifrelenir. IBM Watson Health Core olanağına/olanağından aktarılan tüm veriler şifrelenir. Paylaşılan hizmet, şifreleme anahtarı yönetimini içerir. Müşteri, IBM Watson Health Service ile Müşterinin proxy sunucusu arasındaki tüm ağın bağlanabilirliğinden ve kalitesinden sorumludur.

c. Güvenlik Olayı İzleme

   IBM, güvenlik bilgileri ve olay yönetimi, günlük yönetimi, olay inceleme, tehdit algılama ve güvenlik açığı yönetimi için güvenlik zekası platformundan yararlanır.

d. Kimlik Yönetimi

   - Watson Health Core, OpenID Connect'i kullanan büyük ölçekli hasta ve kullanıcı popülasyonları için açık standartlara ilişkin kimlik sağlayıcılarını destekler.
   - Watson Health Core, IBM'in kimlik sağlayıcısı olduğu kullanıcı popülasyonları için, kimlik doğrulamayı gerçekleştirmeye yönelik uygun dizin hizmetlerinden ve kimlik yönetimi yeteneklerinden yararlanır.

e. Güçlü Kimlik Doğrulama ve Görev Tabanlı Erişim

   - Watson Health Core, Tek Oturum Açma veya dizin hizmetlerini bütünleştirmek amacıyla, Müşterilere yönelik mekanizma olan SAML aracılığıyla kimlik doğrulamayı destekler.
   - Watson Health Core, gerektiğinde, güvenlik ilkelerini yönetmek için bir erişim yönetimi çözümünden ve ilgili bileşenlerden yararlanır.

- Watson Health Core, yazılım tabanlı, iki etkenli kimlik doğrulamayı destekler.
- Watson Health Core, gerektiği şekilde, görev tabanlı erişim denetimi sağlar. Watson Health Core, rol tabanlı erişime olanak tanıyan programa ilişkin uygulama programı arabirimleri aracılığıyla, çalışmanın, kullanıcı profillerinin, görevlerin ve kullanıcı gruplarının yapılandırılmasını destekler.

9.2 Tanımlama Bilgileri

Müşteri, IBM'in, IBM Hizmet Olarak Sunulan Yazılımlarının normal işletimi ve desteklenmesi kapsamında, takip ve diğer teknolojiler aracılığıyla Müşteriden (çalışanlarından ve yüklenicilerinden) IBM Hizmet Olarak Sunulan Yazılımların kullanımına ilişkin kişisel veriler elde edebileceğini bildiğini ve bu bilgilerin toplanmasını kabul eder. IBM, bunu kullanıcı deneyiminin iyileştirilmesi ve/veya Müşteriyle olan etkileşimlerin kişiselleştirilmesi amacıyla IBM Hizmet Olarak Sunulan Yazılımlarının etkinliğine ilişkin kullanım istatistikleri ve bilgileri toplamak için yapmaktadır. Müşteri, IBM'in elde edilen kişisel verileri, yukarıda belirtilen amaç uyarınca IBM, diğer IBM şirketleri ve bunların alt yüklenicileri içerisinde, IBM'in ve alt yüklenicilerinin iş yaptıkları herhangi bir yerde, uygulanabilir olan hukuka uygun olarak işlemesi için izin alacağını ya da almış olduğunu doğrular. IBM, Müşteri çalışanlarının ve yüklenicilerinin elde edilen kişisel verilere erişmeye, bunların güncellenmesine, düzeltilmesine ya da silinmesine ilişkin taleplerini karşılayacaktır.

9.3 Türetilen Yararlanma Lokasyonları

Geçerli olduğunda, vergiler hesaplanırken Müşterinin IBM Hizmet Olarak Sunulan Yazılımlarından yararlandığını belirttiği lokasyon(lar) esas alınacaktır. IBM, Müşteri tarafından IBM'e ek bilgiler sağlanmadıkça, IBM Hizmet Olarak Sunulan Yazılımları sipariş edilirken belirtilen iş adresini birincil Yararlanma lokasyonu varsayarak vergileri uygulayacaktır. Anılan bilgilerin güncel tutulmasından ve herhangi bir değişikliğin IBM'e sağlanmasından Müşteri sorumludur.

9.4 Kesintisiz Hizmet Sağlama

Müşteri, çözümde gerçekleştirilen ve IBM tarafından kesintisiz bulut hizmeti sağlama modelinde devreye alınan yeteneklere ve geliştirmelere hak kazanır.

9.5 Yedekleme ve Geri Yükleme

IBM Watson Health Core, sistem arızası durumunda hizmeti kurtarmak için üretim ortamındaki Müşteri Verilerinin (Veri Gölü ve Veri Havuzu depoları dahil) bilinen son iyi duruma yedeklemesini sağlar.

9.6 Yüksek Düzeyde Kullanılabilirlik

Üretim ortamında bulunan IBM Watson Health Core bileşenleri, iş yükü dağıtımını sağlamak ve tek hata noktasını ortadan kaldırmak üzere veritabanı sunucularının yedeklilik için kümelendiği, yüksek düzeyde kullanılabilirlik yapılandırmalarında uygulanır.

9.7 Olağanüstü Durum Kurtarma

IBM'in olağanüstü durum kurtarmaya yönelik yaklaşımı, Üretim ortamı için iş sürekliliği hedeflerine aşağıda belirtildiği şekilde ulaşmak amacıyla, dağıtılmış coğrafi alanlarda birden fazla veri merkezinden oluşur.

- Kurtarma Süresi Hedefi – olağanüstü durum ilanından itibaren 36 saat
- Kurtarma Noktası Hedefi - Müşteri içeriğinin kaybedilmesinden itibaren en fazla 24 saat

9.8 Ölçüm Araçları

IBM Hizmet Olarak Sunulan Yazılımları, taahhüt edilen hizmet seviyeleri doğrultusunda kullanılabilirliği veya kesintileri izlemek, ölçmek ve raporlamak için sentetik izleme çözümü kullanır. Bu çözüm, statik kullanılabilirlik ve işlemler için genel seviyede kullanıcı yanıtını ve kullanıcı deneyimini takip eder ve bunların benzetimini oluşturur.

IBM Hizmet Olarak Sunulan Yazılımları, aynı zamanda tüm çözüm genelinde ölçümler, olaylar ve uyarılar için bir dahili izleme sistemini kullanır.

9.9 Tanıtım

Müşteri, IBM'in bir basın veya pazarlama iletişiminde Müşteriyi IBM Hizmet Olarak Sunulan Yazılımlarının bir abonesi olarak kamuya açık bir şekilde referans verebileceğini kabul eder.

Ek A

1. IBM Watson Health Core

IBM Watson Health Core, IBM'in sahip olduğu veya denetlediği bir veri merkezinde bulunan IBM'in Geçerli Veri Koruma Yasalarına uygun şekilde, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) ve diğer Sağlık Verileri tarafından tanımlandığı gibi, Koruma Altındaki Sağlık Verilerini depolamak, düzenlemek ve işlemek için Sağlık Verileriyle etkinleştirilen bir hizmet olarak sunulan platform, geliştirme platformu ve operasyon alt sistemidir. Müşteri, aşağıda açıklanan özellikleri ve yetenekleri etkinleştirmek için IBM Watson Health Core ve IBM Watson Health Core Access olanaklarına uygun yetkiler edinmelidir.

1.1 Watson Health Core İşletim Ortamları

Watson Health Core yetkisi, Müşterinin Sağlık Verilerini işlemesini sağlamak üzere tasarlanmış, Sağlık Verilerinin Etkinleştirdiği üç bulut işletim ortamını içerir.

- Kılavuz Program

  Müşterilerin, IBM Hizmet Olarak Sunulan Yazılımlarını kullanarak uygulamaları geliştirip test edebileceği bir korumalı alan ortamı sağlar. Kılavuz program ortamı, Olağanüstü Durum Kurtarma, yüksek düzeyde kullanılabilirlik ve kayıt sistemlerinin yedeklenmesi hariç, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasasının tüm güvenlik denetimlerini uygular.

- Üretim ortamı

  Müşterilerin Sağlık Verilerine ilişkin iş yüklerini devreye alabildiği tam ölçekli ortam sağlar. Üretim ortamı, yüksek düzeyde kullanılabilir, yükü dengelenmiş bir ortamdır ve Olağanüstü Durum Kurtarma yerinde Yedek Sisteme Geçiş gerçekleştirebilir.

- Olağanüstü Durum Kurtarma

  Üretim ortamına ilişkin ikizleme eşlemesi sağlar ve ayrı bir veri merkez lokasyonunda bulunur.

1.2 Uygulama Geliştirme

IBM Watson Health Core, Müşteri aygıtlarından veya Müşterinin yetkili kullanıcılarına ait aygıtlardan güvenli veri toplama ve uygulama geliştirmesi sağlar. Uygulama programı arabirimleri, Müşterinin üçüncü kişi hizmet sağlayıcıları dahil olmak üzere, Müşterinin yetkili kullanıcılarının, IBM Hizmet Olarak Sunulan Yazılımları ile veri alışverişi yapabileceği ve uygulamalar geliştirebileceği program arabirimlerini ve belgelerini sağlar. Uygulama programı arabirimlerinin Müşteri veya onun geliştiricileri tarafından kullanımı, Uygulama Programı Arabirimi Geliştirme Gereksinimlerine uygunluğa tabidir.

- REST Uygulama Programı Arabirimleri

  Watson Health Core, Watson Health Core platformu için bir dizi REST Uygulama Programı Arabirimi ve hizmeti sağlar. Uygulama Programı Arabirimi yetenekleri; veri havuzlarına erişmeye yönelik mekanizmalar, veri düzenleme hizmeti, kullanıcı yönetimi ve denetim günlüklerini içerir ancak tümü bunlarla sınırlı değildir.

- Apple HealthKit ve Apple ResearchKit

  Watson Health Core, iOS tabanlı araştırma çalışmaları için Apple ResearchKit Uygulama Programı Arabirimi çerçevesi ile ve sağlık verilerini kaydetmek için Apple HealthKit ile bütünleştirmeyi destekler.

1.3 Veri Yönetişimi

- Rıza Yönetimi

  Watson Health Core, hastalar veya çalışma katılımcıları tarafından sağlanan rızayı kaydetmeye yönelik çerçeve sağlar ve bir kişi, rızaya dayalı bir Müşteri uygulamasına kaydolduğunda, veri yükü dışında rıza kaydını güvenli şekilde depolayabilir.

- Veri Maskeleme

  Watson Health Core, ad tanımlayıcılarını, yapılandırılmış veri yüklerinden ayırma yeteneği sağlar. Watson Health Core, bulut içindeki verileri programa ilişkin uygulama programı arabirimleri

aracılığıyla alır. Uygulama programı arabirimleri, hasta veya kişi adı tanımlayıcılarını kalan veri yüklerinden ayırma işleminin, ayrı bir şifreli veri deposunda depolanmasını sağlar. Veri yüküne, gelecekte köken takibinde kullanılabilecek, anonim hale getirilmiş bir simge atanır.

1.4 Sağlık Veri Hizmetleri

Watson Health Core, hem yapılandırılmış hem de yapılandırılmamış nitelikte, dış kaynaklı Sağlık Verileri ve diğer Kişisel Veriler dahil olmak üzere veri toplama, depolama ve eşitleme işlemleri sağlar.

- Veri Alma

  Watson Health Core, uygulama programı arabirimleri aracılığıyla, hasta uygulamalarından veya aygıtlarından veri alma yeteneği sağlar. Watson Health Core, sözleşme süresinin her yılında, Müşterinin Yetkili Kişilerine, Health Core olanağına 25 MB'ye kadar veri yükleme hakkı verir. Hizmet, her Kişi için günde en fazla 10 yükleme içerir.

- Opreasyonel Veri Gölü

  İşlenmemiş Müşteri veya hasta verileri, Watson Health Core olanağında, analitik ve modelleme için gerekli olana kadar orijinal biçiminde depolanır.

- Çıkarma-Dönüştürme-Yükleme (ETL)

  Veri, operasyonel alt sistem içinde normalleştirilmiş biçime dönüştürülür. Sağlık hizmetleri tesisleri için sektör standartlarına dayalı bir Kurumsal Hizmet Veriyolu, Müşterinin farklı uygulamalarında ve protokollerinde bütünleştirme sağlar.

- Veri Havuzu

  Veriler, düzenlendiğinde Veri Havuzuna taşınır. Watson Health Core, ticari ve teknik sağlık verilerini analitikte kullanım için normalleştirmek amacıyla, IBM'in Sağlık Hizmetleri için Birleştirilmiş Veri Modelinin özelliklerini kullanır.

- Ana Kişi Dizini

  Watson Health, Doğrusal Veri Kaydı oluşturmak için birden fazla kaynaktan alınan verileri birleştirmek amacıyla Ana Veri Yönetimi araçları sağlar.

2. İsteğe Bağlı Özellikler

2.1 IBM Watson Health Core Terminology Service

Bu eklenti hizmeti, ayrı sağlık sistemleri arasındaki veri bütünleştirmesini ve birlikte çalışabilirliği kolaylaştırarak, tüm Watson Sağlık Bulutu uygulamalarında klinik terminolojisinin tutarlı şekilde kullanılmasını sağlar. Bu hizmet, terminolojiler, kod sistemleri ve yapılandırılmış içeriği kapsayan aşağıda belirtilenler gibi tüm görevler için işlevsel platform sağlar:

- yeni kod sistemlerinin oluşturulması;
- uluslararası kod sistemlerinin çevrilmesi; ve
- yerel kod listeleri ile uluslararası standartlar arasında eşlemeler

Ek B

IBM, Yetki Belgesinde belirtildiği şekilde IBM Hizmet Olarak Sunulan Yazılımları için aşağıda belirtilen kullanılabilirlik hizmet seviyesi sözleşmesini sağlar. Hizmet Seviyesi taahhüdü bir garanti değildir. Hizmet Seviyesi yalnızca Müşteriye sağlanır ve yalnızca üretim ortamlarındaki kullanımlar için geçerli olur.

1. Kullanılabilirlik Alacakları

Kullanılabilirliğe ilişkin geri ödemeler, yalnızca Tekil Öğe yetkilerine yönelik abonelik ücretleri için geçerlidir.

Müşteri, IBM Hizmet Olarak Sunulan Yazılımlarının kullanımını etkileyen bir Olaydan ilk kez haberdar olmasını izleyen yirmi dört (24) saat içinde IBM teknik destek yardım masasında Önem Derecesi 1 olan bir destek sorun kaydı açtırmalıdır. Müşteri, her türlü sorun tanılama ve çözümleme sürecinde makul sınırlar içinde IBM'e yardımcı olmalıdır.

Hizmet Seviyesi Sözleşmesinin koşullarının karşılanamaması halinde, sözleşmenin yürürlükte olduğu ayın sona ermesinden itibaren üç iş günü içerisinde bir destek sorun kaydı talebinin gönderilmesi gerekir. Geçerli Hizmet Seviyesi talebine ilişkin telafi ücreti, IBM Hizmet Olarak Sunulan Yazılımlarının sağlanamadığı üretim sistemi işlemleri boyunca geçen süre ("Kapalı Kalma Süresi") esas alınarak IBM Hizmet Olarak Sunulan Yazılımları için gelecekte Müşteri tarafından kesilecek bir faturaya ilişkin alacak olarak kaydedilecektir. Kapalı Kalma Süresi, Müşterinin kapanma olayını raporladığı zamandan itibaren IBM Hizmet Olarak Sunulan Yazılımlarının yeniden yüklendiği zamana kadar geçen süre esas alınarak ölçülür ve bu süre, planlı ya da önceden duyurulmuş bir bakım için yapılan kesintiyi, IBM'in denetimi dışında ortaya çıkan nedenleri, Müşteri ya da üçüncü kişi içeriğinin veya teknolojisinin yarattığı sorunları, tasarımları ya da yönergeleri, desteklenmeyen sistem yapılandırmalarını veya platformlarını ya da diğer Müşteri hatalarını ya da Müşteri kökenli güvenlik sorunlarını veya Müşterinin güvenlik testlerini içermez. IBM, aşağıdaki tabloda gösterildiği şekilde, Sözleşmenin Yürürlükte Olduğu her Ay boyunca IBM Hizmet Olarak Sunulan Yazılımlarının kümülatif kullanılabilirliği doğrultusunda geçerli olan en yüksek telafi ücretini uygulayacaktır. Sözleşmenin yürürlükte olduğu herhangi bir aya ilişkin toplam telafi ücreti, IBM Hizmet Olarak Sunulan Yazılımlarının yıllık ücretinin on ikide birinin (1/12) yüzde yirmisinden (%20) fazla olamaz.

2. Hizmet Seviyeleri

Sözleşmenin yürürlükte olduğu ay boyunca IBM Hizmet Olarak Sunulan Yazılımının kullanılabilirliği

Bir sözleşmenin yürürlükte olduğu ay boyunca kullanılabilirlik	**Ödemeler (Talebe konu olan sözleşmenin yürürlükte olduğu ay için aylık Tekil Öğe abonelik ücretinin* yüzdesi)**
< %99,95	%10
< %99,0	%20

* Aylık abonelik ücreti, IBM Hizmet Olarak Sunulan Yazılımının bir IBM Çözüm Ortağından edinilmiş olması durumunda, talebe konu olan sözleşmenin yürürlükte olduğu ayda geçerli olan IBM Hizmet Olarak Sunulan Yazılımı güncel liste fiyatına %50 oranında indirim uygulanarak hesaplanır. IBM, geri ödemeyi doğrudan Müşteriye yapacaktır.

Kullanılabilirlik yüzdesel olarak ifade edilir ve aşağıda belirtilen şekilde hesaplanır: sözleşmenin yürürlükte olduğu ay içindeki toplam dakika sayısından sözleşmenin yürürlükte olduğu ay içindeki toplam Kapalı Kalma Süresi dakikalarının sayısı çıkartılır ve sonuç sözleşmenin yürürlükte olduğu ay içindeki toplam dakika sayısına bölünür.

Örnek: Sözleşmenin yürürlükte olduğu ay içinde 108 dakika toplam Kapalı Kalma Süresi

30 günlük sözleşmenin yürürlükte olduğu ayda toplam 43.200 dakika - 108 dakikalık Kapalı Kalma Süresi = 43.092 dakika _____ 43.200 toplam dakika	= Sözleşmenin yürürlükte olduğu ay içinde %99,75 oranında kullanılabilirlik için %10 oranında kullanılabilirlik alacağı

3. Hariç Tutulanlar

Bu hizmet seviyesi sözleşmesi aşağıda belirtilenler için geçerli değildir:

- Hizmet Seviyesi Sözleşmesi, sunucu izlemenin yanı sıra, özel uygulamaları veya Müşteri uygulamalarını desteklemek için barındırılan sanal makineler için geçerli değildir.
- Müşterinin mevcut sözleşme yükümlülükleri kapsamında, sözleşmenin esasına ilişkin herhangi bir yükümlülüğünü ihlal etmesi.

Ek C

Bu Güvenlik ve İş Sürekliliği Eki (bu "SBCA"), IBM'in, IBM Hizmet Olarak Sunulan Yazılımlarını Müşteriye sağlamasıyla ilgili belirli gereksinimleri ve yükümlülükleri belirtir. Bu belgede belirtilen gereksinimler ve yükümlülükler, http://www.ibm.com/cloud/data-security adresinde mevcut olan IBM Hizmet Olarak Sunulan Yazılımları için veri güvenliğine yönelik ilkelerin açıklamasında belirtilenlere ektir. Bu belgede tanımlanmayan, büyük harfle girilmiş koşullar, Sözleşmede veya Kullanım Koşullarında belirtilen anlamı taşıyacaktır.

1. Bilgi Güvenliği Programı

IBM, ISO 27001 çerçevesine ve denetim alanlarına dayalı dahili güvenlik ilkeleri, standartları ve süreçlerine sahiptir. IBM Kurumsal Güvenlik Kuruluşunun yönetişimine ek olarak, bu ilkeler, standartlar ve süreçler, düzenli olarak dahili denetimlerin konusudur.

IBM, en azından bu Güvenlik ve İş Sürekliliği Ekinin gereksinimleri ile tutarlı olan ve Müşteri içeriğinin işlenmesini, depolanmasını ve iletilmesini yöneten kurumsal, operasyonel, idari, fiziksel ve teknik korumalara ilişkin bir bilgi güvenliği programını sürdürür.

Müşterinin sürekli uygunluğunu, yeterliliğini ve etkinliğini makul şekilde belirleyebilmesi için IBM, IBM Watson Health bilgi güvenliği programıyla ilgili bilgileri, Müşterinin talebi üzerine Müşteriyle paylaşacaktır. IBM Watson Health bilgi güvenliği programı, genel kabul gören sektör uygulamaları ve IBM'in Geçerli Yasaları açısından güncel olmaya devam etmek için zaman zaman güncellenecektir.

2. Erişim Denetimleri

IBM, söz konusu Müşteri içeriğini, yalnızca çalışanlarına, alt yüklenicilerine veya IBM Hizmet Olarak Sunulan Yazılımlarını -hangisi geçerliyse- Geçerli Yasalar, Sözleşme veya İlgili Belgeye uygun olarak sağlamak için gerektiği şekilde IBM'in Müşteriye veya diğer kişilere karşı yükümlülüklerini yerine getirmesine yardımcı olmak amacıylaMüşteri içeriğine erişmek için yasal iş gereksinimi olan üçüncü kişilere ifşa edecektir. IBM'in Müşterinin İş Ortağı olması durumunda, IBM ve Müşteri, Kişisel Sağlık Bilgilerini, yalnızca Taraflar arasındaki geçerli İş Ortaklığı Sözleşmesinin koşullarına uygun olarak ifşa edecektir.

IBM, dahili kullanıcı erişimine ilişkin resmi bir yönetim sürecine sahiptir. Bu süreçte, kullanıcı erişimi, resmi olarak talep edilir, kimlik doğrulaması yapıldıktan sonra onaylanır ve en düşük düzeyde öncelik kavramı kullanılarak, bilinmesi gerektiği şekilde verilir. Müşteri içeriğine erişim, yalnızca etkin kullanıcılar ve etkin kullanıcı hesapları ile sınırlandırılacaktır. IBM, etkin kullanıcı hesaplarının dahili erişiminin periyodik olarak yeniden doğrulanması için resmi bir sürece sahiptir.

IBM, Hizmetleri Müşteriye IBM'in kurumsal güvenlik standartları ve ilkeleri doğrultusunda sağlamak amacıyla kullanılan sistemler üzerinde etkin kullanıcı hesapları için benzersiz tanıtıcıların ve güçlü parolaların atanması dahil olmak üzere, kullanıcı kimliğini doğrulamaya ilişkin güvenli protokolleri kullanır:

a. Parolalar, satıcı firma tarafından sağlanmış varsayılan parolalar olmayacak ve korudukları verilerin güvenliğini tehlikeye atmayan bir yerde ve/veya biçimde tutulacaktır.

b. Parolaları görüntüleme ve yazdırma işlemi, maskelenmeli, gizlenmeli veya yetkisiz kişilerin bu parolaları gözleyemeyeceği veya daha sonra geri alamayacağı başka bir şekilde gizlenmelidir. Parolalar girildiğinde loga kaydedilmemeli veya yakalanmamalıdır. Kullanıcı parolaları, açık metin olarak depolanmamalıdır.

c. IBM Hizmet Olarak Sunulan Yazılımlarını oluşturan her teknoloji için parolalar, parola uzunluğuyla ilgili bilinen güvenlik açıklarıyla ilişkili riskleri azaltmak için seçilir ve bunlar belgelenmelidir.

d. Operasyonel nedenlerle dahili, ayrıcalıklı ve paylaşılan işlevsel kimliklerin gerekli olması durumunda, IBM, bireysel hesap verebilirliği sürdürmek için parolaların denetlenmesini gerektiren paylaşılan, işlevsel ve/veya Sistem kimliklerini yönetir.

İşlem yapmamaya ilişkin süre aşımları, Müşteri içeriğini depolayan tüm sistemler ve uygulamalar için belirlenir.

IBM'in Müşteri içeriğini depolayan ağı, sistemleri ve uygulamalarına uzaktan erişim gerekirse, bunlar, Müşterinin talebi ve IBM'in resmi onayı üzerine belirlenecektir. Ayrıca tüm bu uzaktan bağlantıların güvenliği, güçlü kimlik doğrulama ve şifreleme protokolleri kullanılarak sağlanacaktır. Uzaktan erişim etkinliği loga kaydedilecek ve izlenecektir.

IBM Hizmet Olarak Sunulan Yazılımlarının sağlanmasının, IBM'in Müşterinin dahili ağlarında bulunan herhangi bir sisteme uzaktan erişmesini gerektirmesi durumunda, tüm bu uzaktan erişim, yalnızca Müşterinin güvenli uzaktan erişim sistemleri ve protokolleri ve ayrıca, IBM'e Müşteri tarafından sağlanan erişim kimlik bilgileri kullanılarak gerçekleştirilecektir. Müşterinin ağına uzaktan erişim, yalnızca IBM'in talebi ve Müşterinin onayı üzerine ve IBM'e önceden sağlanacak olan Müşterinin o tarihte geçerli ilkeleri doğrultusunda oluşturulacaktır. IBM'in Müşterinin dahili ağlarını kullanımı, IBM'e önceden sağlanacak olan Müşterinin BT kullanımı ve güvenlik ilkelerine tabi olacaktır.

IBM, güvenlik yönetimi, erişim incelemesi ve güvenlik ihlali ile ilgili araştırmalar için görevler ayrılığını uygular.

Müşteriye özel Müşteri içeriğinin depolanması, barındırılması ve işlenmesi, IBM'in hizmet sağladığı diğer müşterilerinkinden mantıksal olarak ayrıdır. Paylaşılan bir depolama, barındırma veya işlemeye ilişkin çalışma alanına Müşteri tarafından izin verildiği durumlarda, IBM, söz konusu Müşteri içeriğinin yetkisiz şekilde ifşa edilmesini engellemek üzere tasarlanmış ve bu Güvenlik ve İş Sürekliliği Ekinde belirtilen gereksinimlerle tutarlı olarak uygulamaya konmuş prosedürlere ve güvenlik önlemlerine sahip olacaktır.

IBM, Müşteri içeriğinin herhangi bir zamanda genel kullanıma açık bir yerde gözetimsiz bırakılmamasını sağlamak için açık masaüstü/açık ekran ilkeleri uygular.

3. Aktarım ve Şifreleme

IBM, alıcı için doğru iletişim bilgilerinin kullanıldığından emin olmak amacıyla Müşteri içeriğinin iletilmesiyle ilgili uygun önlemleri alacak (faks, e-posta, kurye vb.) ve söz konusu bilgilerin alınmasını güvenli hale getirmek için hedeflenen alıcı ile ilgili ön düzenlemeler yapacaktır.

IBM, Müşteri içeriğine ilişkin herhangi bir aktarma, iletişim, uzaktan erişme veya depolama işlemleri dahil, Müşteri içeriğinin işlenmesiyle bağlantılı olarak, uygun şifreleme biçimlerini veya diğer güvenli teknolojileri her zaman kullanacak ve IBM Personelinin de kullanmasını sağlayacaktır. Örneğin IBM,

a. tesis dışındaki bir depolama tesisine aktarma sırasında, yedekleme manyetik bantları dahil, IBM dizüstü bilgisayarları, taşınabilir aygıtları veya taşınabilir elektronik ortamları üzerinde depolanan;

b. basılı kağıt belgeler hariç olmak üzere, Müşteriye veya IBM'e ait fiziksel güvenliği sağlanmış ofislerin ve tesislerin dışında IBM tarafından depolanan veya taşınan;

c. IBM tarafından genel ağlarda dolaşan;

d. IBM sistemlerinden Müşteriye aktarılan;

e. IBM tarafından kablosuz olarak iletilen; ve

f. IBM tarafından sunucular ve veritabanları üzerinde depolanan Müşteri içeriğini içeren tüm kayıt ve dosyaları, sektör standardında uygun şifreleme kullanarak şifreleyecektir.

4. Ağ Güvenliği

IBM, güvenlik duvarları, vekil sunucular, web uygulamasına ilişkin güvenlik duvarları ve arabirimler gibi sistem güvenlik yazılımlarının makul düzeyde güncel sürümlerini kullanır. Söz konusu yazılımlar, kötü niyetli yazılıma karşı koruma ve makul düzeyde güncel yamalar ve virüs tanımları içermelidir. Kurumsal standartlara uygun şekilde, virüse karşı koruma yazılımı, teknik olarak uygulanabilir olduğunda iş istasyonları, sunucular ve ilgili uç noktalarda kurulmalıdır. Yazılım, ilkeyi, dahili yönetim çözümleriyle birleştirecek şekilde yönetilir.

IBM, güvenlik olaylarını mümkün olduğunca erken algılamak ve tanımlamak için IBM Hizmet Olarak Sunulan Yazılımlarını izler. IBM, Müşteriye hizmetler sunmak için kullanılan Müşteri içeriğinin veya bilgi sistemlerinin yetkisiz şekilde ifşa edilmesine, hatalı kullanılmasına, değiştirilmesine veya imha edilmesine yol açabilecek dahili ve harici güvenlik açıklarını ve risklerini belirlemek üzere tasarlanmış, en azından sektör standardında izinsiz girişi algılama araçlarını ve engelleme, izleme ve müdahale etme süreçlerini sürdürecektir.

IBM, güvenlik açığı istihbaratına ilişkin hizmetlere veya bilgi güvenliği danışmanlarına ve sistem güvenlik açıkları hakkında güncel bilgi sağlayan diğer ilgili kaynaklara katkı sağlar. IBM, ağına ilişkin düzenli güvenlik açığı değerlendirmeleri ve iyileştirme gerçekleştirir.

IBM, güvenlik olaylarını algılamak, tanımlamak, kontrol altına almak ve çözmek için IBM Hizmet Olarak Sunulan Yazılımlarını izler.

IBM, IBM yayın yönetimi süreçleri aracılığıyla, IBM Hizmet Olarak Sunulan Yazılımlarının kullanıma sunulduğu ağ güvenlik altyapısının kullanılabilirliğini, bütünlüğünü ve etkinliğini doğrular.

5. Olay Yönetimi ve Bildirimler

IBM Watson Health ekipleri, yazılımla ilgili güvenlik sorunlarını azaltmak için gereken önleyici adımları uygulamak amacıyla, IBM olanaklarıyla ilgili güvenlik olaylarının alınmasını, araştırılmasını ve dahili olarak koordine edilmesini yöneten küresel bir ekip olan IBM Siber Güvenlik Olaylarına Müdahae Ekibiyle birlikte çalışır. "Güvenlik Olayı", IBM Hizmet Olarak Sunulan Yazılımlarını sağlamak için IBM tarafından kullanılan bir bilgi sistemi içinde sistem operasyonlarına ilişkin başarılı yetkisiz erişim, kullanım, ifşa, değiştirme veya müdahale işlemleridir. Bir Güvenlik Olayının saptanması durumunda (rutin tarama, uyarılar, eşik olayları vb. aracılığıyla), IBM, Müşteriyi:

a. Müşteri içeriğinin dahil olduğu onaylı her tür Güvenlik Olayını, mümkün olan en kısa zamanda ve her durumda, söz konusu Güvenlik Olayının araştırılması ve doğrulanmasından sonra en geç 2 iş günü içinde;

b. Yasa veya ilgili emir yasaklamadığı sürece, herhangi bir devlet yetkilisinden (herhangi bir veri koruma kurumu veya herhangi bir yasa uygulayıcı kurum) alınmış herhangi bir Müşteri içeriğine erişime veya bu içerikle ilgili bilgiye yönelik herhangi bir istekten hemen sonra; ve

c. Bu Güvenlik ve İş Sürekliliği Ekinde Erişim Denetimleri başlıklı bölümde izin verildiği durumlar haricinde, Müşteri içeriğinin herhangi bir üçüncü kişiye veya üçüncü kişi tarafından herhangi bir şekilde ifşa edilmesi veya aktarılması veya bu içeriğe üçüncü bir kişi tarafından erişilmesinden önce, bilgilendirecektir.

6. Loga Kaydetme

IBM, IBM'in ilke ve uygulamalarına ve genel kabul gören sektör uygulamalarına uygun şekilde, sistemlerini, Müşterinin İşlenmiş Verilerine erişilmesi veya bu Verilerin yetkisiz şekilde kullanılması açısından makul düzeyde izlemeyi sürdürecektir. Oturum açma veya erişim ile ilgili gerçekleşmiş ihlaller veya ihlal girişimleri, loga kaydedilecektir.

IBM, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası ve IBM'in diğer Geçerli Veri Koruma Yasaları gerektirdiği sürece, Müşteri ve Sağlık Verilerini depolayan, işleyen, ileten ve bu verilere erişen tüm sistemler için erişim etkinliklerinin günlüklerine ve tüm erişim isteklerine ilişkin kayıtlar tutar.

Günlükler ve raporlar en azından şunları içerir: (i) makul tanımlama bilgileri dahil, başarılı olsun veya olmasın tüm oturum açma girişimleri; (ii) uygulama kurulumları, kullanıcı yönetimi değişiklikleri ve dosya erişim izinlerine yönelik değişiklikler dahil, tüm sistem ve ağ yapılandırma değişiklikleri; (iii) herhangi bir dosyaya, ağ paylaşımına, loga veya başka bir kaynağa erişme girişimleri dahil, başarılı olsun veya olmasın, kaynak erişimi girişimleri; ve (iv) yüklemeyi gerçekleştirmek için kullanılan veri ve erişim protokolünün içerik türü dahil, veri yüklemeleri.

7. Yazılım Uygulamasına İlişkin Geliştirme ve Değişiklik Yönetimi

IBM, üretim uygulamalarının bütünlüğünü ve ilgili kaynak kodunu, yetkisiz veya test edilmemiş değişikliklere karşı koruyan güvenli uygulama geliştirme ve kodlama uygulamalarına uygun hareket eder.

IBM, şunları içeren bir değişiklik yönetimi sürecini takip eder: (a) değişikliklerin ve geri alma prosedürlerinin kaydedilmesi ve resmi olarak onaylanması; ve (b) uygun olduğunda kullanıcı kabul testlerinin yanı sıra güvenlik testleri dahil, söz konusu değişikliklerin uygun şekilde test edilmesi.

IBM, Müşteri içeriğine ilişkin depolama, erişim ve iletim işlemlerini gerçekleştirmek veya IBM Hizmet Olarak Sunulan Yazılımları dahil, hizmetleri Müşteriye sunmak için kullanılan tüm sistemler üzerinde kurulum öncesinde test yamalarını içeren bir yama yönetimi sürecini takip eder.

IBM, sistem yöneticilerinden, Müşteri içeriğine ilişkin depolama, erişim ve iletim işlemlerinde kullanılan tüm bilgi sistemlerinin yapılandırmasıyla ilgili eksiksiz, doğru ve güncel bilgileri sürdürmesini istemektedir.

8. Fiziksel ve Çevresel Güvenlik

IBM Watson Health Core platformu, IBM SoftLayer veri altyapısı üzerinde devreye alınır. IBM SoftLayer, Müşteri verilerini, teknik, insan ve çevre kaynaklı ihlal ve etkiden korumak için fiziksel ve çevresel güvenliği, erişim denetimini, denetimleri ve süreçleri sürdürür.

IBM Hizmet Olarak Sunulan Yazılımlarının barındırıldığı tesislere genel erişim, bir kartlı erişim sistemi kullanılarak denetlenir. Kapalı devre televizyon ("CCTV") kameraları, tesisler genelinde kurulur ve güvenlik personeli tarafından izlenir. Seçilen erişim kapılarında alarm bulunur ve güvenlik personeli bu alarmları izler.

Denetimli alanlara erişim, kartlı erişim ve/veya ek biyometrik doğrulama yoluyla kısıtlanır. Denetimli alanlara yetkili erişimi olmayan tüm kişiler, imza atarak giriş yapmalı ve bu kişilere, denetimli alana onaylı erişimi olan bir kişi eşlik etmelidir. Tüm denetimli alanların acil çıkışlarında sesli alarmlar bulunur ve güvenlik personeli bu alarmları izler. Alarmların çalıştığına dair periyodik doğrulama gerçekleştirilir, belgelenir ve saklanır. Denetimli alanlara erişim hakları, üç ayda bir tamamen yeniden doğrulanır. Denetimli alanlara erişim, iş akdinin sona erdirilmesi durumunda iptal edilir.

Tesisler; yangın, su, yangın alarmlarından çıkan ısı, yangın söndürücüler, duman alarmları ve yangın söndürme sistemleri gibi çevresel etkenlere karşı korunur. Tesisler, düzenli olarak sürdürülen ve test edilen Kesintisiz Güç Kaynağı (UPS) sistemleri ve yedek jeneratörler aracılığıyla güç kesintilerine veya arızalarına karşı korunur.

IBM SoftLayer uyumluluk bilgileri ve raporları şu adreste bulunabilir: http://www.softlayer.com/compliance.

9. İş Operasyonlarının Sürekliliği

IBM, Sözleşme kapsamındaki yükümlülüklerle tutarlı hizmet seviyesini sürdürmek üzere tasarlanmış iş sürekliliği ve olağanüstü durum kurtarma planlarına sahiptir. Söz konusu iş sürekliliği ve olağanüstü durum kurtarma planları, periyodik olarak güncellenecek ve test edilecektir (yılda en az bir kez). IBM, genel kabul gören sektör uygulamalarıyla uyumluluğu devam ettirmek için gereken iş sürekliliği ve olağanüstü durum kurtarma planlarına makul tüm değişiklikleri uygulayacak ve her durumda bunlar, Müşteri tarafından kullanılmakta olan IBM Hizmet Olarak Sunulan Yazılımlarına veya üretim ortamına makul olmayan düzeyde müdahale edilmeden gerçekleştirilecektir.

IBM Hizmet Olarak Sunulan Yazılımlarının Müşteriye sağlanamamasına yol açan bir olağanüstü durumun meydana gelmesi halinde, IBM, Müşteriyi derhal bilgilendirecek ve iş sürekliliği ve/veya olağanüstü durum kurtarma planını etkinleştirecektir. Olağanüstü durum ilan edildiğinde, IBM Hizmet Olarak Sunulan Yazılımlarının iş sürekliliği hedefi, Müşterinin IBM Hizmet Olarak Sunulan Yazılımlarına erişimini şu şekilde yeniden sağlamaktır: bir kesinti durumunda, Kurtarma Süresi Hedefi; IBM Watson Health üretim ortamını, olağanüstü durum ilanından itibaren 36 saat içinde geri yüklemektir. Kurtarma Noktası Hedefi, üretim ortamında Müşteri içeriği kaybının 24 saati aşmamasıdır. Belirli Watson Health çözümlerinin iş sürekliliği hedefleri değişiklik gösterebilir.

IBM'in olağanüstü durum kurtarmaya yönelik yaklaşımı, dağıtılmış coğrafi alanlarda bulunan birden fazla veri merkezini içerir.

Tüm IBM SoftLayer veri merkezlerinde, birden fazla güç kaynağı, fiber hatlar, ayrı jeneratörler ve yedek pil yer almaktadır. Bunlar, sektör lideri donanım ve ekipmandan oluşturulmuştur ve en yüksek düzeyde performans, güvenilirlik ve birlikte çalışabilirlik sağlar. Yedekli n+1 güç ve soğutma kaynakları gibi dahil edilecek tüm veri merkezi bileşenleri, veri merkezleri içinde kararlılığı sürdürmek üzere denetlenecektir.

10. Uyumluluk

IBM'in güvenlik uygulamaları, ISO 27001-27002'yi esas alır. Bu uygulamalar, Risk Analizi, Fiziksel Güvenlik, Acil Durum Planlama, Araştırmalar, Bilgi Koruma, Eğitim, Veri Koruma ve Operasyonlar (dahil ancak bunlarla sınırlı olmamak üzere) için denetim yapıları sağlar.

IBM, güvenlik ve gizlilik ile bağlantılı etkinlikleri, IBM'in güvenlik uygulamalarına uygunluk açısından incelemektedir.

IBM, Kapsam Dahilindeki Yetkili Mahkemelerin IBM Geçerli Güvenlik Yasalarına uygun hareket eder.

Ayrıca Müşterinin gizli bilgilerinin uygun şekilde işlenmesi de tüm çalışanların her yıl incelemesi (ve incelendiğini doğrulaması) gereken IBM İş Adabı İlkeleri kapsamında gereklidir.

11. Diğer Koşullar

IBM, IBM Hizmet Olarak Sunulan Yazılımlarının sağlanmasında görevlendirilen tüm alt yükleniciler ve/veya üçüncü kişiler ile yapılan tüm sözleşmelerin, Müşteri içeriğini, en az bu Güvenlik ve İş Sürekliliği Ekinde ve herhangi bir geçerli İlgili Belgedeki koşullar kadar koruyan koşullara sahip olmasını sağlayacaktır. Söz konusu koşulların her biri, ilgili alt yükleniciler ve/veya üçüncü kişiler tarafından gerçekleştirilecek hizmetler için geçerli olmalıdır.

Kabul eden:

Müşteri Şirketinin Ticari Unvanı adına (“**Müşteri**”)

İmza_____

Yetkili imza

Unvan:

İsim (el yazısı veya daktiloyla):

Tarih:

Müşteri Numarası:

Müşteri Adresi:

Kabul eden:

<İlgili IBM Şirketinin Ticarı Unvanı adına> (“**IBM**”)

İmza_____

Yetkili imza

Unvan:

İsim (el yazısı veya daktiloyla):

Tarih:

Sözleşme Numarası:

IBM Adresi: