IBM Watson Health Core

이용 약관은 본 IBM 이용 약관 – SaaS 특정 오퍼링 조건(이하 "SaaS 특정 오퍼링 조건")과 IBM 이용 약관 – 일반 조건(이하 "일반 조건") 문서(URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/ 참조)로 구성됩니다.

조건이 상충하는 경우에는 SaaS 특정 오퍼링 조건이 일반 조건에 우선하여 적용됩니다. IBM SaaS 를 주문하거나 액세스하거나 사용함으로써 고객은 이용 약관에 동의하게 됩니다.

이용 약관에는 해당 IBM International Passport Advantage 계약, IBM International Passport Advantage Express 계약 또는 선택한 IBM SaaS 오퍼링에 관한 IBM 국제 계약(IBM International Agreement for Selected IBM SaaS Offerings)이 적용되며 이용 약관과 함께 완전한 계약을 구성합니다.

1. IBM SaaS

다음 IBM SaaS 오퍼링에는 본 SaaS 특정 오퍼링 조건이 적용됩니다.

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

2. 청구 체계

IBM SaaS 는 거래서류에 지정된 바와 같이 다음 중 하나의 청구 체계 하에서 판매됩니다.

a. **액세스(Access)** – IBM SaaS 가 구매되는 경우 이용되는 산정 단위입니다. 액세스는 IBM SaaS 를 사용할 수 있는 권리입니다. 고객은 고객의 라이센스 증서(PoE) 또는 거래서류에 규정된 산정 기간 동안 IBM SaaS 를 사용하기 위하여 반드시 액세스 권한을 취득하여야 합니다.

b. **개체(Individual)** – IBM SaaS 가 구매되는 경우 이용되는 산정 단위입니다. 하나의 개체는 단일한 사물 또는 사람입니다. 고객의 라이센스 증서(PoE)나 거래서류에 명시된 산정 기간 동안 IBM SaaS 에서 처리하거나 관리되는 각 개체를 포함할 수 있는 충분한 권한을 취득해야 합니다.

본 IBM SaaS 의 목적상, 하나의 개체(Individual)에는 데이터가 IBM SaaS 에서 관리되는 하나의 개인, 디바이스 또는 모바일 애플리케이션이 포함됩니다.

c. **인스턴스(Instance)** – IBM SaaS 가 구매되는 경우 이용되는 산정 단위입니다. 인스턴스는 IBM SaaS 의 특정 구성에 대한 액세스를 의미합니다. 고객의 라이센스 증서 또는 거래서류에 명시된 산정 기간 동안 액세스하여 사용하도록 제공된 IBM SaaS 의 각 인스턴스에 대해 충분한 권한을 취득해야 합니다.

3. 대금 및 청구

IBM SaaS 에 대한 청구 금액은 거래서류에 명시됩니다.

3.1 월 분할(Partial Month) 요금

거래서류에 명시된 월 분할 요금은 비례 배분하여 산정될 수 있습니다.

3.2 추가 요금

산정 기간 동안 고객의 IBM SaaS 실제 사용량이 라이센스 증서에 명시된 권한을 초과하면 거래서류에 명시된 대로 고객에게 초과분에 대한 요금이 청구됩니다.

4. 기간 및 갱신 옵션

IBM SaaS 의 기간은 주문서에 명시된 바와 같이, IBM 이 고객에게 IBM SaaS 에 대한 파일럿(Pilot) 운영 환경의 액세스(접근) 권한에 대해 통지한 날부터 시작됩니다. 개체(Individual) 권한의 사용등록 기간은 IBM 이 고객에게 프로덕션(Production) 운영 환경에 대한 액세스(접근) 권한에 대해 통지한 시점에 시작됩니다. 주문서는 IBM SaaS 가 자동으로 갱신되는지, 계속적으로 사용되는지 또는 기간 만료 시 종료되는지를 명시할 것입니다.

자동 갱신의 경우, 고객이 기간 만료일로부터 최소 90 일 이전에 갱신하지 않겠다는 의사가 기재된 서면 통지를 제공하지 않는 이상, IBM SaaS 는 라이센스 증서에 명시된 기간에 대해 자동으로 갱신됩니다.

계속적인 사용의 경우, 고객이 사전 90 일의 서면 종료 통지를 제출할 때까지 IBM SaaS 는 월단위로 계속 사용할 수 있습니다. 그러한 90 일 기간 이후의 역월(calendar month)의 말일까지 IBM SaaS 가 계속 제공됩니다.

5. 기술 지원

IBM 은 기술 지원 담당자 정보, 유지보수 시간 및 기타 정보와 절차에 대해 설명하는 IBM Software as a Service Support Handbook 을 제공합니다. 기술 지원 담당자 정보 및 지원 운영에 대한 기타 상세 정보는 IBM SaaS Support Handbook(https://support.ibmcloud.com)에서 확인할 수 있습니다.

IBM SaaS 에 대한 기술 지원 및 단순한 구성 요청은 전자적 제출을 통해 제공됩니다. 기술 지원은 IBM SaaS 와 함께 제공되며 별도의 오퍼링으로 제공되지 않습니다.

문제점 발생 사고 보고 시 어떠한 문서나 정보에도 보호된 건강 정보(Protected Health Information, PHI) 및 민감한 개인 정보(Sensitive Personal Information, SPI)를 포함한 개인 정보(Personal Information, PI)가 포함될 수 없습니다.

6. 용어 정의

적용 법령(Applicable Laws) – 본 이용 약관 이행에 적용되는 법령으로 정부 당국에서 발표한 여하한의 법률, 법령, 제정 법률, 규칙, 규정, 지침, 칙령, 판결 또는 기타 요건이나, 일반적으로 공인된 산업 표준을 의미합니다.

API – 소프트웨어 및 애플리케이션을 구축하는 루틴, 프로토콜 및 도구 세트에 해당하는 Application Program Interface 를 의미합니다. API 는 소프트웨어 구성요소가 상호작동하는 방식을 지정하고 APIs 는 그래픽 사용자 인터페이스(GUI) 구성요소를 프로그래밍하는 경우에 사용됩니다.

승인된 관리자(Authorized Administrator) – 플랫폼의 유지와 안정된 운영을 관리해야 하는 고객의 직원, 고객의 공인 계약직 직원, 개인 또는 그룹입니다. 책임사항에는 구성, 지원, 사용자 관리 및 계정 관리가 포함될 수 있습니다. 해당 관리자는 Watson Health 시스템에서 연구의 셋업을 책임지는 임상 시험자(clinical investigator)도 될 수 있습니다.

승인된 개체(Authorized Individual) – Watson Health Core 에 데이터를 전송할 수 있는 접근 권리에 대한 액세스가 제공된 인증된 개인, 모바일 애플리케이션 또는 디바이스입니다. 이에는 고객, 고객의 연구 참여자, 고객 또는 환자가 포함될 수 있습니다.

고객 적용 데이터법(Client Applicable Data Laws) – 본 계약, 관련 문서 및 해당 서비스 명세, 주문서 및 당사자 간 작업 명세서에 의거해서 고객의 책임을 이행하는 데 적용 가능한 데이터법(Data Laws)을 의미합니다.

고객 데이터(Client Data) – 고객의 자체 데이터나 고객의 고객 또는 제 3 자가 직접 입력하거나 대신 입력한 데이터인지 여부에 관계 없이, 제 3 자 웰니스 헬스 디바이스의 데이터를 포함하여 고객이 입력하거나 고객을 위해 입력된 IBM SaaS 의 여하한의 데이터 입력을 의미합니다.

데이터법(Data Laws) – 데이터 보호, 개인정보 보호 또는 보안과 관련된 여하한의 적용 법령(Applicable Laws)을 의미합니다.

데이터 주체(Data Subject) – 개인 데이터(Personal Data)에 대해 식별되어 있거나 식별이 가능한 개인을 의미합니다.

지정 데이터 센터(Designated Data Center) – 거래서류에서 1 차 재해 복구 데이터 센터로 지정되어 고객의 IBM SaaS 인스턴스를 실행하는 데이터 센터를 의미합니다.

건강 데이터(Health Data) – 건강과 관련된 개인 정보로 이미지를 포함한, 데이터 또는 정보를 의미합니다.

건강 데이터 사용(Health Data Enabled) – IBM SaaS 에 대해서, HIPAA(HITECH Act 에 따라 수정됨) 및 건강 데이터(Health Data)에 관한 기타 적용 법령(Applicable Laws)을 이행하는 규정의 이행 명세(Part 164, Subparts A 및 C 에 명시됨)를 포함하여 범주 내 국가에서 건강 데이터에 관한 해당 보안 및 개인정보 보호정책, 법률 및 규정을 충족하는 IBM SaaS 의 자격을 의미하며 단, IBM 이 비즈니스

파트너(Business Associate)나 정보 관리자(Data Controller)의 자격으로 활동하고 있다는 것을 의미하지는 않습니다.

HIPAA - Health Insurance Portability and Accountability Act of 1996(개정판)(Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act of 2009(이하 "HITECH Act"), 미국 Department of Health and Human Services 가 45 C.F.R. Parts 160 및 164 에서 HIPAA 에 의거해서 공포한 특정 규정 및 HITECH Act 에 준하여 공포한 특정 규정 포함)을 의미합니다.

IBM 적용 데이터법(IBM Applicable Data Laws) - 본 계약, 관련 문서 및 해당 서비스 명세, 주문서 및 당사자 간 작업 명세서에 의거해서 IBM 의 책임을 이행하는 데 적용 가능한 데이터법(Data Laws)을 의미합니다.

IBM 인력(IBM Personnel) - (a) IBM, IBM 계열사와 IBM 하도급자 및 이들 각각의 직원, 및 (b) 제 3 자 공급자. 이들 각각은 본 계약 및 관련 문서에 준하여 IBM 대신 서비스를 수행하거나 IBM 으로부터 고객 개인 데이터에 대한 접근 권한을 부여받은 자입니다.

범주 내 국가(In-scope Countries) - 유럽 연합 28 개 회원국과 스위스 및 IBM 이 이 목록에 수시로 추가하는 국가를 의미합니다.

개인 데이터(Personal Data) 또는 **개인 정보(Personal Information)** - 개인에 대해 식별되어 있거나 식별이 가능한 여하한의 매체나 형식으로 된 정보(전자적 기록, 서면 기록 포함)를 의미합니다. "식별 가능한 개인(identifiable individual)"은 특히, 식별 번호 또는 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 정체성에 대한 한 가지 이상의 요인을 참조하여 직접 또는 간접적으로 확인할 수 있는 개인입니다.

프로세스(Process) 및 변형된 용어(**처리(processing)** 등)(대문자로 표시된 여부에 관계없음) - 수집, 기록, 구성, 저장, 조정 또는 변경, 검색, 참고, 사용, 전송에 의한 공개, 전파 또는 가용화, 정렬 또는 조합, 차단, 삭제 또는 파기 등 자동화된 방법 여부에 관계 없이, 데이터에 대해 수행하는 작업이나 작업 세트를 의미합니다.

처리 데이터(Processed Data) - 본 계약, 관련 문서 및/또는 서비스 명세, 주문서 및/또는 작업명세서에 준하여 IBM 이 처리한 데이터, 기밀 또는 독점 정보나 자료(건강 데이터 및 개인 데이터 포함)를 의미합니다.

보안 사고(Security Incident) - SBCA 에 명시된 의미로 사용됩니다.

7. 계정 관리

IBM SaaS 에는 고객의 허가된 사용자("**승인된 관리자**" 또는 "**승인된 개체**")만 액세스할 수 있습니다. 고객은 IBM SaaS 에 대한 액세스가 허가된 계정을 관리하게 되며 이에는 허가된 애플리케이션, 고객 인력, 고객의 제 3 자 서비스 제공자 및 계약직 직원이 포함될 수 있습니다. 또한 (i) 허가된 사용자의 신원 확인을 포함하여(단, 이에 한하지 않음), 모든 허가된 사용자를 관리하고 (ii) 허가된 사용자만 IBM SaaS 에 액세스하는지를 확인해야 할 책임은 전적으로 고객에게 있습니다.

고객의 고객, 환자 또는 연구 참여자인 승인된 개체는 IBM SaaS 에 데이터를 업로드하는 목적에 한해 액세스 권한을 제공받을 수 있으며 이 경우 해당 승인된 개체는 IBM SaaS 에 대한 기타 다른 액세스 권한은 없습니다.

8. 개인정보 보호정책

8.1 일반 요구사항

당사자 간에서 모든 고객 개인 데이터에 대한 단독 관리자는 고객이며 고객은 데이터 처리자로 IBM 을 지명합니다. 적용 데이터법에 따라 고객은 IBM 의 고객 개인 데이터 처리와 관련하여 IBM 에 지시할 수 있는 권리를 보유합니다.

IBM 이 고객 개인 데이터를 처리하는 범위 내에서, IBM 은 다음을 수행해야 합니다.

a. 모든 IBM 적용 데이터법을 준수합니다. 및

b. 다음을 제외하고, 기타 출처의 데이터와 고객 개인 데이터를 혼용하지 않습니다.

- 고객이 구체적으로 지시하지 않은 한, 기타 다른 용도는 아니고 IBM SaaS 를 제공하는 데 필요한 경우, 또는
- 본 이용 약관 및 SBCA 부록의 조항에 준하는 경우.

IBM 이 고객 개인 데이터를 처리하는 범위 내에서, 고객은 다음을 수행해야 합니다.

a. 모든 고객 적용 데이터법을 준수합니다.

b. 고객과 고객의 계열사, 환자, 일반 사용자, 데이터 주체 및/또는 기타 고객의 제 3 자와의 모든 의사 교환에 대해 책임을 집니다.

c. 데이터 처리자 및 관련 재처리자로서 IBM 이 고객 개인 데이터를 처리하는 데 필요한 데이터 처리 계약을 데이터 관리자와 체결합니다. 및

d. IBM 단일 접촉 창구의 역할을 수행하며 IBM 에 대한 기타 주관자인 고객 계열사의 지침이나 요청을 내부적으로 조정하고 검토하여 제출하는 데 전적인 책임을 집니다. IBM 은 고객에게 정보나 주의사항 제공 시 주관자가 되는 여하한의 고객 계열사에게 이를 알리거나 통지해야 할 의무는 없습니다. IBM 은 고객이 아니라 주관자가 된 고객 계열사가 직접 제공한 지침은 거부할 수 있습니다.

양 당사자는 상대방의 적용 데이터법을 위반하도록 요구해서는 안됩니다.

8.2 고객 데이터 권리

고객은 고객이 (a) IBM SaaS 에 입력할 데이터를 소유하고 있다거나 (b) 본 이용 약관 또는 본 계약에 명시된 조항에 따라 고객 데이터를 액세스, 사용 및 공개할 수 있는 권리를 IBM 에게 부여하기 위해 필요한 모든 권리, 권한, 동의 및 허가를 이미 취득하였고 이를 유지 관리해야 할 책임이 있다는 점을 진술하고 보증합니다. 고객은 또한 고객 데이터는 (a) 미국에서 거주하는 개인과 관련되고 미국 데이터 센터에서만 IBM SaaS 에 입력하게 되거나 (b) 범주 내 국가 중 하나 이상에서 거주하는 개인과 관련되고 지정 데이터 센터에서만 IBM SaaS 에 입력하게 되는 경우 중 하나의 경우에만 해당된다는 점을 보증하고 진술합니다.

8.3 데이터 서비스 및 책임사항

a. 고객은 HIPAA 및/또는 기타 적용 데이터법에 의거한 유사한 조항에 준하여 각각 정의된 고객의 "헬스 케어 운영" 또는 "리서치" 중 하나의 활동과 관련해서만 고객 데이터를 분석하거나 IBM 에게 분석을 수행하도록 요청할 것과 해당 및 기타 고객 적용 데이터법에 의거해서 관련된 모든 요구사항(예: 필요한 경우 기관 검토 위원회의 결정 또는 권리 포기)에 준해서만 고객 데이터를 사용하거나 IBM 에게 고객 데이터를 사용하도록 지시할 것에 동의합니다.

b. 고객과 IBM 및 IBM 의 허가된 하도급자가 본 이용 약관과 본 계약에 의거해서 고려한 바와 같이, IBM SaaS 에 고객 데이터를 입력하고 사용하고 공개하기 위해 HIPAA 및 기타 관련 데이터 보호정책, 보안 법령, 규칙 및 규정을 포함한(단, 이에 한하지 않음) 각 범주 내 국가의 고객 적용 법령(Client Applicable Laws)에서 요구한 바대로 모든 등록, 동의, 허가 및 권한을 획득해야 할 책임은 전적으로 고객에게 있습니다. IBM 은 그러한 등록, 동의, 허가 및 권한이 언제 제공되는지 또는 언제 필요한지에 대해 모니터링할 책임은 없습니다.

c. IBM SaaS 에 입력된 모든 고객 데이터가 미국 또는 해당 범주 내 국가에 거주하는 개인에 관한 데이터로 제한되는지 확인해야 할 책임은 전적으로 고객에게 있습니다.

d. IBM 은 범주 내 국가의 데이터와 관련하여 HIPAA 및 기타 IBM 적용 데이터법에 따라 훈련된 인력이 배치된 지원 센터를 보유해야 합니다.

8.4 보안 조치 및 보안 사고

a. IBM 은 (조직 프로세스 및 절차와 본 이용 약관 및 SBCA 에서 명시하거나 참조한 특정 보안 책임사항을 포함하여) 불법적인 사용이나 액세스, 분실 사고, 손상, 수정, 파기, 도난 또는 불법적인 공개로부터 고객 개인 데이터를 보호하기 위한 기술적 및 조직적 조치를 구현하고 유지 관리하고 준수해야 합니다.

b. IBM 은 고객 처리 데이터에 대한 보안 사고(SBCA 정의 참조)를 인지한 경우, SBCA 및 IBM 적용 데이터법의 조항에 따라 이를 고객에게 알려야 하며 그러한 통지에는 보안 사고가 고객이나 데이터 주체(해당하는 경우)에 미치는 알려진 영향 및 IBM 이 수행하였거나 수행하도록 제한된 시정 조치가 포함됩니다.

8.5 문의 및 불만 접수

IBM 은 다음으로부터 고객 개인 데이터와 관련하여 IBM Watson Health Data Privacy Officer 가 질문이나 의사 표시를 수신하거나 IBM 이 불만사항을 수신한 후 즉시, 그리고 IBM 적용 데이터법에서 허용하는 한, 5 영업일(business day) 이내에 고객에게 이를 서면으로 알려야 합니다.

a. 데이터 주체(IBM 이 처리한, 데이터 주체에 관한 개인 데이터 관련). 고객은 데이터 주체의 요청에 응답해야 하며 IBM 은 요청에 대한 고객의 응답을 지원하기 위해 고객의 합리적인 지시사항을 준수합니다. IBM 적용 법령(Client Applicable Laws)에서 요구한 경우, IBM 은 그러한 요청에 직접 응답할 수 있으며 단, IBM 적용 법령에서 허용하거나 달리 가능한 경우, 응답에 앞서 고객에게 통지하고 응답의 양식 및 내용에 관해 고객과 합리적으로 조정하는 것을 전제로 합니다.

b. 법률 기관 또는 규제 기관(고객 개인 데이터에 대한 IBM 의 처리 관련). IBM 은 정부 기관으로부터 수신한 요청에 대해 소환장이나 유사한 법문서 강제 공개를 통해, 또는 적용 데이터법에서 달리 요구한 대로 응답할 수 있으며 단, IBM 은 그러한 공개에 앞서 고객에게 통지하고 응답의 양식 및 내용에 관해 고객과 합리적으로 조정하는 것을 전제로 합니다.

8.6 고객 개인 데이터 처리

IBM 은 서비스를 제공하는 데 있어서 지원이 필요할 수 있는 해당 IBM 인력에게만 고객 개인 데이터를 공개하는 것으로 제한합니다.

IBM 은 적용 법령에 따라 고객 개인 데이터를 수정, 정정, 삭제 또는 차단하도록 요구하는 고객의 합리적인 요청을 준수해야 합니다.

IBM, 고객 또는 그 계열사는 일방 당사자의 요청에 따라 고객 개인 데이터를 보호하기 위해 법률에서 요구한 표준 계약을 체결합니다. 양 당사자는 그러한 계약이 양 당사자 간의 배상 청구 목적상, 본 계약의 책임 제한사항 및 제외사항에 적용된다는 데 동의(하고 각각의 계열사가 동의하도록)합니다. 양 당사자는 적용 데이터법에서 요구하는 대로 추가로 상호 합의된 조항이나 계약을 체결(하거나 당사자의 계열사가 체결하도록)하는 데 협력해야 하며 이를 준수해야 합니다.

8.7 고객 개인 데이터 반환

본 계약 만료 또는 종료 시, IBM 은 고객 독점 정보(Client Proprietary Information) 및 고객 개인 데이터(Client Personal Data)의 사용이나 처리를 중단하고 IBM 인력도 중단하도록 해야 하며 고객의 재량과 요청에 따라 다음을 수행해야 합니다.

a. IBM 이 전자적으로 저장 중인 모든 고객 소유의 정보 및 고객 개인 데이터를 고객이 합리적으로 요청하는 형식 및 저장 매체로 즉시 반환하고 고객의 수령을 확인한 후에는 사본과 백업을 포함한 고객 소유의 정보 및 고객 개인 데이터를 삭제하거나 파기하거나 달리 영구적으로 판독이나 해독이 불가능하도록 합니다. IBM 은 고객의 요청에 따른 저장 매체 및 특정 활동(고객 소유의 정보 및 고객 개인 데이터를 특정 형식으로 전달하거나 고객 소유의 정보 및 고객 개인 데이터를 특정 방식으로 파기하는 경우 등)에 대한 비용을 부과할 수 있습니다.

b. 사본 및 백업을 포함한 고객 소유의 정보 및 고객 개인 데이터를 직접 삭제하거나 파기하거나 달리 영구적으로 판독 또는 해독이 불가능하도록 합니다.

8.8 BAA(Business Associate Agreement)

적합한 범위 내에서 HIPAA 에서 요구되는 바에 따라, IBM 과 고객은 IBM SaaS 프로비저닝 시 고객의 비즈니스 파트너(Business Associate)로서 IBM 의 의무에 적용해야 하는 Business Associate Agreement(이하 "BAA")를 체결합니다. 본 계약 및 BAA 에 의거한 IBM 의 명시적인 의무를 제한함이 없이, 고객은 IBM SaaS 의 사용이나 기타 활동(승인된 사용자에 의한 사용이나 기타 활동 포함)에 적용되는 모든 적용 법령 및 라이센싱 요건의 적용성을 판단하고 이를 준수해야 할 책임은 고객에게 있다는 점을 인정하고 이에 동의합니다.

8.9 유럽 연합 데이터 처리 부칙

고객이 IBM 에게 유럽 연합 개인 데이터의 처리를 지시한 경우, IBM 과 고객은 선택 조항은 삭제되고 적절한 E.U. 모델 조항(Model Clauses)이 포함된 데이터 처리 부칙(Data Processing Addendum)을 체결합니다.

9. IBM SaaS 오퍼링 추가 조건

9.1 보안(Security)

이 IBM SaaS 는 IBM SaaS 에 관한 IBM 데이터 보안 및 개인정보 보호정책(http://www.ibm.com/cloud/data-security 참조) 및 아래와 본 이용 약관의 보안 및 비즈니스 연속성 부록에 명시된 추가 조항을 준수합니다. IBM 데이터 보안 및 개인 정보 보호 정책이 변경되더라도 IBM SaaS 의 보안 수준은 저하되지 않습니다.

IBM Watson Health Core 는 보안 명세(Security Description)에서 자세하게 기술한 바와 같이 ISO 27001 프레임워크에 따라 보안 정책, 보안 기준 및 보안 프로세스를 구현합니다. 해당 솔루션은 보안 기능 중에서 다음을 구현합니다.

a. 보안 작동 구역

IBM Watson Health Core 는 다중 보안 구역을 활용하여 데이터 온보딩(onboarding), 사용자 정의 애플리케이션 개발 등 클라우드 통합 지점을 관리하는 종심 방어 전략(defense in depth strategy)을 구현합니다.

b. 암호화

모든 고객 데이터는 저장(at rest) 시 및 진행(in flight) 시에 암호화됩니다. IBM Watson Health Core 에서 전송 중인 데이터(data in transit)는 모두 암호화됩니다. 공유 서비스는 암호화 키 관리를 제공합니다. IBM Watson Health Service 와 고객의 프록시 서버 간의 모든 네트워크 연결성 및 품질에 대한 책임은 고객이 부담합니다.

c. 보안 이벤트 모니터링

IBM 은 보안 정보 및 이벤트 관리, 로그 관리, 사고 포렌식, 위협 감지 및 취약성 관리에 필요한 보안 인텔리전스 플랫폼을 활용합니다.

d. ID 관리

- Watson Health Core 는 OpenID Connect 를 사용하여 대규모 환자 및 사용자를 관리하는 개방 표준 ID 제공자를 지원합니다.
- ID 제공자가 IBM 인 사용자 집단의 경우, Watson Health Core 는 적합한 디렉토리 서비스와 ID 관리 기능을 사용하여 인증을 처리합니다.

e. 강력한 인증 및 역할 기반 액세스

- Watson Health Core 는 고객이 싱글 사인온(SSO) 또는 디렉토리 서비스를 통합하는 메커니즘으로 SAML 을 통해 인증을 지원합니다.
- Watson Health Core 는 필요한 경우, 액세스 관리 솔루션 및 관련 구성요소를 활용하여 보안 정책을 관리합니다.
- Watson Health Core 는 소프트웨어 기반의 이중(two-factor) 인증을 지원합니다.
- Watson Health Core 는 필요에 따라 기본 역할 기반 액세스 제어를 제공합니다. Watson Health Core 는 역할 기반 액세스가 가능한 Application Programming Interface("API" 또는 "APIs")를 통해 연구, 사용자 프로파일, 역할 및 사용자 그룹의 구성을 지원합니다.

9.2 쿠키

고객은 IBM 이 IBM SaaS 의 정상적인 운영과 지원 과정에서 트랙킹(tracking) 및 기타 기술을 사용하여 IBM SaaS 사용과 관련된 개인 정보를 고객(귀하의 직원 및 계약직 직원)으로부터 수집할 수 있다는 것을 인정하고 이에 동의합니다. IBM 은 사용자 경험을 개선하거나 고객과의 상호작용을 조정할 목적으로 IBM SaaS 의 효율성에 대한 사용 통계와 정보를 수집합니다. 고객은 관련 법령에 따라 IBM, 다른 IBM 회사들 및 이들의 하도급자들에서, 그리고 IBM 및 IBM 하도급자들이 비즈니스를 수행하는 어떤 장소에서도,

상기의 목적으로 수집된 개인 정보를 IBM 이 처리하기 위해 필요한 동의를 이미 획득했거나 획득할 것임을 확인합니다. IBM 은 수집된 개인 정보에 접근하거나 갱신하거나 정정하거나 삭제하고자 하는 고객 직원 및 계약직 직원의 요청을 수용합니다.

9.3 혜택이 제공된 사업장

해당하는 경우, 세금은 고객이 IBM SaaS 의 혜택을 제공받는 것으로 고객이 정한 사업장을 기준으로 부과됩니다. 고객이 추가 정보를 제공하지 않는 한, IBM 은 IBM SaaS 주문 시 주요 혜택 사업장으로 제출한 비즈니스 주소에 따라 세금을 적용합니다. 고객은 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM 에 제공해야 할 책임이 있습니다.

9.4 연속 제공

고객은 연속 클라우드 제공 모델로 IBM 이 솔루션에서 작성하여 배치한 기능과 개선사항을 제공받을 수 있습니다.

9.5 백업 및 복원

IBM Watson Health Core 는 시스템 장애 발생 시 프로덕션 환경(Data Lake 및 Data Reservoir 저장소 포함)에서 마지막으로 알려진 양호한 상태로 고객 데이터 백업을 제공하여 서비스를 복구합니다.

9.6 고가용성(High Availability)

프로덕션 환경의 IBM Watson Health Core 구성요소는 워크로드 분배를 제공하고 단일 장애점(single point of failure)을 제거하기 위해 중복성의 클러스터된 데이터베이스 서버가 포함된 고가용성 구성으로 구현됩니다.

9.7 재해 복구

IBM 은 프로덕션 환경에서 다음과 같은 비즈니스 연속성 목표를 달성하도록 분산된 지역에 여러 개의 데이터 센터를 마련하여 재해 복구에 대처합니다.

- RTO – 재해 선언 후 36 시간 이내
- RPO – 고객 컨텐츠 손실 후 최대 24 시간 이내

9.8 평가 도구

IBM SaaS 는 확약된 서비스 레벨과 비교한 가용성 또는 가동 중단을 모니터링하고 측정하여 보고하는 종합 모니터링 솔루션을 사용합니다. 이 솔루션은 정적 가용성 및 트랜잭션 모두에 대해 글로벌 수준에서 사용자 응답과 사용자 경험을 시뮬레이션하고 추적합니다.

IBM SaaS 는 또한 전체 솔루션을 통한 메트릭, 이벤트 및 경보에 필요한 내부 모니터링 시스템을 사용합니다.

9.9 퍼블리시티(Publicity)

고객은 IBM 이 매스컴이나 마케팅 통신문에서 고객을 IBM SaaS 의 가입자로 공개적으로 언급할 수 있다는 데 동의합니다.

부록 A

1. IBM Watson Health Core

IBM Watson Health Core 는 IBM 적용 데이터법에 따라 PHI(Protected Health Information)(HIPAA 정의 참조) 및 IBM 이 소유하거나 관리하는 데이터 센터의 기타 건강 데이터를 저장하고 큐레이팅하고 처리하는 건강 데이터 사용(Health Data Enabled) PaaS(platform as a service), 개발 플랫폼 및 운영 서브시스템입니다. 고객은 아래 피처 및 기능을 사용하기 위해서는 IBM Watson Health Core 및 IBM Watson Health Core Access 에 대한 적절한 권한을 취득해야 합니다.

1.1 Watson Health Core 운영 환경

Watson Health Core 권한에는 고객이 건강 데이터를 처리할 수 있도록 설계된 세 가지 건강 데이터 사용 클라우드 운영 환경이 포함됩니다.

- 파일럿(Pilot)

  고객이 IBM SaaS 를 사용하여 애플리케이션을 개발하고 구축한 애플리케이션을 테스트할 수 있는 샌드박스 환경을 제공합니다. 파일럿 환경은 재해 복구, 고가용성 및 레코드 시스템 백업을 제외한 모든 HIPAA 보안 제어를 구현합니다.

- 프로덕션 환경(Production Environment)

  고객이 건강 데이터 워크로드를 배치할 수 있는 풀 스케일 환경을 제공합니다. 프로덕션 환경은 고가용성의 로드 밸런싱 환경이며 재해 복구 위치에서 장애 복구가 가능합니다.

- 재해 복구(Disaster Recovery)

  프로덕션 환경의 미러 복제본을 제공하며 별도의 데이터 센터 위치에 존재합니다.

1.2 애플리케이션 개발

IBM Watson Health Core 를 통해 애플리케이션을 개발하고 고객의 디바이스 또는 고객의 승인된 사용자의 디바이스에서 수집한 데이터 컬렉션을 보호할 수 있습니다. APIs 는 고객의 승인된 사용자(고객의 제 3 자 서비스 제공자 포함)가 애플리케이션의 개발 및 IBM SaaS 와의 데이터 교환에 사용할 수 있는 프로그램 인터페이스와 문서를 제공합니다. 고객이나 고객의 개발자가 APIs 를 사용하는 경우 API 개발자 요구사항이 적용됩니다.

- REST APIs

  Watson Health Core 는 Watson Health Core 플랫폼에 필요한 일련의 REST APIs 및 서비스를 제공합니다. API 기능에는 데이터 저장소 액세스 메커니즘, 데이터 큐레이션 서비스, 사용자 관리 및 감사 로그가 포함되며 단, 이에 제한되지 않습니다.

- Apple HealthKit 및 Apple ResearchKit

  Watson Health Core 는 iOS 기반 리서치 연구 목적의 Apple ResearchKit API 프레임워크와 웰니스 데이터를 캡처하는 Apple HealthKit 과의 통합을 지원합니다.

1.3 데이터 거버넌스

- 동의 관리

  Watson Health Core 는 환자나 연구 참여자가 제공한 동의를 캡처하는 프레임워크를 제공하며 개인이 동의를 사용하는(consent-enabled) 고객 애플리케이션을 통해 등록한 경우 데이터 페이로드와 별도로 동의 레코드를 안전하게 저장할 수 있습니다.

- 데이터 마스킹

  Watson Health Core 는 이름 식별자를 정형 데이터 페이로드에서 구분해 내는 기능을 제공합니다. Watson Health Core 는 프로그램 APIs 를 통해 클라우드에서 데이터를 수신합니다. APIs 에서는 환자나 개인의 이름 식별자를 나머지 데이터 페이로드에서 구분해 내어 별도의 암호화된 데이터

저장소에 저장할 수 있습니다. 데이터 페이로드에는 추후 출처 추적에 사용할 수 있는 익명 토큰이 지정됩니다.

1.4 건강 데이터 서비스

Watson Health Core 는 외인성 건강 데이터 및 기타 개인 정보를 포함한 정형 및 비정형 데이터의 수집, 저장 및 동기화 기능을 제공합니다.

- 데이터 인제스트

  Watson Health Core 는 프로그램 APIs 를 통해 환자 애플리케이션 또는 디바이스에서 데이터를 인제스트하는 기능을 제공합니다. Watson Health Core 를 통해 고객의 각 승인된 개체는 계약 기간 동안 연간 최대 25MB 의 데이터를 Health Core 에 업로드할 수 있습니다. 이 서비스는 개체당 일일 최대 10 회 업로드를 허용합니다.

- 운영 Data Lake

  원시 고객 데이터나 환자 데이터는 분석과 모델링에 사용되기 전까지 기본 양식으로 Watson Health Core 에 저장됩니다.

- ETL(Extract Transform Load)

  데이터는 운영 서브 시스템 내에서 정규화된 형식으로 변환됩니다. 헬스 케어용 산업 표준 기반 Enterprise Service Bus 를 사용하면 다양한 고객 애플리케이션과 프로토콜 간의 통합이 가능합니다.

- Data Reservoir

  데이터는 일단 큐레이팅되면 Data Reservoir 로 이동합니다. Watson Health Core 는 IBM Unified Data Model for Healthcare 측면을 사용하여 분석에 사용할 비즈니스 및 기술적 건강 데이터를 표준화합니다.

- Master Person Index

  Watson Health 는 여러 소스의 데이터를 통합하여 LPR(Longitudinal Person Record)를 작성하기 위한 마스터 데이터 관리(Master Data Management) 도구를 제공합니다.

2. 옵션 기능

2.1 IBM Watson Health Core Terminology Service

이 애드온(add-on) 서비스는 전체 Watson Health Cloud 애플리케이션에서 일관된 임상 용어를 사용하도록 하여 다양한 헬스 시스템 간의 데이터 통합 및 상호 운용성이 용이하게 합니다. 이 서비스는 다음과 같이 용어, 코드 시스템 및 정형 컨텐츠와 관련된 모든 태스크에 대한 기능적 플랫폼을 제공합니다.

- 새 코드 시스템 작성
- 국제 코드 시스템 변환, 및
- 로컬 코드 목록과 국제 표준 간 맵핑.

부록 B

IBM 은 라이센스 증서에 명시된 바와 같이 IBM SaaS 의 가용성에 관한 "서비스 레벨 계약"(이하 SLA)을 제공합니다. SLA 는 보증이 아닙니다. SLA 는 고객에게만 제공되며 프로덕션 환경의 사용에만 적용됩니다.

1. 가용성 크레디트

가용성 리베이트는 개별 권한에 대한 사용등록료에만 적용됩니다.

고객은 IBM SaaS 의 가용성에 영향을 준 이벤트를 처음으로 인지한 시점으로부터 24 시간 이내에 심각도 1 지원 티켓을 IBM 기술 지원 헬프 데스크에 로그(log)해야 합니다. 고객은 문제점의 진단과 해결에 있어서 합리적으로 IBM 을 지원해야 합니다.

SLA 미충족에 대한 지원 티켓 클레임은 약정 월 말일 이후 삼(3) 영업일 이내에 제출되어야 합니다. 유효한 SLA 클레임에 대한 보상은 IBM SaaS 의 프로덕션 시스템 처리가 불가능한 시간 동안의 지속 기간(이하 "Downtime")을 기준으로 IBM SaaS 의 추후 청구서에 대한 크레디트가 됩니다. Downtime 은 고객이 이벤트를 보고한 시간부터 IBM SaaS 가 복원된 시간까지로 측정되며 스케줄되거나 발표된 유지보수 중단 시간, IBM 의 통제를 벗어난 원인, 고객 또는 제 3 자 컨텐츠나 기술, 설계나 지침의 문제점, 지원되지 않는 시스템 구성 및 플랫폼 또는 기타 고객의 오류, 고객으로 인한 보안 사고 또는 고객 보안 테스트는 포함되지 않습니다. IBM 은 아래 표와 같이 각 약정 월 동안의 누적 IBM SaaS 가용성에 따라 적용 가능한 최대의 보상을 적용합니다. 약정 개월에 적용되는 보상의 총 금액은 IBM SaaS 에 대한 연간 대금의 12 분의 1(1/12)의 20%를 초과할 수 없습니다.

2. 서비스 레벨

약정 월 동안 IBM SaaS 가용성

약정 월 동안 가용성	**보상 (클레임 대상이 되는 약정된 월의 월별 개별 사용등록(subscription) 사용료*의 %)**
< 99.95%	10%
< 99.0%	20%

* IBM 비즈니스 파트너로부터 IBM SaaS 를 취득한 경우, 월 등록 사용료는 클레임 대상이 되는 약정 월에 유효한, 50%의 할인이 제공된 IBM SaaS 의 당시 적용되는 정가를 기준으로 산정됩니다. IBM 은 고객이 직접 사용할 수 있는 장려금을 제공합니다.

백분율로 표시된 가용성은 약정 월의 총 시간(분)에서 약정 월의 총 Downtime(분)을 차감한 후 이를 약정 월의 총 시간(분)으로 나누어 산출합니다.

예: 약정된 월의 총 Downtime 108 분

약정 월 30 일 동안 총 43,200 분 – Downtime 108 분 = 43,092 분 _____ 총 43,200 분	= 약정 월 동안 가용성 99.75%에 대한 가용성 크레디트 10%

3. 제외

본 SLA 는 다음에 적용되지 않습니다.

- 서버 모니터링은 제외하고, 본 SLA 는 사용자 정의 또는 고객 애플리케이션을 지원하는 호스팅된 가상 머신에는 적용되지 않습니다.
- 고객이 현재 계약 의무사항에 의거해서 중대한 의무를 위반한 경우.

부록 C

본 보안 및 비즈니스 연속성 부록(Security and Business Continuity Appendix, 이하 "SBCA")은 IBM 이 고객에게 IBM SaaS 를 제공하는 데 필요한 특정 요구사항과 IBM 의 의무에 대해 명시합니다. 이 부록에 명시된 요구사항과 의무는 IBM SaaS 데이터 보안 원칙 설명(http://www.ibm.com/cloud/data-security 참조)에 명시된 내용에 추가됩니다. 이 부록에 정의되지 않은, 대문자로 된 용어는 본 계약 또는 이용 약관에 명시된 의미와 동일하게 사용됩니다.

1. 정보 보안 프로그램

IBM 은 ISO 27001 프레임워크 및 관리 영역에 따른 내부적인 보안 정책, 표준 및 프로세스를 준수합니다. 이러한 정책, 표준 및 프로세스는 IBM Corporate Security Organization 거버넌스와 함께 정기 내부 감사의 대상입니다.

IBM 은 고객 컨텐츠의 처리, 저장 및 전송을 관리하는 조직적, 운영상, 관리적, 물리적 및 기술적 보호 조치의 정보 보안 프로그램을 유지 관리하며 해당 보호 조치는 최소한 이 SBCA 요건에 부합합니다.

IBM 은 고객이 IBM Watson Health 정보 보안 프로그램의 지속적인 적합성, 타당성 및 효율성을 합리적으로 판단할 수 있도록 고객의 요청에 따라 해당 정보 보안 프로그램에 대한 정보를 고객과 공유합니다. IBM Watson Health 정보 보안 프로그램은 일반적으로 채택된 산업 규정과 IBM 적용 법령에 맞게 수시로 업데이트됩니다.

2. 액세스 제어

IBM 은 적용 법령, 본 계약 또는 관련 문서에 따라 IBM SaaS 를 제공하는 데 필요에 따라 고객이나 기타 개인에 대한 IBM 의 의무 이행을 지원하기 위해 고객 컨텐츠에 액세스해야 하는 합법적인 비즈니스 필요가 있는 IBM 직원, 하도급자 또는 제 3 자에게만 고객 컨텐츠를 공개합니다. IBM 이 고객의 비즈니스 파트너(Business Associate)인 경우, IBM 과 고객은 양 당사자 간의 해당 BAA(Business Associate Agreement)의 조항에 준해서만 개인 건강 정보(Personal Health Information)를 공개합니다.

IBM 은 최소 권한 원칙에 따라, 사용자 액세스를 공식 요청하고 ID 확인 후 승인하며 알아야 할 필요성(need to know)에 따라 액세스 권한을 부여하는 공식 내부 사용자 액세스 관리 프로세스를 운영합니다. 고객 컨텐츠에 대한 액세스 권한은 활성 사용자 및 활성 사용자 계정으로만 제한됩니다. IBM 은 활성 사용자 계정에 대한 공식적인 정기 내부 액세스 권한 재평가 프로세스를 운영합니다.

IBM 은 IBM 회사 보안 표준 및 정책에 따라 고객에게 서비스를 제공하는 데 사용된 시스템의 활성 사용자 계정에 고유 ID 와 강력한 비밀번호를 지정하는 방법을 포함한 사용자 인증 보안 프로토콜을 사용합니다.

a. 비밀번호는 벤더가 제공한 기본 비밀번호를 사용해서는 안되며 비밀번호를 통해 보호하는 데이터의 보안을 훼손하지 않는 장소와 형식으로 보관해야 합니다.

b. 비밀번호의 표시 및 인쇄는 허가를 받지 않은 당사자가 알아보거나 추후 복원할 수 없도록 가리거나 숨기거나 달리 모호하게 해야 합니다. 비밀번호를 입력하면서 비밀번호를 로그(log)하거나 캡처해서는 안됩니다. 사용자 비밀번호를 일반 텍스트로 저장해서는 안됩니다.

c. IBM SaaS 를 구성하는 각 기술의 비밀번호는 알려진 비밀번호 길이 취약성에 따른 위험을 완화하도록 선택하고 반드시 기록해야 합니다.

d. 운영상의 이유로, 내부, 권한 부여된, 공유 기능 ID 를 사용해야 하는 경우, IBM 은 개별 계정성이 유지되도록 비밀번호 체크아웃을 요구하여 공유, 기능 및/또는 시스템 ID 를 관리합니다.

고객 컨텐츠를 저장하는 모든 시스템과 애플리케이션에는 비활성 제한시간을 설정합니다.

필요한 경우, 고객 컨텐츠를 저장한 IBM 의 네트워크, 시스템 및 애플리케이션에 대한 원격 액세스는 고객의 요청에 따라 IBM 이 공식 승인한 후 설정해야 하며 이러한 모든 원격 액세스는 강력한 인증 및 암호화 프로토콜을 통해 보호됩니다. 원격 액세스 활동을 로그(log)하고 모니터링합니다.

IBM SaaS 를 제공하기 위해 IBM 이 고객의 내부 네트워크 내에 있는 시스템에 원격으로 액세스해야 하는 경우에 한해서, 모든 원격 액세스는 고객의 보안 원격 액세스 시스템과 프로토콜 및 고객이 IBM 에게 제공한 액세스 신임 정보를 통해서만 수행됩니다. 고객의 네트워크에 대한 원격 액세스는 IBM 의 요청에

따라 고객이 승인한 후에만 설정해야 하며 IBM 에게 미리 제공한 고객의 당시 현행 정책을 준수합니다. IBM 이 고객의 내부 네트워크를 사용하는 경우 IBM 에게 미리 제공한 고객의 IT 사용 및 보안 정책이 적용됩니다.

IBM 은 보안 관리, 액세스 검토 및 보안 위반 행위 조사에 있어서 업무 분리 원칙을 준수합니다.

고객의 고유 고객 컨텐츠에 대한 저장, 호스팅 및 처리는 IBM 이 제공한 다른 고객의 컨텐츠와는 논리적으로 별개입니다. IBM 은 고객에 의해 공유 저장, 호스팅 또는 처리 작업 영역이 허가된 인스턴스에서 고객 컨텐츠를 불법적으로 공개하지 못하도록 SBCA 에 명시된 요구사항에 맞게 설계된 적절한 절차와 보호 조치를 사용합니다.

IBM 은 고객 컨텐츠가 어떠한 경우에도 공용 장소에서 방치되지 않도록 클린 데스크/클린 스크린 정책을 구현합니다.

3. 전송 및 암호화

IBM 은 고객 컨텐츠 전송 시(팩스, 이메일, 택배 등 사용) 올바른 수신인 주소를 사용하는지 확인하고 지정된 수신인과 사전에 협의하여 해당 정보를 안전하게 수신하도록 적절한 예방 조치를 취해야 합니다.

IBM 은 고객 컨텐츠를 전송, 통신, 원격 액세스 또는 저장(백업 저장 포함)하는 경우를 포함하여 고객 컨텐츠 처리 시 언제든지 적절한 양식의 암호화 또는 기타 보안 기술을 사용하며 IBM 인력도 이를 사용하도록 합니다. 예를 들어, IBM 은 적절한 산업 표준 암호화를 사용하여 다음 고객 컨텐츠가 포함된 모든 레코드 및 파일을 암호화해야 합니다.

a. IBM 랩탑, 휴대용 디바이스 또는 오프사이트 저장 시설로 전송 시 백업 테이프를 포함한 휴대용 전자 매체에 저장된 컨텐츠,

b. 하드카피 문서를 제외하고, IBM 이 물리적으로 보안된 고객 또는 IBM 사무실 및 시설 외부에서 저장하거나 전송한 컨텐츠,

c. IBM 이 공용 네트워크를 통해 이동하는 동안,

d. IBM 시스템에서 고객에게 전송하는 동안,

e. IBM 이 무선으로 전송하는 동안, 및

f. IBM 이 서버 및 데이터베이스에서 저장한 컨텐츠.

4. 네트워크 보안

IBM 은 방화벽, 프록시, 웹 애플리케이션 방화벽 및 인터페이스와 같은 시스템 보안 소프트웨어의 적절한 최신 버전을 사용합니다. 해당 소프트웨어에는 멀웨어 방지 기능 및 적절한 최신 패치와 바이러스 정의가 포함되어 있어야 합니다. 기업 표준에 따라 안티바이러스 소프트웨어는 기술적으로 실행 가능한 워크스테이션, 서버 및 관련 엔드포인트에 설치되어야 하며 해당 소프트웨어는 내부 관리 솔루션을 사용하여 회사 정책에 따라 관리됩니다.

IBM 은 가능한 한 사전에 보안 사고를 발견하여 식별하도록 IBM SaaS 를 모니터링합니다. IBM 은 고객에게 서비스를 제공하는 데 사용되는 고객 컨텐츠 또는 정보 시스템의 불법적인 공개, 오용, 변경 또는 파손을 초래할 수 있는 내외부의 취약성 및 위험성을 식별하도록 설계된 최소한의 산업 표준 침입 감지 도구 및 방지 조치, 모니터링 및 대응 절차를 유지 관리합니다.

IBM 은 시스템 취약성에 관한 최신 정보를 제공하는 취약성 인텔리전스 서비스, 정보 보안 어드바이저 및 기타 관련 소스에 가입합니다. IBM 은 IBM 네트워크에 대한 정기 취약성 평가 및 구제책을 수행합니다.

IBM 은 보안 사고를 감지하고 식별하고 억제하며 해결하도록 IBM SaaS 를 모니터링합니다.

IBM 은 IBM 릴리스 관리 프로세스를 통해 IBM SaaS 가 가용케 된 네트워크 보안 인프라스트럭처의 가용성, 무결성 및 효율성을 검증합니다.

5. 사고 관리 및 알림

IBM Watson Health 팀은 IBM 오퍼링과 관련된 보안 사고의 접수, 조사 및 내부 조정을 관리하는 글로벌 팀인 IBM 사이버 보안 사고 대응 팀과 협력하여 소프트웨어 관련 보안 문제를 줄이기 위한 예방책을 구현하도록 지원합니다. "보안 사고"는 IBM 이 IBM SaaS 를 제공하는 데 사용한 정보 시스템에서 시스템 운영이나 데이터에 대한 불법적인 액세스, 사용, 공개, 수정 또는 개입이 발생한 상황입니다. 보안 사고를

감지한 경우(루틴 스캐닝, 경보, 스레드 이벤트 등을 통해), IBM 은 고객에게 다음과 같이 알리고 통지합니다.

a. 고객 컨텐츠와 관련하여 확인된 보안 사고에 대해 실행 가능한 한 신속히 그리고 보안 사고 조사 및 확인 후 최대 2 영업일(business days) 이내에,

b. 법령 또는 관련 명령에서 달리 금지하지 않는 한, 고객 컨텐츠의 액세스 권한 또는 정보에 대한 정부 공무원(정보 보호 기관 또는 법집행 기관 포함)의 요청에 따라 즉시, 그리고

c. 본 SBCA 의 액세스 제어 절에서 허용한 경우는 제외하고, 제 3 자에 의한 또는 제 3 자에 대한 고객 컨텐츠의 사전 공개, 전송 또는 액세스에 앞서.

6. 로깅(Logging)

IBM 은 IBM 의 정책과 규정 및 일반적으로 채택된 산업 규정에 따라 고객 처리 데이터에 대한 불법적인 사용이나 액세스에 대한 합리적인 시스템 모니터링을 유지 관리합니다. 실제 로그온 또는 시도된 로그온 위반 및 액세스 위반 행위를 로그(log)합니다.

IBM 은 HIPAA 및 기타 IBM 적용 데이터 법령에서 요구하는 한, 고객 데이터 및 건강 데이터를 저장, 액세스, 처리 및 전송하는 모든 시스템에 대한 모든 액세스 요청 레코드 및 액세스 활동 로그(log)를 유지 관리합니다.

로그(log) 및 보고서에는 최소한 다음 사항이 포함됩니다: (i) 성공 여부에 관계 없이, 적절한 식별 정보를 포함한 모든 로그인 시도, (ii) 애플리케이션 설치, 사용자 관리 변경사항, 파일 액세스 권한 변경사항을 포함하여 모든 시스템 및 네트워크 구성 변경사항, (iii) 성공 여부에 관계 없이, 파일, 네트워크 공유, 로그 또는 기타 자원에 대한 액세스 시도를 포함한 자원 액세스 시도, 및 (iv) 다운로드 실행에 사용된 데이터 및 프로토콜의 컨텐츠 유형을 포함한 데이터 다운로드.

7. 소프트웨어 애플리케이션 개발 및 변경 관리

IBM 은 테스트되지 않은 불법적 개조로부터 프로덕션 애플리케이션 및 관련 소스 코드의 무결성을 보호하는 보안 애플리케이션 개발 및 코딩 관행을 준수합니다.

IBM 은 (a) 변경사항 기록 및 공식 승인, 및 취소 절차, 및 (b) 적절한 경우 보안 테스트와 함께 사용자 승인 테스트를 포함하여, 적절한 변경사항 테스트가 포함된 변경 관리 프로세스를 준수합니다.

IBM 은 고객 컨텐츠를 저장, 액세스 및 전송하거나 IBM SaaS 를 포함한 서비스를 고객에게 제공하는 데 사용된 모든 시스템에 설치하기 전에 테스트 패치가 포함된 패치 관리 프로세스를 준수합니다.

IBM 은 고객 컨텐츠를 저장, 액세스 및 전송하는 데 사용된 모든 정보 시스템의 구성과 관련하여 시스템 관리자가 완전하고 정확한 최신 정보를 유지하도록 요구합니다.

8. 물리적 보안 및 환경 보안

IBM Watson Health Core 플랫폼은 IBM SoftLayer 데이터 인프라스트럭처에서 배치됩니다. IBM SoftLayer 는 고객 데이터를 사용자, 환경 및 기술적 위반이나 영향으로부터 보호하는 물리적 및 환경적 보안, 액세스 제어, 관리 및 프로세스를 유지 관리합니다.

IBM SaaS 가 호스팅된 시설의 일반 액세스 권한은 카드 액세스 시스템을 통해 제어됩니다. 사이트 전체에 CCTV 카메라를 설치하여 보안 직원이 모니터링합니다. 채택한 액세스 도어에는 경보 장치를 설치하고 보안 직원이 경보를 모니터링합니다.

통제 구역에 대한 접근 권한은 카드 액세스 및/또는 추가적인 생체인식 확인을 통해 제한됩니다. 통제 구역에 대한 허가된 접근 권한이 없는 모든 개인은 반드시 등록해야 하며 승인된 통제 구역 접근 권한이 있는 안내자가 동행합니다. 모든 통제 구역 비상구에는 경보 울림 장치가 설치되어 있으며 보안 직원이 경보를 모니터링합니다. 경보 작동에 대해 정기 점검을 수행하여 문서화하고 이를 보관합니다. 분기별로 통제 구역에 대한 접근 권한을 정식으로 재평가합니다. 고용 기간이 종료되고 나면 통제 구역에 대한 접근 권한이 취소됩니다.

화재, 수해, 화재 경보, 소화기, 연기 탐지기, 화재 방지 및 소화 시스템에 따른 열기 등의 환경 요인으로부터 시설을 보호합니다. 정기적으로 유지보수하고 테스트하는 UPS(Uninterruptible Power Supply) 시스템 및 백업 생성기를 통해 전원 공급 중단 또는 장애로부터 시설을 보호합니다.

IBM SoftLayer 준수 정보 및 보고서는 http://www.softlayer.com/compliance 에서 확인할 수 있습니다.

9. 비즈니스 운영 연속성

IBM 은 본 계약에 의거한 의무에 부합하는 서비스 수준을 유지하도록 설계된 비즈니스 연속성 및 재해 복구 계획을 운영합니다. 해당 비즈니스 연속성 및 재해 복구 계획은 정기적으로(최소 1 년에 한 번) 업데이트되고 테스트됩니다. IBM 은 일반적으로 채택된 업계 관행에 대한 준수를 유지하는 데 필요한 비즈니스 연속성 및 재해 복구 계획에 대한 적절한 모든 변경을 구현합니다. 각 경우, 사용 중인 IBM SaaS 또는 프로덕션 환경에 대한 고객의 부적절한 개입은 없습니다.

재해가 발생하여 고객이 IBM SaaS 를 사용할 수 없게 된 경우, IBM 은 고객에게 이를 즉시 통지하고 비즈니스 연속성 및/또는 재난 복구 계획을 활성화합니다. 재해 선언 시, IBM SaaS 비즈니스 연속성 목표는 IBM SaaS 에 대한 고객의 액세스 권한을 다음과 같이 복원하는 것입니다. 가동 중단의 경우, IBM Watson Health 프로덕션 환경을 복원하는 RTO(Recovery Time Objective)는 재해 선언 후 36 시간 이내입니다. RPO(Recovery Point Objective)는 프로덕션 환경 내에서 고객 컨텐츠를 유실한 후 최대 24 시간입니다. 구체적인 Watson Health 솔루션 비즈니스 연속성 목표는 다를 수 있습니다.

IBM 은 분산 지역에 여러 데이터 센터를 마련하여 재해 복구에 대처합니다.

모든 IBM SoftLayer 데이터 센터는 다중 전원 피드, 파이버 링크, 전용 발전기 및 배터리 백업을 유지 관리합니다. 데이터 센터는 최고 수준의 성능, 신뢰성 및 상호 운영성을 제공하는 업계 선두의 하드웨어와 설비로 구축됩니다. 데이터 센터 내에서 안정성을 유지하도록 모든 데이터 센터 구성요소(중복 n+1 전원 및 쿨링 자원 포함)를 점검합니다.

10. 준수

IBM 보안 규정은 ISO 27001-27002 를 기반으로 합니다. 이 규정은 위험 분석(Risk Analysis), 물리적 보안(Physical Security), 긴급 계획(Emergency Planning), 조사(Investigations), 정보 보호(Information Protection), 교육(Education), 데이터 보호(Data protection) 및 운영(Operations)(단, 이에 한하지 않음)에 대한 관리 구성을 제공합니다.

IBM 은 IBM 보안 규정을 준수하기 위해 보안 및 개인 정보 보호 관련 활동을 검토합니다.

IBM 은 범주 내 국가에서 IBM 적용 데이터법을 준수합니다.

고객의 기밀 정보도 IBM 비즈니스 행동 지침(Business Conduct Guidelines)에 의거해서 적절하게 처리해야 합니다. 모든 직원은 해당 지침을 매년 검토(하고 검증 사실을 증명)해야 합니다.

11. 기타 조항

IBM 은 IBM SaaS 의 제공에 참여하는 모든 하도급자 및/또는 제 3 자와의 계약에 최소한 본 SBCA 및 관련 문서에서 보호하는 수준으로 고객의 컨텐츠를 보호하는 조항이 있는지 확인해야 합니다. 각 경우 해당 조항이 그러한 하도급자 및/또는 제 3 자가 수행할 서비스에 적용 가능한 경우에 한합니다.