IBM 클라우드 서비스 명세

IBM OpenPages GRC on Cloud

다음은 주문자용 서비스 명세입니다.

1. 클라우드 서비스

클라우드 서비스 오퍼링은 아래 설명되어 있으며 선택되어 권한이 부여된 오퍼링은 주문서에 지정되어 있습니다. 주문서는 제공된 견적서와 클라우드 서비스의 시작일과 기간 및 청구서 작성을 시작하는 시점을 명시한 귀하가 수령할 라이센스 증서로 구성됩니다.

1.1 IBM OpenPages GRC on Cloud

IBM OpenPages GRC on Cloud(필수 구성요소)는 엔터프라이즈 전체의 리스크 및 준수 이니셔티브를 식별, 관리, 모니터링, 보고하는 기능을 수행하는 Operational Risk Management 의 표준 구성을 제공합니다. 해당 오퍼링을 사용하여 RCSA(risk and control self assessments)를 포함한 모든 리스크 데이터, 손실 이벤트, 시나리오 분석, 외부 손실, KRI(key risk indicator)를 단일한 통합 모듈로 통합할 수 있습니다.

Operational Risk Management 기능은 다음과 같습니다.

- 주요 기능:
  (1) 리스크 식별, 측정 및 완화를 가능하게 함.
  (2) 내부 통제 테스트 및 문서화를 가능하게 함.
- 다음 활동을 수행할 수 있게 하는 손실 이벤트:
  (1) 운영 장애를 초래할 수 있는 내외부 이벤트의 추적, 평가 및 관리.
  (2) 운영 손실과 관련된 여러 영향 이벤트 및 복구 관리.
- 외부 손실 이벤트는 IBM Algo FIRST, ORX(Operational Risk data eXchange Association) 및 ORIC(Operational Risk Consortium) 손실 데이터베이스(별도 등록 필수)에서 손실 데이터를 IBM OpenPages Operational Risk Management 로 가져와서 시나리오 분석, 벤치마킹 및 보고서 생성을 수행하는 기능을 제공합니다. 귀하는 손실 데이터를 분석 도구나 자원 할당 애플리케이션으로 내보낼 수도 있습니다.
- 리스크 조건 또는 경향의 상태나 존재 여부를 잠재적으로 보여 주는 성과 수치를 추적할 수 있는 KRI
- 특정 리스크(특히, 빈도가 낮고 심각도가 높은 이벤트)를 식별하고 측정할 수 있는 평가 기술인 시나리오 분석.
- 보고, 모니터링 및 분석
- IBM SoftLayer 클라우드 구현.

1.2 IBM OpenPages GRC Non-Production Instance on Cloud

IBM OpenPages GRC Non-Production Instance on Cloud 는 내부 개발과 테스트 활동을 위해 클라우드 서비스의 비프로덕션 인스턴스를 제공합니다.

1.3 IBM OpenPages GRC Data Storage on Cloud

IBM OpenPages GRC Data Storage on Cloud(필수 구성요소)는 귀하의 클라우드 서비스 인스턴스에 필요한 GRC 데이터의 스토리지를 제공합니다. 스토리지는 할당량 150 GB 단위로 판매됩니다.

1.4 IBM OpenPages GRC Administrator User on Cloud

IBM OpenPages GRC Administrator User on Cloud(최소 한 가지 필수) 사용자는 클라우드 서비스의 Operational Risk Management 기능과 함께 모든 관리 기능에 액세스할 수 있습니다.

1.5 IBM OpenPages Operational Risk Management User on Cloud

IBM OpenPages Operational Risk Management User on Cloud 사용자는 위에 설명된 Operational Risk Management 기능에만 상호작동할 수 있습니다.

1.6 IBM OpenPages GRC Operational Risk Management Jump Start on Cloud

IBM OpenPages GRC Operational Risk Management Jump Start on Cloud(필수 구성요소)는 클라우드 서비스의 초기 구현 관련 서비스를 제공하고 프로젝트 계획, 유지 및 관리, 입증된 규례의 검토를 위한 초기 코칭 및 지원을 제공합니다.

2. 보안 설명

2.1 보안 정책

IBM 은 IBM 직원에게 통지하는 개인 정보 보호 및 보안 정책을 유지 관리합니다. IBM 은 IBM 데이터 센터를 지원하는 직원에게 개인 정보 보호 및 보안 교육을 받도록 요구합니다. IBM 에는 정보 보안 팀이 구성되어 있습니다. IBM 보안 정책 및 기준은 매년 검토되어 재평가됩니다. IBM 보안 문제는 종합적인 사고 대응 절차에 따라 처리됩니다.

2.2 접근 권한 통제

고객 데이터에 대한 접근이 필요한 경우, 업무 분리 원칙에 따라 권한이 부여된 IBM 지원 담당자만 접근할 수 있습니다. IBM 직원(또는 그에 준하는)은 중간 "게이트웨이" 관리 호스트에 대한 이중(two-factor) 인증 방식을 사용합니다. 고객 데이터 접속 시 모든 연결은 암호화된 채널로 제공됩니다. 고객 데이터에 대한 접근과 호스팅 환경 내외부로의 데이터 전송은 모두 기록됩니다. 이 클라우드 서비스를 지원하는 IBM 데이터 센터 내부에서는 WIFI 사용이 금지됩니다.

2.3 서비스 무결성 및 가용성

운영 체제와 애플리케이션 소프트웨어를 수정하려면 IBM 변경 관리 프로세스를 준수해야 합니다. 방화벽 규칙의 변경도 변경 관리 프로세스에 따라 수행되며 변경사항을 구현하기 전에 IBM 보안 직원(또는 그에 준하는)이 검토합니다. IBM 은 데이터 센터를 24x7 원칙으로 감시합니다. 허가된 관리자와 제 3 자 벤더는 내외부 취약성 스캔닝을 정기적으로 실시하여 잠재적인 시스템 보안 문제를 발견하고 해결할 수 있도록 지원합니다. 모든 IBM 데이터 센터에는 악성 소프트웨어 감지(안티바이러스, 침입 감지, 취약성 스캐닝 및 침입 방지) 시스템이 사용됩니다. IBM 데이터 센터 서비스는 공용 네트워크에서 데이터를 전송하기 위해 다양한 정보 전달 프로토콜을 지원합니다. 예를 들면, HTTPS/SFTP/FTPS/S/MIME, site-to-site VPN 이 있습니다. 오프 사이트 저장 목적의 백업 데이터는 전송되기 전에 암호화됩니다.

2.4 활동 로깅

IBM 은 활동 로깅 용도로 구성된 시스템, 애플리케이션, 데이터 저장소, 미들웨어 및 네트워크 인프라스트럭처 디바이스의 활동 로그를 유지 관리합니다. 로그의 조작을 방지하고 중앙 집중적 분석, 경보 및 보고 기능을 수행할 수 있도록 활동 로깅은 중앙 로그 저장소에서 실시간으로 처리됩니다. 조작 방지를 위해 데이터는 서명됩니다. 이상 동작을 찾기 위해 정기 분석 보고서를 통해 로그를 실시간으로 분석합니다. 운영 직원(또는 그에 준하는)에게 이상 동작을 경보로 통지하고 필요한 경우 24x7 on-call 보안 전문가에게 문의합니다.

2.5 물리적 보안

IBM 은 IBM 데이터 센터에 대한 불법적인 물리적 접근을 제한하기 위해 마련된 물리적 보안 기준을 유지 관리합니다. 데이터 센터에 대해서는 이중 인증 방식과 감시 카메라를 통한 통제와 모니터링이 적용되는 제한적인 접근 지점만 제공됩니다. 데이터 센터에 대한 접근은 접근 권한이 승인된 직원(또는 그에 준하는)만 가능합니다. 운영 직원(또는 그에 준하는)은 승인 여부를 검증한 후 접근 권한을 부여하는 액세스 배지를 발행합니다. 해당 액세스 배지를 획득한 직원은 기타 상이한 액세스 배지는 포기해야 하며 활동 기간에만 데이터 센터 액세스 배지를 소유할 수 있습니다. 액세스 배지의 사용은 기록됩니다. 비 IBM 방문자는 근무지 사이트에 입장 시 등록을 해야 하고 근무지 사이트에 있는 동안 안내자가 동행합니다. 권한이 없는 개인이 현장을 방문할 수 있는 서비스 제공 지역, 물류장 및 기타 지점은 관리 하에 격리됩니다.

2.6 준수

IBM 은 프로덕션 데이터 센터에서 매년 업계 표준 SSAE 16 감사(또는 그와 동등한 감사)를 실시합니다. IBM 은 IBM 비즈니스 요건을 준수하기 위해 보안 및 개인 정보 보호 관련 활동을 검토합니다. IBM 팀은 정기적인 평가와 감사를 통해 정보 보안 정책을 준수하는지 여부를 확인합니다. IBM 직원과 공급업체 직원은 매년 보안 인식 교육을 받습니다. 업무 윤리 강령, 기밀 보호 및 IBM 보안 의무를 준수할 수 있도록 업무 목표와 책임사항을 직원에게 매년 숙지시킵니다.

3. 서비스 레벨 확약

IBM 은 클라우드 서비스의 가용성에 관한 "서비스 레벨 계약"(이하 SLA)을 제공합니다. 귀하는 SLA 가 귀하에게 보증을 제공하는 것이 아님을 이해합니다.

3.1 용어 정의

a. "가용성 크레디트"는 유효한 클레임에 대해 IBM 이 제공하는 배상을 의미합니다. 가용성 크레디트는 클라우드 서비스 등록료를 청구하는 추후 청구서에 대한 크레디트 또는 할인의 형식으로 적용됩니다.

b. "클레임"은 계약 월 동안 서비스 레벨에 부합하지 못한 경우, SLA 에 따라 IBM 에 제출하는 클레임을 의미합니다.

c. "계약 월"은 해당 월 1 일의 12:00 AM(미 동부시)부터 해당 월 말일의 11:59 PM(미 동부시)까지, 해당 기간 동안의 매월을 의미합니다.

d. "중지 시간"은 클라우드 서비스에 대한 프로덕션 시스템 처리가 중지되고 권한을 가진 사용자가 클라우드 서비스의 모든 부문을 전혀 이용할 수 없는 기간 시간을 의미합니다. 중지 시간에는 다음으로 인해 클라우드 서비스를 사용할 수 없는 기간은 포함되지 않습니다.

   (1) 스케줄되거나 통지된 유지보수 목적의 가동 중단

   (2) IBM 의 통제권을 벗어난 이벤트 또는 원인(예: 자연 재해, 인터넷 중단, 긴급 유지보수 등);

   (3) 귀하의 애플리케이션, 설비, 데이터 또는 제 3 자의 애플리케이션, 설비, 데이터와 관련한 문제;

   (4) 필수 시스템 구성 및 클라우드 서비스 액세스를 위한 지원 플랫폼을 이용하지 않은 경우;

   (5) 귀하가 IBM 에게 제공하거나 귀하를 대신한 제 3 자가 IBM 에 제공한 설계, 명세 또는 지침을 IBM 이 따른 경우.

e. "이벤트"는 결과적으로 서비스 레벨에 부합하지 못하게 된 특정 상황 또는 함께 발생한 여러 상황을 의미합니다.

f. "서비스 레벨"은 본 SLA 에서 IBM 이 제공하는 서비스의 레벨을 IBM 이 측정하도록 아래와 같이 설정된 표준을 의미합니다.

3.2 가용성 크레디트

a. 클레임을 제출하기 위해서는 이벤트가 귀하의 클라우드 서비스 사용에 영향을 준 것을 귀하가 처음으로 인식한 시간으로부터의 24 시간 이내에 각 이벤트에 대해 심각도 1 지원 티켓(아래 기술 지원 조항에서 정의된 사항 참조)을 IBM 기술 지원 헬프 데스크에 기록해야 합니다. 귀하는 이벤트에 대한 필요한 정보를 모두 제공하고 이벤트의 진단과 해결을 위해 합리적인 범위 내에서 IBM 에 협력해야 합니다.

b. 귀하는 클레임이 발생한 계약 월의 말일로부터 최소 3 영업일 이전에 가용성 크레디트에 대한 귀하의 클레임을 제출해야 합니다.

c. 가용성 크레디트는 중지 시간이 최초로 발생했다고 귀하가 보고한 시점부터 측정된 중지 시간의 기간을 기준으로 합니다. 유효한 각 클레임의 경우, IBM 은 아래 표와 같이 각 계약 월 동안 달성한 서비스 레벨에 따라 적용 가능한 최대의 가용성 크레디트를 적용합니다. IBM 은 동일한 계약 월에서 동일한 이벤트에 대해 복수의 가용성 크레디트를 제공하지 않습니다.

d. 어떠한 경우에도 계약 월에 적용되는 가용성 크레디트의 총 금액은 귀하가 IBM 에 클라우드 서비스 대가로 지불한 연간 대금의 12 분의 1(1/12)의 10%를 초과하지 않습니다.

3.3 서비스 레벨

계약 당월 동안 클라우드 서비스 가용성

계약 당월 동안 가용성	가용성 크레디트 (클레임 대상이 되는 계약 월의 월 등록(Subcription) 사용료의 %)
< 98%	2%
< 97%	5%
< 93%	10%

백분율로 표시된 가용성은 (a) 계약 월의 총 시간(분)에서 (b) 계약 월의 총 중지 시간(분)을 뺀 후 이를 (c) 계약 월의 총 시간(분)으로 나누어 산출합니다.

예제: 계약 당월 동안 총 중지 시간 900 분

계약 월 30 일 동안 총 43,200 분
- 중지 시간 900 분
= 42,300 분

총 43,200 분

= 달성한 서비스 레벨 97.9%에 대한 가용성 크레디트 2%

3.4 SLA 에 대한 기타 정보

본 SLA 는 IBM 의 고객에게만 제공되며 클라우드 서비스에 대한 귀하의 사용자, 게스트, 참여자 및 허용된 초청객이 청구한 클레임 또는 IBM 이 제공한 베타 서비스나 시험 서비스에는 적용되지 않습니다. SLA 는 프로덕션 용도의 클라우드 서비스에만 적용됩니다. 테스트, 재해 복구, 품질 보증 또는 개발을 포함한(단, 이에 한하지 않음) 비 프로덕션 환경에는 SLA 가 적용되지 않습니다.

4. 권한 부여 및 대금 청구 정보

4.1 과금 체계

클라우드 서비스는 주문서에 지정된 바와 같이 다음 중 하나의 과금 체계 하에서 제공됩니다.

a. 허가된 사용자(Authorized User)는 클라우드 서비스 오퍼링 구입 시 사용되는 측정 단위입니다. 귀하는 어떠한 방법으로든(예: 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 클라우드 서비스에 접속할 수 있는 액세스 권한이 부여된 각 고유한 허가된 사용자에 대해 별도의 전용 권한을 취득해야 합니다. 귀하의 주문서에 명시된 측정 기간 동안 클라우드 서비스에 대한 액세스 권한이 제공된 허가된 사용자 수를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

b. 인게이지먼트(Engagement)는 서비스 구입 시 사용되는 측정 단위입니다. 인게이지먼트는 클라우드 서비스와 관련된 전문 서비스 및/또는 교육 서비스로 구성됩니다. 각 인게이지먼트(Engagement)를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

c. 기가바이트(Gigabyte)는 클라우드 서비스 구입 시 사용되는 측정 단위입니다. 기가바이트는 2 의 30 승 데이터(1,073,741,824 바이트)로 정의됩니다. 귀하의 주문서에 명시된 측정 기간 동안 클라우드 서비스에서 처리한 총 기가바이트 수를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

d. 인스턴스(Instance)는 클라우드 서비스 오퍼링 구입 시 사용되는 측정 단위입니다. 하나의 인스턴스는 클라우드 서비스의 특정 구성에 대한 액세스를 의미합니다. 주문서에 명시된 측정 기간 동안 액세스하여 사용하도록 제공된 클라우드 서비스의 각 인스턴스에 대해 충분한 권한을 취득해야 합니다.

4.2 대금 및 청구

클라우드 서비스에 대해 지불하는 대금은 주문서에 명시됩니다.

4.3 설치(Set-Up) 요금

표준 설치 서비스 및 관련 요금은 IBM OpenPages Operational Risk Management Jump Start on Cloud 오퍼링을 통해 제공됩니다.

만일 귀하가 추가 구성이나 추가 서비스가 필요한 경우에는 귀하는 보충 작업명세서를 통해 IBM OpenPages GRC on Cloud 서비스에 가입해야 합니다.

4.4 월 분할(Partial Month) 요금

월 분할 요금은 비례 배분된 일일 요금입니다. 월 분할 요금은 IBM 이 클라우드 서비스 오퍼링에 대한 액세스를 허용하여 이를 귀하에게 통지한 날부터 해당 월의 나머지 일수를 기준으로 계산합니다.

4.5 추가 요금

측정 기간 동안 귀하의 클라우드 서비스의 실제 사용량이 주문서의 라이센스 증서 부분에 명시된 권한을 초과하면 주문서에 명시된 대로 초과분에 대한 요금이 청구됩니다.

5. 기간 및 갱신 옵션

5.1 기간

클라우드 서비스의 기간은 주문서에 명시된 바와 같이, 클라우드 서비스에 대한 액세스 권한을 가진다고 IBM 이 귀하에게 통지한 날부터 시작됩니다. 해당 기간의 정확한 시작 날짜와 종료 날짜는 주문서의 라이센스 증서 부분에 명시됩니다. 귀하는 IBM 또는 IBM 비즈니스 파트너와의 계약을 통해 해당 기간 동안 클라우드 서비스의 사용 레벨을 상향 조정할 수 있습니다. IBM 은 상향 조정된 사용 레벨을 주문서에 명시합니다.

5.2 클라우드 서비스 기간 갱신 옵션

다음 중 하나를 선택하여 클라우드 서비스의 기간 종료 시 갱신 여부를 주문서에 명시합니다.

5.2.1 자동 갱신

주문서에서 자동 갱신으로 명시한 경우 귀하는 주문서에 지정된 기간 만료일보다 최소 90 일 이전에 서면 요청서를 통해 클라우드 서비스를 해지할 수 있습니다. IBM 또는 IBM 비즈니스 파트너가 만료일까지 그러한 해지 통지를 수신하지 못하면 만료 기간은 1 년 또는 라이센스 증서에 명시된 최초 기간과 동일한 기간만큼 자동으로 갱신됩니다.

5.2.2 연속적 청구

주문서에서 연속적 청구로 명시한 경우 귀하는 기간이 종료된 후에도 계속해서 클라우드 서비스에 대한 액세스 권한을 가지며 연속적 기준에 따라 클라우드 서비스의 사용 대금이 청구됩니다. 클라우드 서비스의 사용을 중단하고 연속적 청구 절차를 중지하려면 클라우드 서비스의 취소를 요청하는 90 일의 서면 통지를 IBM 이나 IBM 비즈니스 파트너에게 제공해야 합니다. 귀하의 액세스가 취소되면 취소가 발효된 해당 월의 미지불된 액세스 대금이 귀하에게 청구됩니다.

5.2.3 갱신

주문서에서 갱신 유형을 "종료"로 지정한 경우에는 기간이 만료되면 클라우드 서비스가 종료되며 클라우드 서비스에 대한 액세스 권한은 소멸됩니다. 종료 날짜 이후에도 클라우드 서비스를 계속 사용하려면 IBM 영업 담당자나 IBM 비즈니스 파트너에게 새로운 등록 기간을 구매하는 주문서를 접수해야 합니다.

6. 기술 지원

클라우드 서비스 기간 동안 http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf 또는 IBM 에서 제공하는 후속 URL 에서 명시된 바와 같이 클라우드 서비스에 대해 기술 지원이 제공됩니다. 기술 지원은 클라우드 서비스에 포함되며 별도의 오퍼링으로 제공되지 않습니다.

7. Safe Harbor 준수

본 클라우드 서비스에 대한 US-EU and US-Swiss Safe Harbor Frameworks 준수 여부에 대해서는 결정된 바 없습니다.

8. 추가 정보

8.1 데이터 수집

귀하는 IBM 이 클라우드 서비스의 정상적인 운영과 지원 과정에서 추적 및 기타 기술을 사용하여 클라우드 서비스 사용과 관련된 개인 정보를 귀하(귀하의 직원과 계약직 직원)로부터 수집할 수 있다는 것을 인정하고 이에 동의합니다. IBM 은 사용자 경험을 개선하거나 상호작용을 조정할 목적으로 클라우드 서비스의 효율성에 대한 통계와 정보를 수집합니다. 귀하는 IBM, 기타 IBM 회사 및 하도급자 내부에서, 그리고 IBM 및 IBM 하도급자가 비즈니스를 수행하는 어디서나, 관련 법률을 준수하면서, 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 직원과 계약직 직원의 요청을 수용합니다.

8.2 파생 혜택 사업장

해당하는 경우, 세금은 귀하가 클라우드 서비스의 혜택이 제공되는 것으로 식별한 사업장을 기준으로 부과됩니다. 추가 정보를 제공하지 않는 한, IBM 은 클라우드 서비스 주문 시 1 차 혜택 사업장으로 제출한 비즈니스 주소에 따라 세금을 적용합니다. 귀하는 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM 에 제공해야 할 책임이 있습니다.

8.3 비프로덕션 제한사항

클라우드 서비스가 "비프로덕션(Non-Production)"으로 지정된 경우, 귀하는 테스트, 성능 조정, 결함 진단, 내부 벤치마킹, 스테이징, 품질 보증 활동 및/또는 공개된 API(Application Progamming Interfaces)를 사용하여 내부적으로 사용되는 추가 기능 또는 확장 기능의 개발을 포함하여(단, 이에 한하지 않음) 내부 비프로덕션 활동 용도에 한해서만 해당 클라우드 서비스를 사용할 수 있습니다. 귀하는 해당 프로덕션 권한을 취득하지 않은 경우에는 기타 다른 용도를 위해 클라우드 서비스의 어떠한 부분도 사용할 수 없습니다.

8.4 준수에 대한 무보증

귀하는 법률, 규정 또는 관례에 기초한 준수 의무를 이행할 수 있도록 클라우드 서비스를 사용할 수 있습니다. 클라우드 서비스에서 제공한 지침이나 사용 권장사항은 법적 자문이나 회계 또는 기타 전문적인 의견은 아니며 필요한 법적 자문이나 전문가의 의견은 귀하가 직접 얻어야 합니다. 귀하와 귀하의 활동이 관련 법률, 규정, 표준 및 관례를 준수하는지 확인해야 할 책임은 귀하에게 있습니다. 클라우드 서비스를 사용한다고 해서 법률, 규정 또는 관례에 대한 준수가 보장되지는 않습니다.

또한 귀하는 클라우드 서비스는 귀하를 지원하기 위한 도구이며 제 3 자에게 자문을 제공하고 투자, 기타 비즈니스 및 위험 관리 의사결정을 수행하는 데 있어서 귀하의 관리팀과 직원의 기술, 판단력, 경험을 대신할 수 없다는 것을 인정합니다. 클라우드 서비스를 사용하여 발생한 결과에 대해서는 귀하가 책임을 집니다.

8.5 제 3 자의 웹 사이트 또는 기타 서비스에 링크

귀하나 클라우드 서비스 사용자가 클라우드 서비스에서 링크되거나 액세스 가능한 제 3 자 웹 사이트 또는 기타 서비스 간에 컨텐츠를 전송하는 경우 귀하와 클라우드 서비스 사용자는 컨텐츠 전송에 필요한 동의를 IBM 에 제공하며 단, 이러한 상호 작동은 귀하와 제 3 자 웹 사이트나 서비스 간에만 수행됩니다. IBM 은 해당 제 3 자 사이트, 서비스 또는 데이터에 대한 보증이나 진술을 제공하지 않으며, 해당 제 3 자 사이트, 서비스 또는 데이터 품질에 대해 책임을 지지 않습니다.

8.6 제 3 자의 혜택을 위한 사용에서의 제한 조치

IBM 이 서면으로 달리 동의하지 않는 한, 귀하는 서비스 사무소, 호스팅 서비스 또는 모든 종류의 상업적 정보 기술 서비스를 제 3 자에게 제공하기 위해 클라우드 서비스에서 생성한 출력 데이터 및 보고서를 포함하여(단, 이에 한하지 않음) 클라우드 서비스 또는 그 구성요소를 사용할 수 없습니다.

8.7 개인 건강 정보

클라우드 서비스는 HIPAA 를 준수하도록 설계되지 않으며 개인 건강 정보를 전송하거나 저장할 목적으로는 사용될 수 없습니다.