# IBM Watson Health Core

本使用條款 ("ToU") 由本 IBM 使用條款 - SaaS 特定供應項目條款（「SaaS 特定供應項目條款」）及標題為 IBM 使用條款 - 一般條款（「一般條款」）的文件構成，該文件可於下列 URL 取得：http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/。

如互有牴觸者，前項「SaaS 特定供應項目條款」較「一般條款」優先適用。一經訂購、存取或使用 IBM SaaS，即表示「客戶」同意本使用條款。

「使用條款」受所適用之「IBM International Passport Advantage 合約」、「IBM International Passport Advantage Express 合約」或 IBM International Agreement for Selected IBM SaaS Offerings（視適用情況而定）（以下稱為「合約」）之規範，「合約」與「使用條款」共同構成本完整合約。

## 1. IBM SaaS

下列 IBM SaaS 供應項目受前項 SaaS 特定供應項目條款之規範：

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

## 2. 計費度量

IBM SaaS 係依「交易文件」所定下列其中一項計費度量而銷售：

a. **「存取」**- 是獲得 IBM SaaS 的一種計量單位。一份「存取權」係指使用 IBM SaaS 的權限。「客戶」應在其「權利證明書 (PoE)」或「交易文件」中所指定的計量期間，取得單一「存取權」的授權，才能使用 IBM SaaS。

b. **「個體」**- 是獲得 IBM SaaS 的一種計量單位。「個體」係指單一個別之物或人。「客戶」應在其「權利證明書」或「交易文件」中所指定的計量期間，取得足夠涵蓋本 IBM SaaS 所處理或管理之「個體」的授權數。

基於本 IBM SaaS 之目的，「個體」包括由本 IBM SaaS 管理其資料之人員、裝置或行動式應用程式。

c. **「實例」**- 是獲得 IBM SaaS 的一種計量單位。一「實例」是對一 IBM SaaS 特定配置的存取權。「客戶」應在其「權利證明書」或「交易文件」中所指定的計量期間，取得足夠讓 IBM SaaS 的每一個實例可供存取及使用的授權數。

## 3. 計費及付款

IBM SaaS 的付款金額明訂於「交易文件」中。

### 3.1 未足月費用

「交易文件」所定未足月費用得按比例計算之。

### 3.2 超額使用計費

若「客戶」在計量期間內的 IBM SaaS 實際使用情形超出「權利證明書」載明之授權數量，則針對超額使用部分將依「交易文件」之規定開立發票給「客戶」。

## 4. 期間及續約選項

IBM SaaS 之期間，自 IBM 通知「客戶」其可存取 IBM SaaS 之試驗作業環境當日起算，詳如「訂購文件」之規定。「個體」授權之訂用期間，自 IBM 通知「客戶」可存取「正式作業」作業環境時起算。「訂購文件」應載明 IBM SaaS 是要自動續約、持續使用方式，或於期間結束時終止。

如係自動續約，除非「客戶」於前項期間到期日九十日（或更早）前為不續約之書面通知，否則，IBM SaaS 將依「權利證明書」所載明之期間自動續約。

如係持續使用，將依按月之方式持續提供 IBM SaaS，至「客戶」提供九十日前終止之書面通知為止。IBM SaaS 將繼續提供至前述九十日期間到期之日當月月底。

## 5. 技術支援

IBM 將提供 IBM Software as a Service Support Handbook（IBM 軟體即服務支援手冊），內含技術支援聯絡資訊維、護時間及其他資訊及程序。技術支援聯絡資訊及其他支援作業相關詳細資料，請參閱下列網址：IBM SaaS Support Handbook：https://support.ibmcloud.com。

本 IBM SaaS 之技術支援及簡式配置申請，係透過電子提交為之。技術支援僅隨附於 IBM SaaS 而提供，無法作為單獨供應項目而提供。

**通報問題意外事件時，說明文件或資訊中不得包含個人資訊 (PI)，包括「受保護健康資訊」(PHI) 及機密個人資料 (SPI)。**

## 6. 定義

**「適用法律」**- 係指由政府機關所頒布適用於本「服務說明」之履行之法律、法令或法條、規則、規章、指示、命令、政令或其他規定，或公認適用於本「服務說明」之業界標準。

**API** - 一組用於建置軟體應用程式之常式、通訊協定及工具。API 會規定各軟體元件應如何互動，且係於進行圖形使用者介面 (GUI) 元件程式設計時使用。

**「授權管理者」**- 係指負責維護平台並使其可靠運作之「客戶」員工、業經核准之「客戶」承包商、個人或團體。其責任包括配置、支援及使用者與帳戶管理。前揭管理者亦可能為臨床調查員，負責在 Watson Health 系統中設定研究案例。

**「授權個體」**- 係指業經鑑別，且已被授與存取權，有權將資料傳送至 Watson Health Core 之人員、行動式應用程式或裝置。「授權個體」可能包括「客戶」或研究參與者、客戶或「客戶」之病患。

**「客戶適用資料法」**- 係指「雙方當事人」所訂立之本合約、「相關文件」及適用之「服務說明」、「訂購文件」及「工作說明書」項下所訂「客戶」義務履行規定所適用之「資料法」。

**「客戶資料」**- 係指由「客戶」輸入或為其輸入本 IBM SaaS 中之資料，不問「客戶」自己資料或由其客戶或第三人輸入或代其輸入之資料，均同，且包括由第三人保健裝置提供之資料。

**「資料法」**- 係指有關資料保護、隱私權或安全之「適用法律」。

**「資料當事人」**- 係指其相關「個人資料」已被識別或可識別之人。

**「指定資料中心」**- 係指「交易文件」中針對主要資料中心及災難回復資料中心指定之資料中心，在適用情形下，該（該等）資料中心係用於執行「客戶」之 IBM SaaS 實例。

**「健康資料」**- 係指任何與「個人資訊」相關之資料或資訊，包括影像。

**「啟用健康資料」**- 就本 IBM SaaS 而言，係指其符合「健康資料範圍內管轄區」適用安全與隱私權之標準、法律及規章之程度，包括施行細則 HIPAA（HITECH 法案增修條款）分篇 A 與 C 第 164 編，以及其他「健康資料」有關「適用法律」，但並非意指 IBM 係以「事業夥伴」或「資料控制者」之身分執行相關事項。

**HIPAA** - 係指 1996 年醫療保險轉移與責任法 (Health Insurance Portability and Accountability Act of 1996) 增修條款，包括 2009 年美國復甦與再投資法案 (American Recovery and Reinvestment Act of 2009) 之經濟與臨床健康資訊科技法 (Health Information Technology for Economic & Clinical Health Act)（「HITECH 法案」）、美國衛生與公眾服務部 (United States Department of Health and Human Services) 於 45 C.F.R. 第 160 編及第 164 編 HIPAA 項下頒布之若干規章，以及依 HITECH 法案頒布之特定規章。

**「IBM 適用個資法律」**- 係指 IBM 對以下各項項下 IBM 義務之履行所適用之「個資法律」：本合約、「相關文件」，以及雙方當事人所訂立之適用「服務說明」、「訂購文件」及「工作說明書」。

**「IBM 人員」**- 係指 (a) IBM、IBM 之關係企業、轉包商，以及其等之僱員；及 (b) 依本合約及適用「相關文件」之規定，代表 IBM 執行服務或以其他方式獲得 IBM 授與「客戶個人資料」存取權限之第三人供應商。

**「範圍內國家」**- 係指 28 個歐盟會員國、瑞士，以及 IBM 可能隨時新增至名單內之其他國家。

**「個人資料」**或**「個人資訊」** - 係指任何媒體中或採用任何格式之資訊，包括有關已識別或可識別個人之電子及紙本記錄，所稱「可識別個人」，指可予直接或間接識別之人，尤其是指涉該人之識別碼或一或多項身體、生理、心理、經濟、文化或社會身分專屬因子者。

**「處理程序」**及其變體（例如：**處理**，不問有無特別標明）– 係指以自動化或非自動化方式，對資料所執行之一項作業或一組作業，例如：蒐集、記錄、編排、儲存、改寫或變更、擷取、商議、使用、揭露（藉由傳輸、散布或以其他方式供人使用）、調準或組合、封鎖、消除或毀損等作業。

**「已處理資料」**- 係指由 IBM 依本合約、「相關文件」及/或「服務說明」、「訂購文件」及/或「工作說明書」之規定所處理之資料、機密資訊或專有資訊或著作物，包括「健康資料」及「個人資料」。

**「安全意外事件」**- 其意義定於 SBCA 中。

## 7. 帳戶管理

本 IBM SaaS 僅限由「客戶」之授權使用者（「**授權管理者**」或「**授權個體**」）存取。「客戶」應控管被授權存取本 IBM SaaS 之帳戶，其可能包括授權應用程式、「客戶」之人員、「客戶」之第三人服務提供者與承包商，且對下列事項負完全責任：(i) 控管一切授權使用者，包括但不限於驗證授權使用者身分；及 (ii) 確認僅有授權使用者存取本 IBM SaaS。

「客戶」之客戶、病患或研究參與者等「授權個體」，僅限基於上傳資料至本 IBM SaaS 之目的而被授與存取權限，「授權個體」不得基於其他目的而存取本 IBM SaaS。

## 8. 隱私權

### 8.1 一般規定

依雙方當事人之約定，「客戶」為一切「客戶個人資料」之唯一控制者 (controller)，且「客戶」係指派 IBM 擔任資料處理者 (processor)。依「適用個資法律」之規定，「客戶」有權指示 IBM 如何處理「客戶個人資料」。

就 IBM 對「客戶個人資料」之處理，IBM 應遵守下列規定：

a. 遵循一切「IBM 適用個資法律」；及

b. 不得將「客戶個人資料」與其他來源所提供之資料合併；但有下列情形者不在此限：

- 為提供本 IBM SaaS 而有必要合併者，惟不得用於其他目的，如係由「客戶」明確指示者不在此限；或
- 依本「使用條款」及「SBCA 附錄」之規定者。

就 IBM 對「客戶個人資料」之處理，「客戶」遵守下列規定：

a. 遵循一切「客戶適用個資法律」；及

b. 負責與「客戶」之「關係企業」、病患、使用者、「資料當事人」及/或其他「客戶」之第三人進行各項協商；

c. 與資料控制者訂立資料處理合約，據以許可 IBM 以資料處理者與再處理者 (sub-processor) 之身分處理「客戶個人資料」；及

d. 擔任 IBM 單一聯絡人，並自行負責對作為 IBM 其他控制者之「客戶關係企業」所為之指示或要求，進行內部協調、審查及提交。IBM 於其提供此等資訊予「客戶」或通知「客戶」後，對於作為控制者之「客戶關係企業」，不負告知或通知之義務。IBM 有權拒絕由作為控制者（而非「客戶」本身）之「客戶關係企業」直接提供之指示。

不得要求任一方當事人違反該方之「適用個資法律」。

### 8.2 「客戶」之資料權限

「客戶」聲明並保證 (a) 「客戶」擬於本 IBM SaaS 中輸入之資料，為其所有；或(b) 為授與 IBM 依本「使用條款」或本合約之規定，或依其提供本 IBM SaaS 時所需遵循之規定，存取、使用及揭露「客戶資料」之權利，「客戶」已取得一切必要之權利、權限、同意及授權，並應負責持續維持其等之有效性。「客戶」進一步聲明並保證「客戶資料」符合下列條件：(a) 僅與居住於美國之個人有關，且僅輸入至位於美國資料中心之本 IBM SaaS 中；或 (b) 僅與居住於一或多個「範圍內國家」之個人有關，且僅輸入至位於「指定資料中心」之本 IBM SaaS 中。

## 8.3 資料之服務與責任

a. 「客戶」同意，「客戶」僅就包含「客戶」之「健康照護作業」或「研究」之活動，執行「客戶資料」分析，或要求 IBM 執行之（「健康照護作業」或「研究」之意義，依 HIPAA 及/或其他「適用個資法律」項下類似條款所定者），且同意於其使用「客戶資料」或指示 IBM 使用「客戶資料」時，僅依照此等法律及其他「客戶適用個資法律」一切相關規定（例如：人體試驗委員會 (Institutional Review Board) 於必要時所為之判斷或拋棄）為之。

b. 「客戶」應自行負責於各適用「範圍內國家」中取得「客戶適用法律」所規定之一切註冊、同意、授權及權限，包括但不限於 HIPAA 及其他適用之資料隱私權及安全法律、規則及規章，以使「客戶」及 IBM 與 IBM 許可轉包商得依本「使用條款」及本合約之規定，於本 IBM SaaS 中輸入「客戶資料」，以及使用及揭露之。IBM 對於何時收受或需要前揭註冊、同意、授權及權限，不負監控之責。

c. 「客戶」應自行負責確認，一切輸入於本 IBM SaaS 中之「客戶資料」，悉以居住於美國或適用「範圍內國家」之人有關資料為限。

d. IBM 應設立支援中心，並於該等中心編制完訓人員（受過 HIPAA 及其他有關「範圍內國家」提供資料之「IBM 適用個資法律」相關訓練之人員）。

## 8.4 安全措施及安全意外事件

a. IBM 應施行、保持及遵循技術及組織措施，包括組織程序及本「使用條款」及 SBCA 所規定或載明之特定安全義務，藉以防止「客戶個人資料」發生未獲授權之使用或存取、不慎滅失、損毀、修改、破壞、竊取或未獲授權之揭露等情事。

b. IBM 於其發覺有關「客戶已處理資料」之「安全意外事件」（如 SBCA 所定義者）時，應依 SBCA 及「IBM 適用個資法律」條款之規定通知「客戶」，且該通知書中應包含已知之有關對「客戶」或受該「安全意外事件」影響之「資料當事人」所生影響，以及應由或擬由 IBM 採取之更正動作。

## 8.5 查詢與申訴之受理

IBM 於 IBM Watson Health Data Privacy Officer 受理由 IBM 所收受有關下列之人或機關所提供「客戶個人資料」之查詢、溝通或申訴後，應即以書面通知「客戶」，且於「IBM 適用個資法律」許可範圍內，該項通知，最遲應於收受後五個營業日內為之：

a. 「資料當事人」- 有關由 IBM 處理之該等「資料當事人」之「個人資料」。「客戶」應回應「資料當事人」所提出之前揭要求，且 IBM 應遵循「客戶」之合理指示，協助「客戶」回應該等要求。如「IBM 適用法律」有其規定者，IBM 得直接回應前揭要求，惟 IBM 應於回應前事先告知「客戶」，如「IBM 適用法律」或其他法律許可者，應以合理之方式協助「客戶」處理該項回應之表單及內容相關事宜。

b. 立法機關或法規主管機關 - 有關 IBM 對「客戶個人資料」所為之「處理」；但 IBM 得以傳票或據以強制 IBM 為資料揭露之類似法定書件或「適用個資法律」所規定之其他書件，回應所收受之政府機關所提出之前揭要求，惟 IBM 應於為該資料揭露前事先告知「客戶」，如法律或其他規定許可者，應以合理之方式協助「客戶」處理該項回應之表單及內容相關事宜。

## 8.6 「客戶個人資料」之處理

IBM 應規定僅限將「客戶個人資料」揭露予需要協助其提供「服務」之「IBM 人員」。

「客戶」對 IBM 提出合理要求，要求其依「適用法律」修訂、更正、刪除或封鎖「客戶個人資料」者，IBM 應遵循該合理要求。

於當事人之一方提出要求時，IBM、「客戶」或其「關係企業」應就「客戶個人資料」依法訂立標準合約。「當事人」同意（並應使其各別「關係企業」同意），前揭合約應受本合約中之賠償責任限制條款與排除條款之拘束，該等條款係基於「當事人」間所為求償之目的所訂者。「當事人」應依「適用個資法律」之規定，配合訂立（或使該方當事人之「關係企業」訂立）後續雙方合意之條款或合約。

## 8.7 「客戶」個人資料之歸還

於本合約到期或終止時，IBM 應停止使用或處理「客戶專有資訊」及「客戶個人資料」，並使一切「IBM 人員」停止使用或處理之，且應依「客戶」之選擇與要求，執行下列事項：

a. 採用「客戶」合理要求之格式及儲存媒體，將 IBM 以電子方式儲存之一切「客戶專有資訊」及「客戶個人資料」即時歸還「客戶」，且應於「客戶」確認收到後，即時將該等「客戶專有資訊」及「客戶個人資料」（包括複本與備份）刪除、銷毀或以其他方式使其永遠無法讀取或辨認。IBM 得就儲存媒體之成本及依「客戶」要求執行之特定活動（例如：以特定格式交付「客戶專有資訊」及「客戶個人資料」，或以特定方式銷毀「客戶專有資訊」及「客戶個人資料」）；及

b. 直接將前揭「客戶專有資訊」及「客戶個人資料」（包括複本與備份）刪除、銷毀或以其他方式使其永遠無法讀取或辨認。

### 8.8 事業夥伴合約

於 HIPAA 所規定之適當範圍內，IBM 及「客戶」應訂立「事業夥伴合約」("BAA")，據以規範本 IBM SaaS 之條款中 IBM 身為「客戶事業夥伴」所應承擔之義務。在不限制本合約及 BAA（視適用情形而定）項下 IBM 明定義務之前提下，「客戶」承認並同意，「客戶」應負責判斷一切「適用法律」及其對本 IBM SaaS 之使用或其相關事項所適用授權規定之適用性，並遵循之。

### 8.9 歐盟資料處理附錄

倘若「客戶」指示 IBM 處理「歐盟個人資料」，IBM 及「客戶」應訂立「資料處理附錄」，包括適用之「歐盟示範條款」（已刪除選用條款）。

## 9. IBM SaaS 供應項目附加條款

### 9.1 安全

本 IBM SaaS 遵循 IBM 之 IBM SaaS 資料安全與隱私權原則（該等原則提供於下列網站：http://www.ibm.com/cloud/data-security），以及以下及本「使用條款」之「安全與業務持續性附錄」所訂附加條款。IBM 資料安全與隱私權原則之變更不會降低本 IBM SaaS 之安全。

IBM Watson Health Core 係依照 ISO 27001 架構（如「安全說明」所詳述者）實作安全原則、標準及處理程序。本解決方案實作下列安全功能：

a. 安全作業區

IBM Watson Health Core 實作深度策略防禦，運用多重安全區域管理雲端整合點，例如：資料裝載及客製應用程式開發。

b. 加密

一切「客戶資料」，不管處於靜止狀態或使用中，一律予以加密。利用 IBM Watson Health Core 進行傳輸之一切資料，一律予以加密。共用服務提供加密金鑰管理。IBM Watson Health Service 與「客戶」Proxy 伺服器間之一切網路連線功能與品質，悉由「客戶」負責。

c. 安全事件監視作業

IBM 運用其安全情報平台，進行安全資訊與事件管理、日誌管理、意外事件剖析、威脅偵測及漏洞管理。

d. 身分管理

- Watson Health Core 支援採用 OpenID Connect 之大量病患與使用者族群之開放式標準身分提供者。
- 針對 IBM 係為其身分提供者之使用者族群，Watson Health Core 會運用適用之目錄服務與身分管理功能處理鑑別作業。

e. 強型態鑑別與角色型存取

- Watson Health Core 支援透過 SAML（作為鑑別機制）所進行之鑑別，以供「客戶」整合其單一登入 (SSO) 或目錄服務。
- Watson Health Core 可在必要時運用存取管理解決方案及相關元件管理安全原則。
- Watson Health Core 支援軟體型雙重鑑別。
- Watson Health Core 依需求提供基本角色型存取控制；Watson Health Core 支援透過啟用角色型存取之應用程式設計介面（"API") 進行研究、使用者基本資料設定檔、角色及使用者群組之配置。

## 9.2 Cookie

「客戶」知悉並同意，IBM 得就 IBM SaaS 之使用，藉由追蹤及其他技術，蒐集「客戶」（「客戶」之員工及約聘人員）所提供之個人資料，以作為 IBM SaaS 一般作業及支援之一部分。IBM 蒐集前述資料之目的，在於蒐集有關 IBM SaaS 效率之使用統計資料與資訊，以改善使用者之使用體驗及/或調整與「客戶」之互動方式。「客戶」確認其將取得或已取得同意，以允許 IBM 及其承包商執行業務時，得依適用法律，基於前項目的，於 IBM、其他 IBM 關聯公司及其承包商內處理前項所蒐集之個人資料。IBM 將依「客戶」之員工及約聘人員之要求，存取、更新、更正或刪除其所蒐集之個人資料。

## 9.3 衍生受益之地點

在適用情形下，稅金之核算係以「客戶」於其收受 IBM SaaS 之權益時所指明地點為依據。除非「客戶」提供其他資訊予 IBM，否則 IBM 於核算稅金時，將以下列公司地址為依據，該地址係「客戶」訂購 IBM SaaS 時指明為主要受益地點。「客戶」應負責保持最新之前述資訊，並將其變更提供予 IBM。

## 9.4 持續交付

「客戶」有權使用為解決方案提供且由 IBM 於持續雲端交付模型中部署之各項功能及加強功能。

## 9.5 備份及還原

IBM Watson Health Core 在正式作業環境中提供最後一次已知良好狀態之「客戶資料」之備份（包括 Data Lake 及 Data Reservoir 等儲藏庫），以備於系統失效時用以回復服務。

## 9.6 高可用性

正式作業環境中之 IBM Watson Health Core 元件，係以高可用性配置實作，該等配置包含備用之叢集化資料庫伺服器，用以分配工作量及消除單點故障。

## 9.7 災難回復

IBM 之災難回復方式，包括在不同地理區域設立多個資料中心，以達成正式作業環境中之下列 IBM 業務持續目標：

- RTO - 災難宣告後 36 小時內
- RPO -「客戶」內容滅失後 24 小時內

## 9.8 測量工具

本 IBM SaaS 利用綜合監視解決方案，依照已承諾服務水準，進行服務之可用性或中斷狀態之監視、測量及提報。本解決方案會模擬並追蹤全面性使用者回應與使用者體驗 - 二者均針對靜態可用性與交易。

本 IBM SaaS 亦將內部監視系統運用於整個解決方案之測量、事件及警示。

## 9.9 公開

「客戶」同意 IBM 得於宣傳或行銷傳播時公開指稱「客戶」為本 IBM SaaS 之訂用者。

# 附錄 A

## 1. IBM Watson Health Core

IBM Watson Health Core 係為一種「啟用健康資料」平台即服務 (PaaS)、開發平台及作業子系統，用以儲存、策劃及處理「受保護健康資訊」(PHI)（如 HIPAA 所定義者），以及其他符合「IBM 適用個資法律」規定之「健康資料」（存放於 IBM 所擁有或所控管之資料中心）。「客戶」需取得適當之 IBM Watson Health Core 及 IBM Watson Health Core Access 授權，始得啟用以下所示特性與功能。

### 1.1 Watson Health Core 作業環境

Watson Health Core 授權包含三種「啟用健康資料」雲端作業環境，可供「客戶」用以處理「健康資料」：

- 試驗環境

  提供沙盤推演環境，可讓「客戶」開發及測試使用本 IBM SaaS 建置之應用程式。試驗環境會實作記錄系統之一切 HIPAA 安全控制項目（「災難回復」除外）、高可用性及備份。

- 正式作業環境

  提供完整規模之環境，「客戶」可在其中部署「健康資料」工作量。正式作業環境係為高可用性之負載平衡環境，並可針對「災難回復」位置進行失效接手。

- 災難回復

  提供正式作業環境之鏡映抄本，並將其存放於不同資料中心位置。

### 1.2 應用程式開發

IBM Watson Health Core 可供「客戶」從其裝置或其授權使用者之裝置，進行應用程式開發及安全資料蒐集。API 提供程式介面及說明文件，可供「客戶」之授權使用者（包括「客戶」之第三人服務提供者）用以開發應用程式並與本 IBM SaaS 交換資料。「客戶」或其開發人員對 API 之使用，應遵循「API 開發人員規定」。

- REST API

  Watson Health Core 提供 Watson Health Core 平台適用之一系列 REST API 及服務。API 功能包括但不限於資料儲藏庫存取機制、資料策劃服務、使用者管理及審核日誌。

- Apple HealthKit 及 Apple ResearchKit

  Watson Health Core 支援與 iOS 型研究適用之 Apple ResearchKit API 架構整合，並與 Apple HealthKit 整合，以擷取健康資料。

### 1.3 資料控管

- 同意管理

  Watson Health Core 提供用以擷取病患或研究參與者所為同意之架構，並以安全方式儲存同意記錄，此儲存作業係與個人透過同意啟用之「客戶」應用程式登記時所產生之資料有效負載分開進行。

- 資料遮罩

  Watson Health Core 可供使用者將名稱 ID 與結構化資料有效負載分開。Watson Health Core 係透過程式 API 接收雲端中之資料。前揭 API 可將病患或個人之名稱 ID 與其他資料有效負載分開，以儲存於不同之已加密資料儲存庫。資料有效負載會獲配一個匿名化記號，以利進行後續之出處追蹤。

### 1.4 健康資料服務

Watson Health Core 提供結構化與非結構化資料之蒐集、儲存、同步化，包括外生之「健康資料」及其他「個人資訊」。

- 資料汲取

  Watson Health Core 可供使用者透過程式 API，從病患應用程式或裝置汲取資料。Watson Health Core 於契約有效期間，每年最多可讓「客戶」之「授權個體」上傳 25 MB 資料至 Health Core。本服務每日最多可供每一個體進行 10 次上傳。

- 作業 Data Lake

  原始之「客戶」資料或病患資料係以其原生格式儲存於 Watson Health Core，至需要用於分析及建模為止。

- 擷取轉換載入 (ETL)

  資料係於作業子系統中轉換成正規化格式。保建機構適用之業界標準型企業服務匯流排，可透過不同之「客戶」應用程式及通訊協定進行整合。

- Data Reservoir

  資料於其完成策劃後，會移至 Data Reservoir。Watson Health Core 會利用 IBM Unified Data Model for Healthcare 之各項功能，將業務資料及技術健康資料正規化，以供分析之用。

- 主要人員索引

  Watson Health 提供 Master Data Management 工具，用以合併來自多重來源之資料，以建立「縱向人員記錄」(LPR)。

## 2. 選用特性

### 2.1 IBM Watson Health Core Terminology Service

此附加程式服務有助於進行不同健康系統間之資料整合及交互作業能力，進而透過一切 Watson Health Cloud 應用程式提供一致之臨床術語用法。本服務提供有關術語、程式碼系統及結構化內容之一切作業所適用之功能平台，例如：

- 建立新程式碼系統；
- 轉譯國際程式碼系統；及
- 進行區域碼清單與國際標準間之對映。

# 附錄 B

IBM 依「權利證明書」之規定提供本 IBM SaaS 之下列可用性服務水準協定 ("SLA")：本 SLA 並非保證。本 SLA 僅限提供予「客戶」，且僅適用於正式作業環境中之使用。

## 1. 可用度扣抵

可用度退款僅適用於「個體」授權之訂用費用。

「客戶」應在得知事件影響本 IBM SaaS 可用性之 24 小時內，先向 IBM 技術支援中心服務台記載「嚴重性層次 1」支援問題單。「客戶」應於合理範圍內協助 IBM 進行問題之診斷與解決。

就未能符合 SLA 而提出之支援問題單請求，應於合約月份結束後三個營業日內提出。對於有效 SLA 請求之補償，將以本 IBM SaaS 未來發票折抵方式提供之，該項折抵之計算期間為無法提供本 IBM SaaS 正式作業系統處理之期間（「停用時間」）。「停用時間」之計算，自「客戶」提報事件時起，至本 IBM SaaS 回復時止，但不包括因下列事由所致時間：基於維修目的而排定或公布之停止；非 IBM 所能掌控之原因；因「客戶」或第三人內容或技術、設計或指示所生問題；不受支援之系統配置及平台或其他「客戶」錯誤；或「客戶」所致資安事件或「客戶」安全測試。IBM 將依各合約月份期間之 IBM SaaS 累計可用度，套用最高可適用之補償，如下表所示。 任何合約月份相關之補償總額，以本 IBM SaaS 年費十二分之一 (1/12) 的百分之二十金額為上限。

## 2. 服務水準

合約月份期間的 IBM SaaS 可用度

| **「合約月份」期間的可用度** | **補償<br>（「請求」事由發生之「合約月份」的每月「個體」訂用費用*之百分比）** |
|---|---|
| < 99.95% | 10% |
| < 99.0% | 20% |

*如 IBM SaaS 係向「IBM 事業夥伴」取得者，每月訂用費用應以「請求」所主張之「合約月份」之有效 IBM SaaS 當時最新標價計算，且其折扣率為 50%。IBM 將直接折讓給「客戶」。

可用度（以百分比表示）之計算為：合約月份中的總分鐘數減去合約月份中「停用時間」的總分鐘數，除以合約月份的總分鐘數。

範例：「合約月份」期間的「停用時間」總共 108 分鐘

$$\frac{\text{30 天「合約月份」，總共 43,200 分鐘 - 停用時間 108 分鐘 = 43,092 分鐘}}{\text{總共 43,200 分鐘}} = \text{合約月份期間可用度達 99.75\% 時為 10\% 可用度扣抵}$$

## 3. 除外條款

本 SLA 不適用於下列情況：

- 除伺服器監視以外，本 SLA 不適用於用以支援客製應用程式或「客戶」應用程式之受管理虛擬機器。
- 「客戶」違反現行合約義務項下重大義務。

# 附錄 C

本「安全與業務持續性附錄」("SBCA") 就 IBM 提供本 IBM SaaS 予其「客戶」之相關事項，訂定 IBM 應遵循之若干規定與義務。本「附錄」所定前揭規定與義務，係為 IBM SaaS 資料安全原則說明（提供於 http://www.ibm.com/cloud/data-security）所定規定與義務之增修條款。未定義於本「附錄」中之專有名詞，係於本合約或本「使用條款」中另有定義。

## 1. 資訊安全方案

IBM 依據 ISO 27001 架構及控制區域訂有安全原則、標準及處理程序。除 IBM Corporate Security Organization 控管作業外，前揭原則、標準及處理程序亦為例行性內部審核之審核項目。

IBM 制定組織、作業、管理、實體及技術保護措施之資訊安全方案，據以規範「客戶」內容之處理、儲存及傳輸等相關事項，該等保護措施符合或超過本 SBCA 之規定。

IBM 於「客戶」提出要求時，應與「客戶」共用 IBM Watson Health 資訊安全方案相關資訊，使「客戶」得合理判斷其持續之適宜性、充分性及有效性。本 IBM Watson Health 資訊安全方案應隨時更新，以維持最新之公認界業常規及「IBM 適用法律」。

## 2. 存取控制

IBM 僅限將「客戶」內容揭露予符合下列條件之 IBM 僱員、IBM 轉包商或第三人：為協助 IBM 履行其對「客戶」之義務，或對有必要依「適用法律」、本合約或「相關文件」（視適用情況而定）之規定提供本 IBM SaaS 之「客戶」或其他人之義務，而有正當業務需求必須存取該「客戶」內容者。IBM 如係為「客戶」之「事業夥伴」者，IBM 及「客戶」僅限依「當事人」間所訂適用「事業夥伴合約」之條款，揭露「個人健康資訊」。

IBM 訂有正式內部使用者存取管理處理程序，依該管理處理程序之規定，使用者存取需於正式提出申請後始得為之、需經身分驗證之核准，並依知悉、使用最低權限概念之需求授與權限。「客戶」內容存取權限之被授權者，以作用中使用者及作用中使用者帳戶為限。IBM 訂有正式處理程序，據以對作用中使用者帳戶進行定期內部存取重新驗證。

IBM 採用安全使用者鑑別通訊協定，包括在用於依 IBM 企業安全標準與原則為「客戶」提供服務之系統上指定作用中使用者帳戶之唯一識別及高保護性密碼。

a. 密碼不得設為供應商提供之預設密碼，且密碼存放之位置及/或格式不得危及其所保護資料之安全性。

b. 顯示及列印密碼時，應予遮罩、抑制或以其他方式遮蔽，以防止未獲授權之人看到或於其後恢復而取得該密碼。輸入密碼時，不得記載或擷取密碼。使用者密碼不得以明碼儲存。

c. 本 IBM SaaS 所含各項技術，其密碼之選用，係以降低已知密碼長度漏洞相關風險為目的，應予妥善記載於文件中。

d. 因作業而需使用內部、特許、共用之部門 ID 者，IBM 規定必須檢查共用 ID、部門 ID 及/或系統 ID 之密碼，以利進行個別問責。

用以儲存「客戶」內容之一切系統與應用程式，均設有未使用逾時。

如有必要，應於「客戶」提出要求並經 IBM 正式核准後，設定對用以儲存「客戶」內容之 IBM 網路、系統及應用程式所為之遠端存取權限，該等遠端連線均應採用強型態鑑別及加密通訊協定，以維護其安全性。遠端存取活動應予記載及監視。

IBM 為交付本 IBM SaaS 而需遠端存取「客戶」內部網路中之系統者，進行該等遠端存取作業時，應一律使用「客戶」之安全遠端存取系統與通訊協定，以及「客戶」提供予 IBM 之存取認證。對「客戶」網路之遠端存取權限，於 IBM 提出要求，並經「客戶」核准後始得設定，且應依「客戶」當時最新原則為之，該等原則應事先告知 IBM。IBM 對「客戶」內部網路之使用，受「客戶」之 IT 使用與安全原則之拘束，該等原則應事先告知 IBM。

IBM 對於安全管理、存取審查及安全違規調查，實作權責區分原則。

「客戶」特定內容之儲存、管理及處理，係以符合邏輯之方式，與其他由 IBM 提供服務之客戶內容之儲存、管理及處理予以分開進行。「客戶」如有授與 IBM 使用共用儲存、管理或處理工作區域之權限者，IBM 應依本 SBCA 之規定訂定程序與保護措施，用以防止對前揭「客戶」內容所為未獲授權之揭露。

IBM 施行清除桌面/清除畫面政策，以確保公用位置中之「客戶」內容不論何時均無疏於照顧之虞。

## 3. 傳輸與加密

IBM 於傳輸「客戶」內容時，應採取適當預防措施（利用傳真、電子郵件、快遞公司等等方式進行傳輸），以確認所使用之收件人聯絡資訊正確無誤，並優先安排預定收件人，以確保該資訊收受之安全性。

IBM 於處理「客戶」內容時，一律採用適當加密格式或其他安全技術，並要求「IBM 人員」比照辦理，包括「客戶」內容之傳送、通訊、遠端存取或儲存（包括備份儲存）等相關事項。例如，IBM 對於內含「客戶」內容之一切記錄與檔案，會以適當業界標準加密方式予以加密：

a. IBM 筆記型電腦、可攜式裝置或可攜式電子媒體（包括於傳輸至離站儲存設施時所使用之備份磁帶）所儲存之記錄與檔案；

b. 由 IBM 於「客戶」或 IBM 之施行實體安全措施之辦公室及設施外部所儲存或傳輸之記錄與檔案，紙本書面文件除外；

c. 由 IBM 透過公用網路進行遠程作業時所傳輸之記錄與檔案；

d. 從 IBM 之系統移轉至「客戶」系統時所傳輸之記錄與檔案；

e. 於 IBM 進行無線傳輸時所傳輸之記錄與檔案；及

f. 由 IBM 儲存於伺服器與資料庫之記錄與檔案。

## 4. 網路安全

IBM 採用適當之最新版系統安全軟體，例如：防火牆、Proxy、Web 應用程式防火牆及介面。前揭軟體必須包含惡意軟體保護程式及適當之最新修補程式及病毒定義。依企業標準，防毒軟體應安裝於工作站、伺服器及技術上可行之相關端點，且該軟體應遵循內部管理解決方案之企業原則。

IBM 會監視本 IBM SaaS，以儘早偵測及識別安全意外事件。IBM 在最低限度內，至少會持續採用業界標準入侵偵測工具，以及預防、監控及回應等處理程序，所用方式足以識別可能致生下列結果之內外部漏洞與風險：對「客戶」內容或用於交付服務予「客戶」之資訊系統所為之未獲授權之揭露、不當使用、更改或破壞。

IBM 訂用漏洞情報服務或資訊安全諮詢服務及其他提供有關系統漏洞最新資訊之相關來源。IBM 會定期進行其網路之漏洞評量與修正。

IBM 會監視本 IBM SaaS，以偵測、識別、遏制及解決「安全意外事件」。

IBM 會利用 IBM 版本管理處理程序，驗證用以提供本 IBM SaaS 之網路安全基礎架構之可用性、完整性及有效性。

## 5. 意外事件管理與通知

IBM Watson Health 小組配合「IBM 網路安全意外事件回應小組」一起執行安全意外事件相關事項。該回應小組係為全球性小組，負責 IBM 供應項目相關安全意外事件之受理、調查及內部協調，並實作必要之預防步驟，以減少有關軟體之安全問題。「安全意外事件」係指成功致使 IBM 用於提供本 IBM SaaS 之資訊系統中之系統作業或資料遭受未獲權限之存取、使用、揭露、修改或干擾。如有發現「安全意外事件」（透過例行掃描、警示、臨界事件等等方式），IBM 應執行下列事項：

a. 盡快通知「客戶」有關「客戶」內容之已確認「安全意外事件」，惟最遲不得晚於該「安全意外事件」經查屬實後之二個營業日；

b. 通知「客戶」即時遵循政府主管機關（包括資料保護機關或執法機關）所公布有關「客戶」內容之存取要求或資訊，但法律或相關命令規定不得遵循者除外；及

c. 事先通知「客戶」第三人對「客戶」所為揭露、傳輸或存取，但本 SBCA 中標題為「存取控制」一節許可者不在此限。

## 6. 記載

IBM 依 IBM 原則與常規及公認業界常規，持續對系統進行適當監控，以查驗「客戶處理資料」有無遭受未獲授權之使用或存取。實際發生或嘗試進行之登入違規及存取違規，應予記載。

一切用以儲存、存取、處理及傳輸「客戶資料」與「健康資料」之系統，其一切存取要求及存取活動日誌，IBM 均予保留記錄，保留期限依 HIPAA 及其他「IBM 適用個資法律」之規定。

前項日誌與報告至少應載明以下各項：(i) 一切登入嘗試（不問成敗），包括適當之識別資訊；(ii) 一切系統與網路配置之變更，包括應用程式安裝、使用者管理變更及檔案存取權限修正；(iii) 資源存取嘗試（不問成敗），包括存取檔案、網路共用、日誌或其他資源等嘗試；及 (iv) 資料下載，包括資料之內容類型及進行下載時所使用之存取通訊協定。

## 7. 軟體應用程式之開發及變更管理

IBM 遵循安全應用程式開發及編碼常規，該等常規之目的，在於防止正式作業應用程式及相關原始碼之完整性遭受未獲授權及未經測試之修改。

IBM 遵循變更管理處理程序，此處理程序包括以下各項：(a) 變更之記錄及正式核准，以及取消之程序；及 (b) 對該等變更進行適當測試，包括適用之使用者驗收測試，以及安全測試。

IBM 遵循修補程式管理處理程序，此處理程序包括在一切用於儲存、存取及傳輸「客戶」內容，或交付服務（包括本 IBM SaaS）予「客戶」之系統上安裝修補程式之前，所進行之修補程式測試。

IBM 規定，系統管理者對於一切用於儲存、存取及傳輸「客戶」內容之資訊系統，應使其配置相關資訊維持完整、準確及最新之狀態。

## 8. 實體安全及環境安全

IBM Watson Health Core 平台係部署於 IBM SoftLayer 資料基礎架構。IBM SoftLayer 維護實體安全及環境安全、提供存取控制、控制項及處理程序，以防止「客戶」資料遭受人為、環境及技術破壞或影響。

用以管理本 IBM SaaS 之設施，其一般進出係利用卡式進出管制系統施行管制。各場所一律安裝閉路電視 (CCTV) 錄影機，並由保全人員負責監控。特定進出門戶裝有警報器，並由保全人員負責監控。

管制區之進出，採用卡式進出管制及/或其他生物特徵驗證等方式施行管制。不具管制區進出許可權限之人，進出時必須登記，並由具有管制區進出許可權限之人陪同。各管制區緊急出口均裝設發聲警報器，並由保全人員負責監控。定期檢查警報器功能是否正常，並記載及保留檢查結果。管制區進出權限每季施行全面重新驗證。管制區進出權限，於僱用關係終止時撤銷之。

各項設施均裝設火災警報器、滅火器、煙霧警報器及滅火系統，以防止設施因火、水及熱度等環境因子而受損。各項設施均裝設不斷電 (UPS) 系統及備用發電機，以防止設施因斷電或停電而受損，經定期維護及測試。

IBM SoftLayer 循規準則資訊與報告，請參閱下列網站：http://www.softlayer.com/compliance。

## 9. 業務運作持續性

IBM 訂有業務持續與災難回復計劃，其目的為依本合約項下 IBM 義務維持其服務水準。該等業務持續與災難回復計劃應定期更新與測試（每年至少實施一次）。IBM 為遵循公認業界常規，有必要對業務持續與災難回復計劃進行一切適當之變更，惟不得不當干擾「客戶」正在使用之 IBM SaaS 或正式作業環境。

因發生災難致使「客戶」無法使用本 IBM SaaS 者，IBM 應即通知「客戶」並啟動業務持續及/或災難回復計劃。宣告災難後，本 IBM SaaS 業務持續目標係為依下列方式，回復「客戶」對本 IBM SaaS 之存取：服務停止者，回復 IBM Watson Health 正式作業環境之回復時間目標 (RTO) 為宣告災難後 36 小時內。回復點目標 (RPO) 為正式作業環境內之「客戶」內容滅失後 24 小時內。各特定 Watson Health 解決方案之業務持續目標可能不盡相同。

IBM 之災難回復方式，包括在不同地理區域設立多個資料中心。

一切 IBM SoftLayer 資料中心均備有多組供電系統、光纖鏈結、專用發電機及備用電池。該等裝備係以業界頂尖硬體與設備製成，可提供最高層級之效能、可靠性及交互作業能力。為維持各資料中心之穩定性，其所含元件（例如：備用 n+1 電力與冷卻資源）業經檢驗合格。

## 10. 循規準則

IBM 安全常規係依 ISO 27001-27002 定之。該等常規提供控制結構，包括但不限於下列項目之控制結構：「風險分析」、「實體安全」、「緊急計劃」、「調查」、「資訊保護」、「教育」、「資料保護」及「作業」。

IBM 會檢閱安全及隱私相關活動，以確認是否符合 IBM 安全常規。

IBM 遵循「範圍內管轄區」內之「IBM 適用個資法律」。

此外，「IBM 商業行為準則」亦規定必須適當處理「客戶」之機密資訊，所有的員工每年均需審查該等準則，並提供其完成審查之證明。

## 11. 細項

IBM 應確認，IBM 與一切轉包商及/或參與本 IBM SaaS 交付作業之第三人所立合約，其條款對「客戶」內容之保護效力應至少同於本 SBCA 及適用「相關文件」中所訂條款，且該等合約之條款適用於由該等轉包商及/或第三人執行之服務。