和黃醫藥
HUTCHMED

和黃醫藥（中國）有限公司

個人信息管理政策

董事會於 2017 年 3 月 14 日採納
並由董事會於 2023 年 1 月 1 日修訂

目錄

1. 政策聲明

和黃醫藥（中國）有限公司（「本公司」）、其附屬公司及受控制聯屬公司（統稱「集團」）確認保護個人信息是維持公眾信任的關鍵。集團致力保障及保護從(i)僱員、代理人、顧問、承包商、供應商、服務提供商，(ii)使用集團產品的患者或臨床研究對象和其他客戶，(iii)研究或開出集團產品處方的醫療保健專業人士，及(iv)與集團投資或業務發展活動相關的人士所獲取的個人信息，包括在集團經營所在司法管轄區，遵守適用資料保護法律的集團盡職審查程序。

本政策載列集團保障僱員、客戶及上述其他個人信息當事人的個人信息的管理架構。本政策應與和黃醫藥信息安全政策及和黃醫藥道德規範以及集團或其成員公司的當地政策及程序一併閱讀。

本政策適用於集團以及集團所有董事、高級人員及僱員。

有關本政策的任何問題，請聯絡各集團公司的法律部（或集團法律部（如適用））。如任何僱員知悉任何法律或規例阻止他們遵守本政策或在違反本政策（包括資料安全漏洞）的情況下採取規定的行動，則該僱員必須於緊隨知悉有關法律或規例（或違反本政策的行為）後通知各集團公司的法律部（或集團法律部（如適用））。

附錄一及二載列本政策所用的常用詞彙及主要概念概要。

2. 管理架構

各集團公司的高級管理人員須對有效實施本政策（包括下文所載的資料私隱原則及程序）負責。高級管理人員須確保在（及遵守）適用資料保護法律的規限下，本政策獲併入及納入當地政策及程序。

作為客戶、僱員及其他個人信息當事人的「個人信息處理者」（亦稱為「管理者」），各集團公司必須以能夠證明遵守其適用資料保護法律的方式實施其當地政策及程序，包括（如需要）：

(a) 確保立法及監管規定獲納入涉及處理個人信息的所有操作程序及活動中（如確保涉及處理個人信息的所有新項目有「保護私隱的設計」）；

(b) 實施適當的技術及機構措施，旨在有效實施資料私隱原則及在處理活動中加入必要保障，並按照其營運所在司法管轄區的規定保護個人信息當事人的權利；

(c) 為僱員進行保護私隱及資料意識的培訓，以確保他們關注及了解本政策以及在保護個人信息管理及私隱方面的責任；

(d) 對其業務進行定期私隱風險評估，以評估私隱風險（包括與第三方供應商有關的風險）及緩和控制措施是否充分；

(e) 確保個人信息按其敏感度分類及處理，並按知情需要限制存取；及

(f) 指派適當的私隱及資訊科技安全專家支援業務管理其資料私隱風險（如委任資料保護人員（如需要））。

所有參與處理個人信息的僱員均應了解及遵守本政策，以及集團公司實施的任何相關政策、程序及指引。未有按照本政策處理個人信息或會導致紀律行動。嚴重及／或故意違反本政策者或會被解僱。

3. 資料私隱原則

集團任何時候均應按照以下資料私隱原則處理個人信息。

3.1. 合法、公平及透明地處理

(a) 僅會以合法、公平及透明的方式使用個人信息。

(b) 個人信息的使用應遵守集團營運所在各司法管轄區內的適用資料保護法律。各集團公司對於處理客戶、僱員及其他個人信息當事人的個人信息的時間、方式及目的，以及個人信息當事人在該司法管轄區就其個人信息的處理擁有哪些選擇及權利應保持透明。

(c) 個人信息的存取應僅限於需要知悉有關資訊以履行其在集團內職責的僱員，而敏感個人信息（包括其存取）須獲得最高程度保護。

3.2. 資料私隱原則

僅應基於特定、明確及合法的目的並在需要達到該等目的時收集個人信息。使用個人信息有助改善集團提供的服務，但使用該等資料應具有明確目的。禁止過度收集個人信息。

3.3. 資料準確性

應採取合理措施確保持有的任何個人信息屬準確及最新。

3.4. 保留資料

個人信息僅應於有必要保留以作其指定用途的期間保存。各集團公司應向相關管理人員及員工發出有關文件保留期的指引。

3.5. 合法、公平及透明地處理

(a) 個人信息應按照集團營運所在各司法管轄區內適用資料保護法律下的個人信息當事人權利處理。

(b) 個人信息當事人對存取、修改、刪除或其他涉及其個人信息的所有要求均應以符合適用資料保護法律的方式處理，並以適當的程序接獲及回應該等要求。

3.6. 資訊安全

(a) 應採取適當的技術及機構安全措施以保障受託於集團的個人信息，免受未經許可或非法處理，並避免意外遺失、損毀或損壞，以確保與風險切合的安全水平（如個人信息去識別化／採用假名及加密及／或其他適當的安全措施）。

(b) 應定期實施及檢討安全措施，以確保其提供適當的保護水平。

(c) 應採用同等的安全水平保護代表第三方處理的個人信息（如任何集團公司擔任「合約處理者」或「資料處理者」）。

3.7. 個人信息的跨境傳送

集團在全球經營業務，故有需要在國際間傳送資訊。除非有關傳送符合適用資料保護法律，否則個人信息不應傳送至並無提供充足資料保護及適當保障的國家或地區。

4. 程序

各集團公司須實施適當的程序以確保個人信息按照資料私隱原則及適用資料保護法律公平及合法地處理。

4.1. 處理記錄

如適用資料保護法律有所規定，各集團公司應保存處理活動的記錄及有關遵守資料保護的文檔。集團及各集團公司應定期對其個人信息處理以及遵守資料私隱原則和適用資料保護法律進行審計。

4.2. 私隱影響評估

如適用資料保護法律有所規定或在管理私隱風險的適當情況下，應對新產品、技術及業務營運進行私隱影響評估。例如，如項目涉及以下一項或多項：處理大量個人信息或處理過程影響大量個人信息當事人；將現有個人信息用作新及／或更具侵犯性的目的；處理敏感個人信息及／或遺傳或生物特徵資料（如指紋掃描、人臉識別）；引入新及侵犯性的技術（如閉路電視錄影機、定位技術、自動決策）；向外傳送個人信息、承包個人信息處理、向非集團實體或個人提供個人信息或披露個人信息；或進行任何類型的僱員監察（包括任何記錄及／或審查僱員的通訊或活動，包括電話通話、電子郵件及電腦文件）。除了自我評估外，在若干情況下可能需要由私隱機構進行安全評估。例如，當任何在中國內地營運的集團公司傳送其性質或數量需要由中國國家互聯網信息辦公室（「國家網信辦」）批准的個人信息時，將需要由國家網信辦進行強制性安全評估。

4.3. 私隱通知

如適用資料保護法律有所規定，各集團公司應實施適當的私隱政策／通知（「私隱通知」），包括但不限於向客戶、僱員及其他個人信息當事人使用清晰易懂的語言解釋處理的個人信息類別及用途。該等私隱通知應隨時可供查閱及更新，如適用資料保護法律有所規定，應備有簡單機制供個人信息當事人選擇不處理或不同意處理其個人信息。

4.4. 個人信息當事人的要求

個人信息當事人對存取、修改、刪除或其他涉及其個人信息的所有要求均應根據符合適用資料保護法律的程序處理。

4.5. 向執法機構／其他監管機構披露個人信息

集團可能有責任在若干特定及有限情況下向執法機關或其他監管機構披露個人信息。回應個人信息的正式要求應與保護個人信息的義務作出平衡。所有僱員必須遵守相關程序，如有疑問，必須諮詢集團資料保護主管（或集團法律部（如適用））。

4.6. 與私隱機構合作

集團致力配合私隱機構的查詢及調查，特別是如其關注僱員、客戶或任何集團公司網站用戶及其他個人信息當事人的私隱。私隱機構發出的通訊應立即轉介至集團資料保護主管（「資料保護主管」）（或集團法律部（如適用））處理。

4.7. 資料安全事故

當發生涉及個人信息的資料安全事故（「資料安全事故」）時，相關集團公司應致力盡快減輕潛在後果並確保個人信息免受進一步未經許可存取、使用或損壞。各集團公司應迅速及按照適用資料安全事故程序作出回應，當中可能包括通知私隱機構及／或受影響個人信息當事人（如需要）。如資料安全事故涉及個人信息，應立即通過

dpo@hutch-med.com 通知集團資料保護主管。應不時發出通知及處理資料安全事故的進一步指引。

4.8. 使用閉路電視

使用閉路電視可能涉及處理個人信息當事人的可識別影像。當使用時，各集團公司必須考慮使用閉路電視及處理所收集資料時所捕捉影像的潛在敏感性質。參與使用閉路電視的僱員應接受有關使用的培訓，以確保符合適用資料保護法律。

4.9. 將個人信息用於營銷活動和銷售個人信息

為直接營銷目的處理個人信息和銷售個人信息受不同司法管轄區適用資料保護法律的特殊監管規定約束。為直接營銷目的處理個人信息必須嚴格遵守適用資料保護法律的監管規定。

集團並無銷售個人信息以換取金錢上的代價。如集團於任何時候預計銷售個人信息，則該建議必須獲集團資料保護主管經諮詢集團法律部後批准。如　閣下認為披露或潛在披露個人信息可能構成銷售，　閣下應立即聯繫集團資料保護主管。

4.10. 第三方處理者

如在涉及處理個人信息的部分業務營運中委聘第三方服務供應商，則必須確保：

(a) 在篩選該等供應商時已進行適當審查，並持續監察及檢討第三方供應商；

(b) 個人信息當事人在私隱通知中獲知會有關披露情況，並在適用資料保護法律規定的情況下提供選擇退出權或必要的選擇加入同意；

(c) 該第三方根據本政策實施充足的私隱及安全保障措施；

(d) 於開始處理前已擬定包括資料私隱條款的合約並經相關集團公司的法律部批准；及

(e) 實施有關聘用第三方的私隱影響評估得出的任何建議（如適用）。

附錄一：詞彙

詞語	釋義
適用資料保護法律	指相關國家確保保護個人信息的適用法律及規例。
客戶	指集團公司貨品及服務的所有客戶（不論線上及／或線下），包括客戶會員計劃的會員。
合約處理者或資料處理者	指代表資料管理者處理個人信息的實體（而資料處理的涵義將根據本定義詮釋）。
資料處理	指對個人信息作出的任何行動（不論是否利用自動方式），包括收集、記錄、組織、儲存、修改或更改、檢索、諮詢、使用、披露、提供、排列、合併、限制、刪除及銷毀個人信息。
資料安全事故	指個人信息的安全、機密、完整或提供已經或可能受損的任何實際或懷疑事件。例如：資料或儲存個人信息的設備遺失或被竊；共用或不當使用密碼，以致允許未經許可存取個人信息；資訊科技系統故障；人為錯誤；不可預見的情況，如火災或水災；資訊科技系統遭黑客攻擊；不當處理或處置個人信息；及透過欺詐獲得個人信息的罪行。
僱員	指為集團工作的所有人士，包括持有臨時、定期及永久僱傭合約的僱員。
個人信息	指直接或間接識別自然人的資訊，不論是客戶、僱員或集團公司網站用戶或其他個人信息當事人。
個人信息處理者或資料管理者	指單獨或與他人共同決定個人信息處理目的和方式的實體。
個人信息當事人	指與個人信息識別或關聯的自然人。
私隱機構	指相關國家負責管理及執行相關適用資料保護法律的資訊專員公署或同等監管機構。
敏感個人信息	指基於其敏感性質而在處理時受到額外法律管制的任何個人信息，包括以下特殊類別的個人信息：關於個人信息當事人的種族或民族起源、意識形態或政治觀點、宗教或哲學信仰、工會會員、身體或精神健康、性生活或取向、刑事定罪或涉嫌干犯任何罪行的資料，以及任何遺傳或生物特徵資料。

附錄二：主要概念

何謂「處理」？

適用資料保護法律監管「處理」（即處理）個人信息。處理的定義非常廣泛，並包括收集、記錄、組織、儲存、修改或更改、檢索、諮詢、使用、披露、提供、排列、合併、限制、刪除及銷毀個人信息等一系列活動。該等規則適用於持有電腦數據庫、經文檔處理的文件及錄音帶內的資料，或錄影帶、CD、DVD 或以數碼影像形式儲存可識別人物的影像。適用資料保護法律亦監管以檔案系統持有的紙張資訊。

何謂「個人信息」？

如資料有關(a)從該等資料中，或(b)從集團管有或其很可能管有的該等資料及其他資訊中可以被「識別」或「可予識別」的活著的個人，則該資料便是個人信息。因此，個人信息的概念極其廣泛。在某些國家，與公司實體有關的資訊乃被視為個人信息。

例子：如一個電話號碼可以識別活著的個人，則該電話號碼本身可能是個人信息。信用卡載有的資訊構成個人信息，因為其載有持卡人的姓名。根據適用資料保護法律，客戶會員卡號碼本身被視為個人信息，因為會員卡發卡人可識別該號碼所屬的個別人士。錄影機內的片段如可識別個人，便可是個人信息。電話或電子郵件記錄資料包含個人信息，因為可以直接或間接識別進行通訊的個人。

個人信息亦包括對個人的意見的任何表達以及本公司或任何集團公司或任何其他人士就該個人的意向的任何指示。

何謂敏感個人信息？

敏感個人信息指處理時受到額外法律管制的各類型資料，並包括關於個人種族或民族起源、意識形態或政治觀點、宗教信仰或類似性質的其他信仰、工會會員、身體或精神健康狀況、性生活、刑事定罪或涉嫌干犯任何罪行的資料。請注意，在某些司法管轄區，有關定義可能有別，而在某些司法管轄區，與犯罪及訴訟有關的資訊將構成「司法資料」並須遵守特定規則。許多國家對處理敏感個人信息及司法資料有更嚴謹的規則。如本公司或任何集團公司依靠同意處理

敏感個人信息，該同意必須是「明確」的，即個人信息當事人需要採取一些主動步驟以顯示其接受。此外，根據集團營運所在若干司法管轄區（如歐盟和中國）的適用資料保護法律，需要獲得「獨立」同意。

資料管理者與資料處理者有何分別？

個人信息處理者或**資料管理者**是控制收集資料的方式及目的的實體，即使其本身並非實際持有資料。因此，即使資料由代表本公司及各集團公司行事的第三方持有（如工資管理外判予第三方），本公司及集團公司將是有關其僱員、客戶或其他個人信息當事人的資料的資料管理者。代表資料管理者持有及處理個人信息的人士是**合約處理者**或**資料處理者**。如本公司或集團公司聯同另一人士控制處理的方式及目的，雙方可為聯合資料管理者。

例子：集團公司有若干學術培訓資料希望發送予所有相關醫護專業人員。第三方機構代表並根據集團公司的指示進行處理（如發送學術培訓資料）。相關集團公司為資料管理者，而該機構將為資料處理者。