和黃醫藥
HUTCHMED

和黃醫藥（中國）有限公司

信息安全政策

董事會於 2012 年 2 月 10 日採納

目錄

1. 目的及範圍
2. 問責
3. 相稱性
4. 需者方知
5. 組織角色及責任
   5.1. 集團信息安全主管
   5.2. 信息安全託管人
      5.2.1. 委任信息安全託管人
      5.2.2. 信息安全託管人的責任
   5.3. 信息所有者
   5.4. 人力資源
6. 信息管理
   6.1. 分類及標註
   6.2. 持續保護
   6.3. 信息披露
   6.4. 變更控制
7. 獲取控制
8. 評價
9. 惡意軟件
10. 意識
11. 教育
12. 事件管理
13. 經營持續性及應急計劃
14. 法律、監管及合約規定
15. 信息私隱
16. 政策的記錄及管理
17. 豁免遵守本政策
18. 違反政策

附錄一：《數據分類及標註指引》

1. 數據分類
   1.1. 公開
   1.2. 內部使用
   1.3. 部門內
   1.4. 機密
   1.5. 高度機密
2. 信息標註

1. 目的及範圍

本文件旨在界定及協助傳達將在整個和黃醫藥集團（包括和黃醫藥（中國）有限公司（「和黃醫藥」）、其附屬公司及共同控制實體，（「和黃醫藥集團」））應用的關於信息保密、完整及可獲取方面的一般政策。本政策之目的在於通過在和黃醫藥集團內預防安全風險及將安全風險的影響降至最小來確保業務的持續經營。

本信息安全政策適用於和黃醫藥集團的所有成員公司，包括位於所有國家的所有業務實體。

該政策適用於和黃醫藥集團內所有不同類型信息的創建、交流、存儲、傳輸及銷毀。該政策適用於所有形式的信息，包括但不限於電子文件、紙質文件以及不論通過口述、電話或以其他方式作出的口頭披露。

任何公眾已知悉的信息不在本文件範圍內。

2. 問責

和黃醫藥集團內的各人均有責任保護信息。

- 信息安全問責及責任必須在整個和黃醫藥集團內清楚界定及承認。
- 和黃醫藥集團內的各方（員工、顧問、承包商及臨時工）對其各自獲取及使用信息（如增補、修改、複製及刪除）負責。
- 所有責任方必須妥善保管任何實體鑰匙、ID 卡及電腦／網絡賬號。此包括創建難以猜測的電腦密碼。
- 所有責任方必須及時行動、相互協調，以防止出現違反信息安全及信息系統（人工或電腦，或兩者）的行為和威脅，或者對這些行為作出回應。
- 所有責任方必須在捨棄包含在任何實體文件（如備忘錄、報告、縮微膠卷、縮微膠片）或任何電子、磁力或可選存儲媒介（如 U 盤、光盤、硬盤、磁帶、軟盤）內的任何無法使用的機密或高度機密信息前，將其銷毀。

3. 相稱性

信息安全控制應與信息被修改、拒絕使用或披露的風險相稱。

- 信息安全措施應與信息的價值及敏感程度以及信息容易受到的威脅相稱。
- 信息安全措施應抵銷信息存儲、傳輸、處理或使用所在的內外部環境中的內在風險。

4. 需者方知

公司信息應僅限於擁有明顯業務理由獲取信息的人士可獲取。

5. 組織角色及責任

和黃醫藥集團應識別組織角色及責任，以創建、傳達、實施及規管本政策。

除本文件所識別的特定角色及責任以外，各業務實體的管理層均有責任確保本文件內包含的政策在其管轄範圍內得到實施。

5.1. 集團信息安全主管

集團信息安全主管（和黃醫藥高級財務經理）應負責：

1. 建立及完善整個和黃醫藥集團的信息安全文化。
2. 管理和黃醫藥集團信息安全政策的制定、部署及維護。
3. 保證整個和黃醫藥集團的信息安全狀況，包括和黃醫藥集團信息安全政策的適當部署及遵守狀況。
4. 協調與重大安全事宜相關的活動。

特別是，集團信息安全主管應：

- 於必要時發佈本政策的遵守標準。
- 檢討和黃醫藥集團信息安全措施的成效，包括（如有必要）審查及監察和黃醫藥集團內的安全事件。
- 執行業務實體報告程序，以匯報其信息安全狀況及重大信息安全事宜。
- 制定和黃醫藥集團層面的信息安全治理及風險評價方法。
- 促進整個和黃醫藥集團了解潛在威脅、漏洞及控制技術。
- 監控和黃醫藥集團內外部的信息安全趨勢，並讓和黃醫藥集團的高級管理層隨時了解影響組織的信息安全相關問題及活動。

5.2. 信息安全託管人

5.2.1.委任信息安全託管人

各業務實體的管理層應委任一名信息安全託管人（各業務部門的財務總監）。信息安全託管人應負責：

1. 建立及完善業務實體的信息安全文化。
2. 確保制定及部署額外的程序及標準，以配合和黃醫藥集團的信息安全政策及相關政策、程序及標準。
3. 保證業務實體的信息安全狀況，包括和黃醫藥集團信息安全政策、程序及標準的適當部署及遵守狀況。
4. 協調與重大安全事宜相關的活動。

5.2.2. 信息安全託管人的責任

信息安全託管人應：

- 在業務實體內界定額外的信息安全角色及責任。
- 確保部署方法、程序及風險評價，以配合和黃醫藥集團的信息安全政策、程序及標準。
- 確保部門程序配合保密、完整及可獲取的目標。
- 確保限制有效傳達給以任何形式（實體或電子）使用、管理、獲取、存儲、處理或轉移信息的人士。
- 提供信息安全教育，並確保培訓課程舉行及得到參加。
- 確保每位員工明白其信息安全相關責任。
- 在業務實體內執行信息安全狀況報告程序，並在必要時向業務實體管理層及和黃醫藥集團匯報。
- 檢討業務實體信息安全措施的成效，包括審查及監控業務實體內的安全事件，並（如有必要）向和黃醫藥集團匯報。
- 幫助業務實體考慮持續經營及計劃經營的信息安全風險。
- 與業務實體管理層合作評價信息安全風險。
- 促進業務實體內了解潛在威脅、漏洞及控制技術。
- 監控業務實體內外部的信息安全趨勢，並讓業務實體的高級管理層隨時了解影響業務實體的信息安全相關問題及活動。

5.3. 信息所有者

各業務實體的管理層應確保和黃醫藥的任何信息均獲分配一名所有者，簡稱「信息所有者」。在本文件中，「信息所有者」一詞僅適用與本政策相關的信息安全事宜，並不意味對信息的任何形式的法定所有權。

一般而言，除非另行指定，否則

1. 一項信息的創建者應被假定為信息所有者。
2. 對於從外部方接收的信息，指定接收者應為默認信息所有者。

信息所有者負責：

- 確定與信息相關的授權及處理程序。
- 採取步驟確保對信息的存儲、處理、分發及常規使用已採取適當的控制措施。
- 確保需要知道信息的所有相關人員均可獲取信息。

5.4. 人力資源

人力資源（HR）部門在安全管理方面起到至關重要的作用。HR 負責：

- 核實員工招聘申請表上的信息，如背景調查；
- 確保所有員工開始工作前簽訂的僱傭協議內包含保密條款，並確保員工了解該保密條款的條款及條件。

6. 信息管理

6.1. 分類及標註

為管理及控制信息的獲取，業務實體執行人員應考慮正式的信息分類及標註，但須在充分考慮業務需要、成本（內部及外部）及切實可行性的前提下進行。《數據分類及標註指引》載於附錄一。

6.2. 持續保護

信息必須持續得到保護，而不論其所在地點、所採取形式或目的。

6.3. 信息披露

各業務實體的管理層，在諮詢信息安全託管人及遵守集團信息安全主管頒佈的標準後，將可就披露及接收任何敏感信息(例如發出或簽訂保密協議)以及處理從外部方接收的敏感信息制定及實施具體規則及指引。

6.4. 變更控制

與信息安全程序相關的變更，包括系統及程序變更，必須經過適當批准、記錄及傳達相關各方。和黃醫藥集團應為機密信息實施正式的變更控制程序。

7. 獲取控制

和黃醫藥集團應制定適當控制措施以平衡信息及配套信息資源的獲取，從而抵禦相關風險。

- 信息的獲取必須以需者方知為基礎加以控制，並根據與其分類相應的具體業務要求而定，而不論要求獲取信息的人士的職位高低。
- 信息的獲取必須經過授權。每個信息系統（不論是電腦信息系統與否）都應執行授權程序。授權程序應經過信息所有者及相關信息安全託管人的批准。

8. 評價

和黃醫藥集團應定期評價信息及信息系統風險。

- 業務實體執行人員應確保定期及在情況需要時進行風險評價，以確定已實施的信息保護控制措施的成效。風險評價過程中發現的不足之處應在符合風險發生可能性及影響的時間框架內得到解決。
- 各業務實體的信息安全實施情況應定期或在業務實體發生重大改變而將可能改變其風險環境時，進行獨立審查。

9. 惡意軟件

惡意代碼或軟件（如特洛伊木馬、邏輯炸彈及混合威脅）可導致嚴重破壞，為降低相關風險，全體員工在接入互聯網及使用任何形式的可移除式媒體以將信息轉入／轉出和黃醫藥集團工作站時必須加以注意。

10. 意識

需者方知的所有各方應可獲得已應用於或可用於信息及信息系統安全的原則、標準、慣例或機制，並應了解對信息安全的相關威脅。

- 在允許獲取信息或配套信息資源前，應對與所有各方的誠信、是否有需要知道及技術權限相關的適當資格進行核實。
- 和黃醫藥集團的全體人員必須了解和黃醫藥集團的信息安全政策及程序，且必須同意按照該等政策及程序開展工作。
- 和黃醫藥集團的業務合作夥伴、供應商、客戶及其他有業務往來人士必須通過界定他們與和黃醫藥集團之間關係的合同上所載的具體措辭了解他們的信息安全責任。
- 集團信息安全主管應建立渠道及組織在和黃醫藥集團業務實體之間分享及交流信息安全相關知識及經歷。

11. 教育

本信息安全政策應傳達全體人員，確保他們了解本政策以及他們在其下的責任。

- 全體員工必須參加信息安全培訓。培訓應包括政策、標準、基準、程序、指引、責任、相關強制執行措施以及未能遵守後果。培訓及進修培訓應定期舉行。
- 和黃醫藥集團的全體人員必須獲提供配套參考材料以讓他們能夠適當保護及以其他方式管理和黃醫藥集團的信息。

12. 事件管理

所有信息安全事件都應得到迅速及有效回應，以確保將任何對業務的影響降至最小以及確保減少發生類似事件的可能性。

- 信息安全事件，即任何損害或可能損害信息安全的事情，必須向相關各方匯報，包括信息所有者、信息安全託管人以及該業務實體內或和黃醫藥集團的其他實體內可能受到事件潛在影響的人士。處理事件所採取的步驟及事件的解決方案亦必須匯報。

13. 經營持續性及應急計劃

信息系統應以維持組織經營的持續性為目標進行設計及運行。

- 和黃醫藥集團的業務實體應落實一項計劃以確保維持信息的保密、完整及可獲取，從而在干擾或災難發生時支持業務持續經營。該計劃必須記錄以及傳達相關各方，並定期舉行相關演習。

14. 法律、監管及合約規定

所有與信息安全相關的法律、監管及合約規定都必須得到考慮和關注。

- 在處理信息安全時，和黃醫藥集團必須至少滿足所有適用的監管規定。由於不同業務實體可能有不同甚至相互抵觸的監管問題，因此各業務實體均有責任確保遵守其各自的監管及其他法律規定。

15. 信息私隱

各業務實體在實施信息安全措施時應小心謹慎以遵守適用法律及和黃醫藥集團的信息私隱政策。

16. 政策的記錄及管理

和黃醫藥集團應制定及維護政策及配套標準、基準、程序及指引，以解決信息安全的各個方面。相關指引必須分配責任、斟酌權限以及各單獨實體或組織實體獲授權承擔的風險水平。

- 本信息安全政策可能會更新，需要定期進行審閱及維護。本政策的維護及更新可能包括但不限於監管問題及法律變更、核心業務變更和技術變更。

17. 豁免遵守本政策

豁免遵守本政策有時可能是為了業務或切合實際目的而需要。此時必須經過業務實體負責人在聽取信息安全託管人的建議以及獲得集團信息安全主管的批准後授權。

- 豁免（包括其理據、持續時間及詳情）必須在合理時間框架內記錄。
- 豁免應在業務或風險變動、負責執行人員變更時重新評價及重新批准，或在集團信息安全主管確定的一段期間後重新評價及重新批准，以孰早者為準。

18. 違反政策

違反信息安全政策會被認為是嚴重違反情節，在重點防範未來違反的同時，將進行適當處理。

- 未遵守信息安全政策、標準或程序會導致採取紀律行動，包括解僱。

附錄一：《數據分類及標註指引》

1. 數據分類

所有信息都應根據其敏感程度進行分類。建議分為五大默認類型，分別是：

- 公開
- 內部使用
- 部門內
- 機密
- 高度機密

該等分類已根據「需要知道」政策（即公司信息應僅限於擁有明顯業務理由獲取信息的人士可獲取）進行設計，以保護信息不會被未經授權披露、使用、修改或刪除。

未明確分類的信息應進行審查以確定分類，若此無法進行，則該信息應默認被視為分類為「內部使用」，並應據此進行處理。

在本附錄中：

- 一項信息的獲取控制名單是獲授權有權獲取信息的各人士或各方的名單；
- 分發名單是信息以實體形式分發給各人士或各方的名單。

1.1. 公開

「公開」分類適用於經過相關業務實體的管理層明確批准用於向和黃醫藥集團外的公眾披露的信息。

- 僅指定人士可將信息分類為「公開」。
- 僅指定人士可披露「公開」信息。相關披露應遵循預定程序、規則及指引。

1.2. 內部使用

「內部使用」分類適用於若不經意或未經授權披露可能會導致業務單位、子集團或和黃醫藥集團遭受不利後果以及在糾正這些後果時可能導致產生費用的信息。

「內部使用」信息未經信息所有者的事先批准，不得向和黃醫藥集團外的任何人士披露。若「內部使用」信息存在任何獲取控制名單，該名單未經信息所有者的事先批准，不得向相關獲取限制外的任何其他人士披露。無獲取控制名單的「內部使用」信息可在和黃醫藥集團內披露。

信息所有者亦可對「內部使用」信息施加額外的披露或處理限制。額外限制不得減弱本文件所載基本披露規則的效力。

1.3. 部門內

「部門內」信息可在自身部門成員之間自由分享。與自身部門外的個人分享該等信息需要經過相關信息所有者的授權。

1.4. 機密

「機密」分類適用於若不經意或未經授權披露可能會導致業務單位、子集團或和黃醫藥集團遭受嚴重不利後果以及在糾正這些後果時可能導致產生重大費用的信息。

「機密」信息應一直存置分發名單或獲取控制名單，且未經信息所有者的事先批准，不得向相關分發名單或獲取控制名單外的任何人士披露。獲取控制名單不存在時，分發名單應被視作獲取控制名單。分發名單及獲取控制名單同時不存在時，未經信息所有者的事先批准，「機密」信息不得向任何人士披露。

信息所有者亦可對「機密」信息施加額外的披露或處理限制。額外限制不得減弱本文件所載基本披露規則的效力。

此外，「機密」信息必須在處理（包括展示、存儲、傳輸及清理）時得到進一步保護，以防止被蓄意及不經意未獲授權披露。

1.5. 高度機密

「高度機密」信息以「需要知道」為基礎，僅可在有限數量的被相關信息所有者認定的個人中分享。

由於和黃醫藥集團的業務及地方法律的多樣性，和黃醫藥集團的業務單位應進一步考慮其業務需要、遵守各項法例及行業要求，以設定其合適的分類。然而，最終分類應可歸入於五大默認分類之中，且不得違反本政策所載原則或與之抵觸

2. 信息標註

業務實體的管理層負責為其各自的業務實體評價、設計及實施適用的具體信息標註程序。然而，該活動應符合及支持以下標準：

1. 為當地法律所規定；或
2. 在無其他替代方案的情形下，單獨標註是利益相關者可以知悉該信息的敏感程度的唯一方法，且：
    - 該方法在技術上可行；及
    - 該方法在經濟上可負擔，即採用該方法產生的利益合計超過包括持續維護成本在內的成本。

若業務實體確實決定採用標註方法，則以下規則應適用：

- 「機密」信息應為首要標註對象。
- 信息所有者負責根據信息分類對信息進行標註。
- 僅信息所有者或信息所有者指定的人士應獲授權變更信息的分類標籤。
- 分類標籤應顯眼。
- 獲取控制名單及任何額外限制應清楚地載於分類標籤上或以其他方式顯眼。例如，分類標籤可為「內部使用－僅供 X 公司使用」或「機密－僅供 XX 部門使用」或「內部使用－僅供和黃醫藥集團內部使用」。
- 獲取控制名單或額外限制不可取代分類，即不論是何額外限制，信息的分類（如「機密」）應顯示在標籤上。