

# 從分享到銷售：使用區塊鏈技術建立數位健康資料市場的挑戰與機遇

Mohamed A. Maher, MBA<sup>1,2\*</sup>  和 Imtiaz A. Khan, PhD<sup>(1)</sup> 

<sup>1</sup>卡地夫科技學院，卡地夫都會大學，卡地夫，英國；<sup>2</sup>Balsamee LTD，卡地夫，英國

## 摘要

在 COVID-19 大流行期間，我們見證了生物和生物醫學資料的分享如何促進研究人員、醫療工作者和政策制定者在全世界範圍內應對該大流行。儘管醫師對電子健康記錄 (EHR) 及個人可穿戴式數位小工具的使用日增，但仍有 80% 的健康及醫療資料未被使用，對研究人員及醫務人員的工作幾乎毫無價值。與健康資料分享相關的立法限制、傳統資料管理系統的集中式孤島設計，以及最重要的缺乏獎勵模式，都被認為是健康資料分享的根本瓶頸。

隨著歐盟 (EU) 「一般資料保護條例」 (GDPR) 的出現，以及區塊鏈和分散式總帳技術 (DLT) 等技術的發展，現在有可能創造一種新的資料分享模式，將激勵模式從目前的權威或利他形式轉變為共享經濟模式，其中財務激勵將成為資料分享的主要驅動力。這可透過建立數位健康資料市場 (DHDM) 來實現。

在此，我們回顧提出技術模型或實作框架的論文，這些論文將類區塊鏈技術用於健康資料。我們試圖了解並比較這些文章中概述的與實施和優化 DHDM 運作相關的不同技術挑戰。我們也檢視歐盟和其他國家 (如美國) 背景下的法律限制，以適應此類市場的任何合規要求。最後但並非最不重要的是，我們回顧了研究此類市場對廣泛利益相關者的短期、中期和長期社會經濟影響的論文。

Keywords: *blockchain; EHR; marketplace; GDPR; general data protection regulation; incentives*

部分：敘述/系統性評論/元分析

收到：22 September 2021; Revised: 27 September 2021; Accepted: 接受：2021 年 12 月 30 日; 發表：2022 年 1 月 28 日

自從數位醫療的早期導入以來，資訊與通訊技術 (ICT) 開發人員一直認為使用數位技術處理健康資訊將可產生大量資料，進而改變醫療照護產業。將這些資料餵給機器學習演算法，將可讓我們去除醫療實務的技巧，並提出新的診斷和治療流程。DeepMind Health 等專案是最近的一個範例，一家位於倫敦、由 Alphabet 擁有的人工智慧公司開發了行動應用程式流 (1)，利用倫敦皇家自由醫院的 EHR

資料來預測和識別即將患上急性腎臟損傷的病患 - 在英國，這種情況每年導致 10 萬人死亡 (2)。此外，Patients-LikeMe (3) 等門戶網站可讓有類似病症及/或疑慮的病患分享有關治療的資訊，對使用者有顯著的助益 (4、5)。

當這些專案開始顯示資料分享的價值時，歐盟 (EU) 於 2018 年推出的《一般資料保護條例》 (GDPR) (6)，透過重新定位所有權和管理權，從根本上改變了患者資料的分享和使用模式

\*Correspondence: Mohamed A. Maher. 電子郵件: m.maher2@outlook.cardiffmet.ac.uk ; mohamed.maher@balsamee.co.uk

**表 1.** 歐盟的一般資料保護條例從根本上改變了分享和使用病患資料的模式，將醫療資料的所有權和管理權由服務供應商重新定位為病患，同時賦予病患以下權利 (6)

一般資料保護規範	定義
GDPR 第 12 和 13 條	知情權 <ul style="list-style-type: none"> <li>個人有權獲知其資料的蒐集及任何用途。</li> </ul>
GDPR 第 15 條	存取權： <ul style="list-style-type: none"> <li>個人有權查閱其資料。</li> </ul>
GDPR 第 16 條	更正權： <ul style="list-style-type: none"> <li>若個人資料不完整，個人有權要求修正或填寫不完整的個人資料。</li> </ul>
GDPR 第 17 條	刪除權： <ul style="list-style-type: none"> <li>個人要求刪除個人資料的權利，通常稱為「被遺忘的權利」。</li> </ul>
GDPR 第 18 條	限制處理的權利： <ul style="list-style-type: none"> <li>個人要求限制或壓制其資料的權利。</li> </ul>
GDPR 第 20 條	資料可攜性的權利 <ul style="list-style-type: none"> <li>允許個人在不影響其可用性的情況下，安全且有保障地輕鬆將資料從一個 IT 系統攜帶、移動、複製或傳送另一個 IT 系統。</li> </ul>
GDPR 第 21 條	反對權 <ul style="list-style-type: none"> <li>在某些情況下，個人有權反對處理其資料。</li> </ul>
GDPR 第 22 條	關於自動決策和個人資料側寫的權利： <ul style="list-style-type: none"> <li>如果組織正在執行對個人有重大影響的自動化決策，則會制定保護個人的規則。</li> </ul>

的醫療資料，同時賦予表 1 所列的下列權利。

如果 DeepMind 不是在 GDPR 引入之前啟動，或者 PatientsLikeMe 是在歐洲經濟區 (EEA) 的管轄範圍內，上述兩個專案甚至都無法啟動。現在更明顯的是，資料在存取權或散佈權上只有一位擁有者和把關人。即使是匿名，也只有患者才有權允許存取其資料，並允許以對所有人都有利的方式使用資訊。具有諷刺意味的是，患者尚未意識到這種新所有權的價值，以及如何管理其管理權。這是因為沒有為他們創造直接的贏利，以及間接的贏利，而間接的贏利還不夠明確，不足以克服資料洩漏和隨之而來的隱私暴露的合理憂慮。因此，我們的目標是找到新穎的方法和工具，在個人隱私和透明的資料存取之間取得平衡，以達到研究目的 (7)。

GDPR 為服務供應商引入的這一範式轉變，也為個人透過向醫學研究人員或科技公司出售資料，將其醫療資料貨幣化帶來了機會。與 Airbnb 讓個人能夠將其空餘居所貨幣化的做法類似，擁有 GDPR 賦予的新所有權和其他權利的患者，現在可以透過「數位健康資料市場」(DHDM)，利用共享經濟模式將其個人健康資料貨幣化。圖 1 展示了 DHDM 的運作流程。然而，在目前的集中式資料管理架構下，電子健康記錄 (EHR) 分散於

不同的服務單位，因此，DHDM 的運作流程可能會有差異。

在不同組織和地理管轄區有不同法規的情況下，提供者的存取和管理將是極具挑戰性的，尤其是在這種分散式環境中的微交易行為。在此背景下，區塊鏈與相關的智慧型契約已被視為改變遊戲規則的技術，其內建的分散式架構，能以分散的方式管理資訊內在治理，適用於以交易為基礎的數位服務。

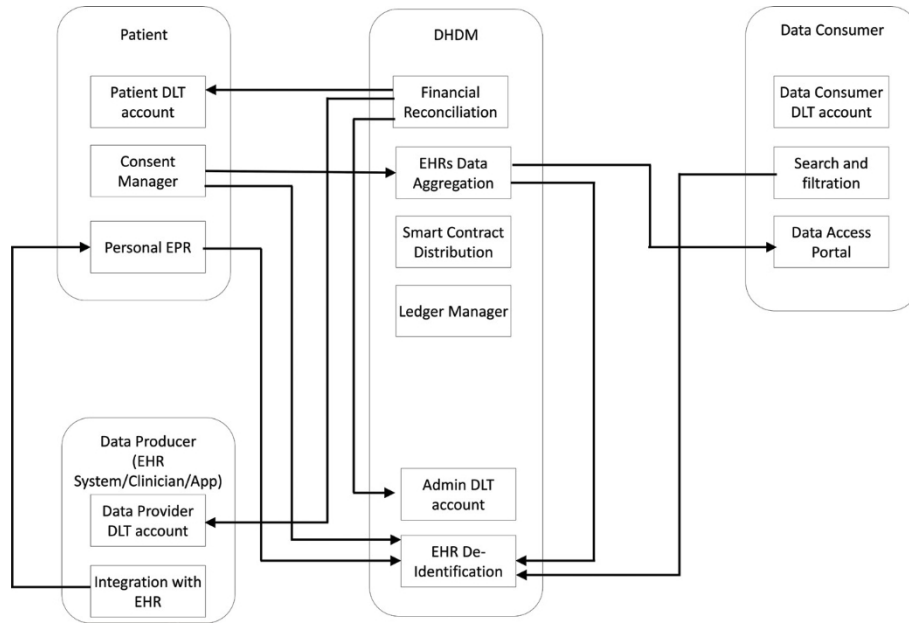
本文其餘部分的組織如下：首先，我們檢閱了 36 篇關於技術挑戰的論文，重點在三個領域，例如資料所有權與存取控制、資料互通性與資料安全性。接著，我們檢閱了 7 篇關於法律問題的論文，最後是 9 篇關於社會經濟問題的論文。

## 技術挑戰

### *資料所有權與存取控制*

誰擁有醫療照護資料？這個問題一直引人好奇，並從技術、法律和哲學角度引起爭論。Kostkova 等人曾針對此議題提出爭論，並質疑健康資料是否應該開放給研究使用，試圖在個人隱私與全球數百萬人生活的資料支持研究價值之間取得平衡 (7)。作者在結論中敦促國際層面上的決策者制定一個監管框架，以保障個人資訊、限制商業利用，同時又能讓資料用於研究和商業用途。

在提出基於區塊鏈的存取控制工具和模型方面，已經做了大量的工作、



**圖 1.** DHDM 作業工作流程的四個介面：透過病患介面（左上方），病患可設定其帳號、完成其電子健康記錄 (EHR)，並透過同意與其選擇的研究人員共用其資料來管理存取控制。透過資料製造者介面（左下），照護提供者和其他資料製造者可建立他們的帳號，並透過照護提供者的資訊技術系統管理將病患連結至他們的本地檔案。研究人員則可透過資料消費者介面（右上方）設定帳號、搜尋資料集、請求存取資料，並為存取的資料付款。市場的後端管理將透過 DHDM 介面、EPR (電子病歷) 和 DLT (分散式總帳技術) 進行。

這將病人置於駕駛座上，並給予他們所有的控制權，以允許或拒絕存取其 EHR 的部分或全部內容。大多數的研究都嘗試賦予病人這樣的控制權，以獲得臨床和操作上的好處。然而，從資產管理的角度來看，同樣的建議模型也能讓資料控制獲益。Bahar 等人提供了一份特定的文獻回顧，涵蓋了此領域的大部分工作。在這份調查中，作者主要涵蓋並討論了數位身分記錄管理和 EHR 資料自我主權的工作 (8)。他們製作了一份使用 Ethereum 智慧契約實作的社群資料解決方案清單，並根據獎勵、資料市場、啟用 PHR、分散式資產追蹤、Web/行動應用程式、物聯網、EHR 兼容性/互通性，以及概念實作驗證，對這些解決方案進行比較。

如上文所述，Nguyen 提出了一個針對儲存在 InterPlanetary File System (IPFS) 配置中的 EHR 的安全存取控制模型 (9)。該模型提出了一個基於智慧契約的 EHR 管理員來管理存取和資料交易請求，同時為患者提供一個基於區塊鏈介面的行動應用程式，以行使他們控制存取的權利。儘管這個模型可能是解決電子病歷 (EHR) 分離化特性的迷人解決方案，同時也提供安全且可追蹤的資料存取控制及輸入稽核追蹤工具，但這個配置的所有實際測試都顯示在操作上有非常高的延遲。

在操作上有非常高的延遲。Rif 等人也使用相同的概念，使用區塊鏈來管理 EHR 中的跨動作(10)。作者處理了從個人醫療裝置和感應器取得的資料控制，並建議使用 DApp eHealth 區塊鏈來控制雲端或 IPFS EHR 資料庫的讀/寫。

Nortey 等人提供了另一個關於 EHR 隱私管理的區塊鏈框架提案範例，讓患者可以控制誰可以存取他們的 EHR。(11)作者引入了一個通道機制，確保患者授權分散式網路內的實體存取其資訊。其他作者則採用不同的方法，他們的目標是建立資料共用的同意模式 (12、13)。他們提出了一個交易工作流程，並基於 LUCE 創建了 Ethereum 智慧合約 (14)。用於監控資料 License accountability 和 ComplianceE 的區塊鏈解決方案，並在其基礎上建立了一個基於同意的架構模型，然後在 29 位參與者的 DINAMO 資料集上實作 (15)。此外，還提出了一種半去中心化的方法，因為每個委託的區塊鏈網路分佈在不同的機構 (13)。存取控制規則被編碼到分佈在區塊鏈網路的智慧契約中。Guo 等人提出了相同的路徑，但提出了混合區塊鏈-邊緣架構 (16)。

EHR 資料儲存在邊緣節點上，這些邊緣節點會強制實施以個人身為基礎的存取控制政策。作者使用 Hyperledger Composer Fabric 區塊鏈，以智慧型契約和存取控制清單政策編程，透過測量交易處理和回應未經授權重新擷取嘗試的時間來評估效能。實驗顯示，該系統可以毫秒為單位提供結果，因此適合納入即時且安全的 EHR 資料存取控制架構。最重要的結果是，在所有實驗中，不同大小的實作都顯示出一致性。此結果顯示此架構可能是 EHR 同意書管理中最具擴充能力的模型。

其他人也提供了基於屬性的區塊鏈標誌性模型，以實現患者資料的機密性、完整性和驗證，同時支援相關各方之間的資料共享 (17-20)。Seol 等人以從不同政策制定者的觀點來檢視模型的方式預備了他們的研究，並分兩個階段 (存取控制與數位簽章) 建立了他們的模型，允許智慧合約依次強制執行每項政策規則。

(20) Yang 等人 (21) 在 Wang 等人 (17) 所提出的基於屬性的模型上，建立了一個示範來確保效能，特別是加密和搜尋時間，並證明時間與屬性的數量無關。

Guang 等人提供了一個依賴於護理提供者來控制 EHR 交易的模型 (22)。此模型的有趣之處在於作者提出了一個架構，利用現有的 EHR 系統實作區塊鏈技術。考慮到 EHR 系統必須具備多重存取系統，且醫療服務提供者會根據其流程設計個別維護記錄，因此該模型賦予服務提供者主要責任，包括建立、驗證及附加新區塊。該設計使用智慧型契約，其中此架構獨立於任何特定的區塊鏈平台，其變化有可能適用於任何 EHR 系統。

#### 資料互通性

由於資料的異質性以及不同 EHR 系統缺乏標準化，資料互通性是健康資訊學的重要挑戰之一。

MedRec (23) 是許多區塊鏈研究用來安全地從分散式系統交換/傳輸資料到統一的病患 EHR 的基礎。MedRec 發表了一份工業白皮書，說明了一個開放源碼的區塊鏈模型，以處理 EHR 資料項目從醫療保健提供者系統到患者節點的安全傳輸，反之亦然。其目的是安全地收集在任何數目的本地病患檔案中建立的資料，並將這些資料彙集到一個整合的檔案中。

的病患檔案中建立的資料，並將這些資料匯集到一個由病人控制的整合檔案中。由於是開放原始碼，因此鼓勵許多研究人員在試驗實作中使用，同樣地也鼓勵產業試點採用他們的模型。此白皮書模型是極少數已實作的醫療照護區塊鏈模型之一。Yang 等人的工作是在 MedRec 框架 (24) 上進行學術建構的範例。

MedShare (25) 是早期提出使用區塊鏈的 EHR 資料交換控制模型之一。作者一開始提出一個處理層來管理現有醫療保健提供者雲端基礎架構之間的資訊交換。然而，模擬結果顯示延遲相對較高，且會隨著使用者數量的增加而增加。MedBlock (26) 是一個類似的模型。在此，作者建議使用非傳統的區塊鏈實體，例如驗證伺服器與憑證授權，來提供頒發身分和保護加密資料的方法，這些加密資料將用於加密區塊鏈上的所有資料。雖然 MedBloc 的設計是為了配合紐西蘭的醫療 IT 基礎建設，但研究人員並沒有發現其獨特之處會妨礙其在其他地方的實施。

Xiaoguang 等人 (27) 提出了 MedRec 模型的最新改編。這次的目的是提供並實作一個防篡改的醫療資料分享方案--以 Delegated Proof of State 機制作為輕量且可靠的共識機制。分析結果證實該方案令人滿意，且具有較低的計算和通訊成本。此方案除了是非付費方案外，與資料市場的研究範圍完全吻合。

Zhuang 等人 (28) 提供了另一個與 MedRec 模式不同的架構。儘管它的目標相同，都是達成以病患為中心的健康資訊交換，但此框架著重於賦予病患控制工具的權力。該架構隨後為病患建立了一個 DApp，病患可以透過給予權限、允許接觸點，以及透過連結與請求模組管理存取請求，來調整智慧契約中的參數。此架構為系統提供了實用的特質：為通訊、傳送/接收醫療記錄而設定的區塊鏈轉接器，並為使用者建立簡易互動的圖形化呈現；兩層安全層以確保只有授權的智慧型契約功能才能執行，並將資料外洩的風險降至最低；哈希 (hash) 以保證資料一致性；資料分割可讓部分資料共享；以及觸點選擇可讓醫師選擇專科的相關資料分割。

#### 資料安全

消除病患記錄的身分識別對於確保隱私及安全性至關重要。這需要在兩個

方面同時進行。一是將可識別的患者參數與臨床資料分離。必須在應用程式、通訊和儲存層進行分隔。另一個是在臨床資料本身。例如，根據設計，任何醫學數位影像與通訊 (DICOM) 影像都會包含可識別的資料，例如病患姓名、出生日期、轉診機構等。因此，在將資料放到不可變區塊鏈網路之前，必須先進行去識別和匿名化。

有幾個研究採用了將電子健康記錄存儲在區塊鏈中的模式 (29, 30)。由於技術和法律原因，隨著時間的推移，這種方法被打折了。在技術上，這是因為區塊的大小以及在多個節點複製的鏈中儲存大量資料的能力。在法律上，它幾乎不符合 GDPR 第 17 (6) 條關於被遺忘權的要求，因為一旦記錄被儲存在鏈上，就無法修改或刪除。其中一項採用 EHR on the chain approach 的研究是由 Tang 等人所做 (30)。當然，這與本研究無關。然而，作者提出了一個有趣的認證模型，透過為基於區塊鏈的 EHR 系統去簽署一個具有多個權限的基於身份的簽名方案。該方案提供了高效的簽名和驗證演算法。

大量出版物提出了大多被稱為雲端輔助區塊鏈 EHR 安全性的建議。Wang 等人 (31) 提出了一個基於聯合區塊鏈的雲端輔助安全與隱私保護 EHR 分享協定。換句話說，EHR 儲存在雲端，而 EHR 索引 (日誌保存) 則保存在區塊鏈上。在他們的工作中，作者提出了一個基於區塊鏈的 EHR 共享方案，該方案具有 conjunctive keyword searchable encryption 和 conditional proxy re-encryption，以實現不同醫療機構之間的資料共享的資料安全和隱私保護。

此外，Kim 等人 (32) 為使用區塊鏈的雲端輔助 EHR 系統提供了一個安全協定模型和模擬試驗。他們使用實際網路安全協定與應用程式的自動驗證 (AVISPA) 模擬，展示了所提出的方案對中間人 (MITM) 與重播攻擊的安全性。同樣地，Vora et al.

(33) 提出了一個使用區塊鏈來增強 EHR 資料庫安全性的模型。在此，作者利用 Ethereum 智慧合約來管理同意書、權限、分類和服務。該模型看起來很有前途，並建議了六種演算法來處理交易安全性與隱私權保護。不過，該模型顯示，要完全隱藏所有資訊並維持一個可存取且可互操作的系統是不可能的。

可存取和可互操作的系統。然而，透過使用智慧型契約來分隔資訊，所提出的模型仍能提供顯著的隱私保護與資料完整性。此外，透過智慧契約，人們可以決定資訊存取等級，但在公開區塊鏈中，與智慧契約的整合具有挑戰性且不切實際。

雖然是匈牙利的研究，Magyar et al.

(34) 提出了一個以區塊鏈簽章為基礎的模型，採用美國健康保險可攜性與責任法案 (HIPAA) 法規。該模型使用智慧契約與密碼學產業的創新技術、盲簽署、多重簽章、層級簽署以及其他可確保資訊存取的安全程序。同時，在路線圖上，任何人都無法讀取任何開放文字資料。

上述研究將 EHR 視為單一資料庫 (本地或雲端儲存)，並討論了使用區塊鏈安全新增、刪除及修改 EHR 中條目的不同方法。然而，區塊鏈被認為提高 EHR 及其相關交易穩健性的潛在技術的主要原因之一，是 EHR 本質上是去中心化的。一個典型的病人會在一級、二級和三級護理中擁有不同的 EHR。在病人的一生中，僅這三個層級就會產生數以萬計的記錄，需要將這些記錄結合起來，形成一個完整的病人電子健康記錄。

相比之下，Ayesha 等人 (35) 討論了另一種架構，同樣挑戰了雲端 EHR 儲存的原則。作者提出了一個架構，該架構提出了一些措施，以確保系統在利用 IPFS 的離鏈儲存機制時，能夠解決資料儲存的問題。他們的論文評估了不同拓撲架構在執行時間、吞吐量和延遲上的效能。他們提出一個結合安全記錄儲存與 EHR 區塊鏈存取規則的架構。

Nguyen 等人 (9) 所提出的另一個模型則是針對 EHR 的安全存取控制，同時也提出了一種用於 EHR 儲存的 InterPlanetary File System (IPFS) 配置。其構想是在每個護理提供者形成一個 IPFS 節點，並建立一個 EHR 管理員 (伺服器)，該管理員將扮演最初由雲端 EHR 扮演的角色。然後，該模型使用區塊鏈來索引交易軌跡，並將 EHR 管理員視為雲端服務來處理。在內部，EHR 管理員負責根據要求從所有 IPFS 節點彙集患者記錄，並在患者在不同護理提供者之間移動時創建更多節點。該模型建議 EHR 管理員本身應基於智慧契約來管理存取和資料交易請求，同時為病患提供區塊鏈介面的行動應用程式，以行使其控制存取的權利。

## 法律和道德挑戰

法律爭論的起點總是誰擁有資料？所有權通常與存取權相混淆。Kostkova 等人 (7) 旨在區分資料所有權與存取權，並尋找平衡的新方法，以滿足商業利益並積極鼓勵大眾參與，同時確保資料存取的透明性，以滿足研究需求和大規模整合的需要，並保護個人隱私。Castillo 等人(36)的研究在經濟與臨床醫療健康資訊科技(HITECH)法案(The Health Information Technology for Economic and Clinical Health Act)的背景下，找出資訊交換的障礙，以創造更有效率與效益的醫療照護系統。研究結果顯示，當醫院與醫療系統以外的醫院使用相同的 EHR 供應商，則該醫院更有可能與其他醫院交換臨床摘要。作者強調 EHR 供應商中立性的重要性，以及因此 EHR 系統互通性的重要性不言而喻。

在 Yadav 等人 (37) 有關從病患 EHR 擷取臨床資料的嚴謹調查中，作者探索、討論並提出有關 EHR 如何運用資料擷取技術的新觀點。在這篇系統性回顧中，他們討論了大量臨床資料挖掘計畫的應用、研究設計和資料挖掘方法。此外，作者還討論了在臨床實踐中廣泛使用資料挖掘的障礙。評論本身並不涵蓋 DHDM 的法律與法規需求。然而，它處理了通過 DHDM 促進的資料挖掘研究（人工智能、ML 等）的倫理和合規性。

Mello Michelle 在北美法律的背景下，針對健康資料交換成長的障礙提出了一份全面的手冊 (38)。作者分析了聯邦和各州的健康資訊隱私權法令和規範以及次要資料，然後認為一些關鍵的法律障礙仍然存在，但許多醫療照護提供者承認為障礙的問題在某種程度上是虛幻的。作者強調，醫療保健提供者認為健康資訊隱私權法律妨礙電子健康資料交換的發展，並歸咎於幾個因素，例如病患同意法律的不一致、敏感健康資料的特殊處理，以及未能建立統一的病患索引系統。

一份技術規範文件比較了健康資料傳輸標準 (ISO/IEEE 11073、IHE PCD-01 和 HL7 DoF) 的差異，並建議最適合使用各標準的環境 (39)。作者的結論是，ISO/IEEE 11073 訊息無法包含病患資訊，IHE PCD-01 訊息只有有限的裝置資訊，而 HL7 DoF 在研究的所有四個參數 (人類可讀性、可學習性、實施性和可擴展性) 中擁有最全面的資訊涵蓋範圍。

## 社會經濟挑戰

Joseph Schumpeter 提出的「創造性破壞」一詞解釋了產業轉型過程如何透過破壞現有的經濟結構，同時創造新的經濟結構，從內部徹底改變經濟結構 (40)。對於像區塊鏈這樣的破壞性技術，以及像醫療保健這樣的產業，在利害關係人的參與和經濟動力方面，結構是非常複雜的。

儘管並非醫療行業，但一項研究提出的模型 (41) 以日本商用車資料市場的現有模式為基礎，提供了一個很有前景的市場實作。ID-Link 是日本政府發起建置資訊基礎架構以分享不同商業領域資料的成功模式。其中一個領域是個人 EHR 的資料分享。在他們的論文中，作者以 EHR 的醫療資料取代車速、時間、距離、排放量等汽車資料。該研究討論了參與選項 (Opt-In vs. Opt-Out)、存取控制權限和資料標準化，特別是採用特定格式，例如 HL7 (論文建議使用 V2.5。然而，FHIR HL7-V3.0 目前已在全球廣泛使用)、WHO ICD-10 和 SNOMED-CT 作為臨床術語庫。本論文也提供一個醫療適應化的 Automotive ID-Link 流程工作流程，將其轉換成可行的七個步驟模型，從病人同意、醫生互動、身份檢查、商業使用、付款和利潤分享。ID-Link 分為商業層、功能層、資料層及技術層四個架構層。

Guo 等人 (42) 批評數位醫療創新者為了得出解決方案和實施結果所遵循的流程。作者也強調數位健康解決方案缺乏實作，因此不容易得出任何實證性的再結果。本研究分析了一些主要的數位健康解決方案實作，並選擇非獨家的相關法規標準，以及創新者在評估其解決方案時所採用的方法。儘管如此，作者承認創新者並未製造障礙，創新者在數位健康領域陷入「無證據、無實施-無實施、無證據」的悖論。作者建議，模擬研究等方法可以產生品質更高、成本更低、更及時的證據。

Affinito 等人的調查 (43) 則是要了解醫師使用何種數位方式與病患互動，以及醫師認為數位方式對臨床健康結果的影響。調查結果顯示，利用數位工具實現病患授權及改善健康結果的主要成功因素為臨床證據及實際使用者 (病患及照護者) 參與設計數位解決方案。研究

結論是，使用數位工具確實能提高病患的能力。儘管如此，到目前為止，仍沒有證據顯示健康成果有所改善。

Angeline 和 Sharon (44) 進行了一項研究，探討醫療照護人員的數位素養水平是否應該受到責備。這項研究顯示，大多數員工對於使用 ICT 都表現出信心。不過，據了解，研究地點（澳洲）可能影響了研究結果，我們應該預期其他地區的其他結果。臨床研究的電子健康記錄 EH-R4CR 是歐洲的一個專案，目的是透過開發一個可存取現有病患電子健康記錄 (EHR) 的平台，來加強以病患為中心的試驗 (45)，使得該專案與 DHDM 研究專案有許多相似之處。除了它不處理病人使用其 EHR 資料的補償問題。Dupont et al. (46) 是一項評估計劃財務結果的研究。該研究將 EHR4CR 與現有做法比較，得出的結論是 EHR4CR 解決方案似乎可為臨床試驗的主要贊助者節省成本。研究結果顯示，隨著 EHR4CR 解決方案在歐洲及其他地區的廣泛採用，節省成本的潛力將會增加。研究結果反過來也顯示，若能建立一個醫療資料市場，讓病人可以為了自己的利益而出售其 EHR 記錄的存取權，長遠而言將可節省醫療成本。工業與臨床試驗。

在一篇論文中，Timo 和 Harri (47) 旨在開發一個生態系統評估框架 (EEF)，以瞭解數位商業平台的生存機會。作者將 EEF 模型描述為六個參數（平台、平台試圖減少的问题、平台的目的、生態系統、平台促成的交易以及平台的收入模式）。作者強調了考慮補償模式的重要性，這與我們的研究目標完全吻合。他們指出，在芬蘭的 Pirkanmaa 地區，錯誤的獎勵成份是區域健康資訊系統 RHIS 未能達到臨界值的主要原因。

Alina 和 Jose Luis (48) 討論了作者所謂的 FAIR 市場。他們指出資料的屬性為可尋找、可存取、可互用及可重用，這就是 FAIR 的由來。這兩位作者提出了一個架構，可容納各層次以收集來自病患、照護提供者和其他平台（例如 EHR4CR）的資訊。

信用評分一直是 DHDM 研究的最大限制。幾乎在所有的調查、投票，甚至是友好的聊天中，這個問題都被提出來。人們不禁要問，這個專案是否會像信用評分一樣，讓他們的財務狀況曝光。

信用評分一樣暴露他們的財務狀況。人們總是很擔心在沒有顯著暴露健康記錄的情況下獲得的服務會被拒絕或支付更多費用，例如續保汽車保險。他們擔心一旦保險公司知道他們健康的更多詳細資料，保費就會提高，或者更糟的是，如果他們不允許存取自己的記錄，就會像信用分數一樣被拒絕提供服務。

然而，從技術商業的角度來看，信用評分架構是資料彙集與許可分享的最佳範例。Dumitru 和 Gatti (49) 討論了與共用健康資料以及將資料用於信用評分目的的相關的限制和機會。作者提出了一個可信資料市場的架構，可以非常有用地在 DHDM 專案中作為稱重系統。稱重系統可計算每個 EHR 對整個資料集的貢獻。它將被用來在數據擁有者之間公平地分配來自醫學研究者的付款，以獎勵 EHR 基於他們對福祉的承諾和他們對保持 EHR 最新的承諾。

Roman 和 Stefano (50) 進行的一項研究是利用成功的信用評分模式計算每項電子健康記錄的權重/價值的實例。根據每個項目和每個 EHR 在研究中的貢獻，在 EHR 擁有者之間公平分配財富的過程中，權重部分具有巨大的價值。

Ryuji 的研究(41) 是另一個實例，可使 DHDM 研究計畫受惠。它提供了一個可行的商業資金交換模式，利用汽車產業中已實施的技術來交換資料。

## 結論

儘管已耗資數十億美元讓目前的健康資料管理系統更有效率，但資料分享仍是健康領域難以達成的目標。由於 GDPR 引進了資料擁有者和控制的範式轉變，以及類似區塊鏈的技術，提供了分散式資料管理的技術能力；現在是透過類似 DHDM 的開放市場模式來改變不穩定的激勵模式的適當時機。

基於以上觀點，MedRec(23)等以區塊鏈為基礎的解決方案，顯然可以透過應用程式介面(API)，以獨立層的方式與原生資料庫整合，而不會影響原生資料管理系統與文化，這對技術適應過程絕對有利。此外，由於 MedRec 是開放源碼，類似解決方案將在從現有資料管理系統安全收集資料方面扮演重要角色，並可將現有資料管理系統與 MedRec 相結合。

在患者控制下的彙總 EHR。智慧型契約與 IPFS/ 雲端儲存系統可讓病患控制不同類型與時間長度的去辨識化資料，並安全地授予存取權。本檢討展示了不同的資料存取建議，以及資料製造者與消費者之間的安全共用。然而，還需要進一步研究數位資料的複製，以及如果消費者在未經同意的情況下複製資料，如何確保資料製造者的權利。此外，也需要進一步的研究，以確定如何在不同的地理管轄區和時間，以不同的法規來調整資料分享程序。

被認為最適合 DHDM 情境的共享經濟型激勵模式也需要廣泛評估。雖然像 Airbnb 這樣的公司對提供者和消費者都有顯著的經濟利益，但分享個人健康資料可能與個人住宿有不同的社會和情感背景。儘管有這些疑慮，但幾乎可以肯定的是，開放市場將引進生產競爭，並促進根據消費者需求分享高品質資料。反過來，這將有助於研究人員和醫療從業人員根據他們的需求隨時存取資料。

### 經費聲明

本文創作過程中未提供任何經費。

### 財務及非財務關係與活動

作者聲明沒有潛在的利益衝突。

### 作者貢獻

文章的兩位作者都對本工作做出了重大貢獻。Mohamed Maher 構思了模型、進行了文獻回顧並撰寫了文章。Imtiaz Khan 協助設計、撰寫並排版文章。

### 參考文獻

1. Heather B. Google DeepMind 與皇家免費醫院簽訂五年合約。Digitalhealth; 2016.Available from: <https://www.digitalhealth.net/2016/11/google-deepmind-and-royal-free-in-five-year-deal/> [cited 19 September 2021].
2. Kowelle J. NHS 數據價值數十億，但誰該存取？衛報》。2019.Available from: <https://www.theguardian.com/society/2019/jun/10/nhs-data-google-alpha-bet-tech-> [cited 19 September 2021].
3. PatientsLikeMe. patientslikeme.com. 2021.
4. Jeana HF, Michael PM.網上病人社區 PatientsLikeMe 內個人健康資訊的社交使用：當病人可以存取彼此的資料時會發生什麼事。2008; 10(3):e15. Doi: 10.2196/jmir.1053
5. Paul W, Michael M, Jeana F, et al.J Med Internet Res. 2010;12(2):e19. Doi: 10.2196/jmir.1549
6. GDPR.一般資料保護規範。Intersoft Consult-ing.2016.Available at: <https://gdpr-info.eu> [cited 19 September 2021].
7. Kostkova P, Brewer H, de Lusignan S, et al. Who owns the data?醫療保健的開放資料。前沿公共衛生。2016;4:7. doi: 10.3389/fpubh.2016.00007
8. Bahar H, Abdelhakim Senhaji H, Dimitrios M. A sur-vey on blockchain-based self-sovereign patient identity in healthcare.IEEE Access.DOI: 10.1109/ access.2020.2994090
9. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Block-chain for secure EHRs sharing of mobile cloud based e-health systems.IEEE Access.DOI: 10.1109/ ACCESS.2019.2917555
10. Rifi N, Rachkidi E, Agoulmine N, Taher NC.邁向使用區塊鏈技術進行電子健康資料存取管理。IEEE; 2017, p. 1-4.
11. Nortey RN, Yue L, Agdedanu PR, Adjeisah M, editors.使用區塊鏈的分散式電子健康記錄 (EHR) 隱私模組。2019 IEEE 第四屆大數據分析國際會議 (ICBDA), 2019 年 3 月 15-18 日。
12. Jaiman V, Urovi V. A consent model for blockchain-based health data sharing platforms.IEEE Access 2020;8:143734-45. DOI: 10.1109/ACCESS.2020.3014565
13. Ryno A, Bertram H. A permissioned blockchain approach to the authorization process in electronic health records.2019 國際多學科資訊科技與工程會議 (IMITEC)。2020.
14. Havelange A, Dumontier M, Wouters B, et al. LUCE: A blockchain solution for monitoring data License accoUnt-ability and Compliance.2019.網址: <https://arxiv.org/abs/1908.02287> [於 2021 年 9 月 19 日引用]。
15. Fabien D, Jean-Eudes R, Stefano B, Jean-Paul C, Juan R, Mi-chael S. The open D1NAMO dataset: 非侵入性 1 型糖尿病管理研究的多模式資料集。Informat Med Unlocked.2018;13:92-100. DOI: 10.1016/j.imu.2018.09.003
16. Guo H, Li W, Nejad M, Shen C, editors.使用混合區塊鏈-邊緣架構的電子健康記錄存取控制。2019 IEEE 區塊鏈國際會議 (Block-chain), 2019 年 7 月 14-17 日。
17. Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain.J Med Syst.2018;42(8):1-9. DOI: 10.1007/s10916-018-0994-6
18. Guo R, Shi H, Zhao Q, Zheng D. Secure attribute-based signature scheme with multiple authorities for blockchain in elec-tronic health records systems.IEEE Access.2018;6:11676-86. DOI: 10.1109/ACCESS.2018.2801266
19. Sun Y, Zhang R, Wang X, Gao K, Liu L, 編輯。醫療保健區塊鏈的去中心化屬性簽章。2018 第 27 屆電腦通訊與網路國際會議 (ICCCN), 2018 年 7 月 30 日至 8 月 2 日。
20. Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K.基於 XML 的電子健康記錄系統的隱私保護屬性存取控制模型。IEEE Access.2018;6(99):9114-28. DOI: 10.1109/ACCESS.2018.2800288
21. Yang X, Li T, Rui L, et al. Blockchain-based secure and search-able ehr sharing scheme.2019 第四屆機械、控制與電腦工程國際會議 (ICMCCE), 2019 年 10 月 24-26 日。
22. Guang Y, Chunlei L.基於區塊鏈的電子健康記錄 (EHR) 系統安全架構設計。2018 IEEE 國際雲端運算技術與科學會議 (CloudCom)。2018.

23. Azaria A, Ekblaw A, Vieira T, Lippman A, editors. MedRec: 使用區塊鏈進行醫療資料存取與許可管理。2016 第二屆開放與大數據國際會議 (OBD), 2016 年 8 月 22-24 日。
24. Yang H, Yang B, editors. 基於區塊鏈的醫療資料安全共享方法。Norwegian Information Security Conference 論文集; 2017 年。
25. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeD-Share: 透過區塊鏈在雲服務供應商之間共享無信任的醫療資料。IEEE Access.2017;5:14757-67. DOI: 10.1109/ACCESS.2017.2730843
26. Huang J, Qi YW, Asghar MR, Meads A, Tu Y, 編輯。Med-Bloc: 用於分享和存取醫療資料的基於區塊鏈的安全 EHR 系統。2019 第 18 屆 IEEE 計算與通訊信任、安全與隱私國際會議/第 13 屆 IEEE 大數據科學與工程國際會議 (TrustCom/BigDataSE); 2019 年 8 月 5-8 日。
27. Xiaoguang L, Ziqing W, Chunhua J, Fagen L, Gaoping L. 基於區塊鏈的醫療資料共享和保護方案。IEEE Access. DOI: 10.1109/access.2019.2937685
28. 莊 Y, Sheets LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR. 使用區塊鏈技術的以患者為中心的健康資訊交換框架。IEEE J Biomed Health Informat 2020;24(8):2169-76. doi: 10.1109/JBHI.2020.2993072
29. Xu L, Bagula A, Isafiade O, Ma K, Chiwewe T, editors. 可信區塊鏈基於電子健康記錄 (CB-EHRS) 平台的設計。2019 ITU Kaleidoscope: ICT for Health: 網路、標準與創新 (ITU K), 2019 年 12 月 4-6 日。
30. Tang F, Ma S, Xiang Y, Lin C. An efficient authentication scheme for blockchain-based electronic health records. IEEE Access.2019;7:41678-89. DOI: 10.1109/ACCESS.2019.2904300
31. Wang Y, Zhang A, Zhang P, Wang H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access. DOI: 10.1109/ACCESS.2019.2943153
32. Kim M, Yu S, Lee J, Park Y, Park Y. 使用區塊鏈為雲端輔助電子健康記錄系統設計安全的 protocol。Sensors (Basel, Switzerland) 2020;20(10):2913. Doi: 10.3390/s20102913
33. Vora J, Nayyar A, Tanwar S 等人, 編輯。BHEEM: A block-chain-based framework for securing electronic health records. 2018 IEEE Globecom Workshops (GC Wkshps); 9-13 December 2018.
34. Magyar G, 編輯。區塊鏈: 解決 EHR 資料隱私權與再研究可用性的取捨問題: 健康資料管理的新顛覆性技術。2017 IEEE 第 30 屆 Neumann Colloquium (NC); 2017 年 11 月 24-25 日。DOI: 10.1109/NC.2017.8263269
35. Ayesha S, Usman Q, Ayesha K. Using blockchain for electronic health records. IEEE Access.2019;7:147782-95. DOI: 10.1109/access.2019.2946373
36. Castillo AF, Sirbu M, Davis AL. 選擇供應商與促進健康資訊交換政策的成效。BMC Health Serv Res 2018;18(1):405-12. Doi: 10.1186/s12913-018-3230-7
37. Yadav P. Mining electronic health records (EHRs): A survey. ACM Comput Surv.2017;50(6):1-41. Doi: 10.1145/3127881
38. Michellem M. 健康資訊交換成長的法律障礙-巨石還是卵石? Milbank Q 2018;96(1):110-44. Doi: 10.1111/1468-0009.12313
39. Lee S, Do H. Comparison and Analysis of ISO/IEEE 11073, IHE PCD-01, and HL7 FHIR messages for personal health devices. Health Inform Res. 2018;24(1):46-52. Doi: 10.4258/hir.2018.24.1.46
40. Schumpeter JA, Stiglitz JE. Capitalism, socialism and democracy. Florence, SC: Taylor & Francis Group; 2010.
41. Ryuji I. ID-link, an enabler for medical data marketplace. IEEE. 2016. doi: 10.1109/ICDMW.2016.0117
42. Guo C, Ashrafian H, Ghafur S, Fontana G, Gardner C, Prime M. 數位健康解決方案評估的挑戰--呼籲創新的證據生成方法。NPJ Digit Med. DOI: 10.1038/s41746-020-00314-2
43. Affinito L, Fontanella A, Montano N, Brucato A. Physicians 如何利用數位工具賦予病患權力。J Public Health. 2020;1-13. doi: 10.1007/s10389-020-01370-4
44. Kuek A, Hakkennes S. 醫護人員的數位素養水平及其對資訊系統的態度。健康資訊學 Doi: 10.1177/1460458219839613.
45. EHR4CR | 用於臨床再研究的電子健康記錄系統。創新藥物計畫。2016. 網址: <https://www.imi.europa.eu/projects-results/project-factsheets/ehr4cr> [於 2021 年 9 月 19 日引用]。
46. Dupont D, Beresniak A, Schmidt A, Proeve J, Bolanos E. Assessing the financial impact of reusing electronic health records data for clinical research: EHR4CR 歐洲專案的結果。J Health Med Informat. 2016;7(3):235. DOI: 10.4172/2157-7420.1000235
47. Timo I, Harri T. Difficult business models of digital business platforms for health data: 生態系統可行性評估框架 2017 IEEE 19th Conference on Business Informatics (CBI); 2017. doi: 10.1109/cbi.2017.6
48. Alina T, Jose Luis O. A FAIR marketplace for biomedical data custodians and clinical researchers. 2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS); 2018. doi: 10.1109/cbms.2018.00040
49. Dumitru R, Gatti S. 邁向可信資料市場的參考架構: 信用評分的角度。2016 第二屆開放與大數據國際研討會 (OBD)。2016. DOI: 10.1109/OBD.2016.21
50. Roman D, Stefano G, editors. 邁向可信資料市場的參考架構: 信用評分的觀點。2016 第二屆開放與大數據國際會議 (OBD); 2016 年 8 月 22-24 日。DOI: 10.1109/OBD.2016.21

**版權所有:** 這是一篇依據 Creative Commons Attribution Non Commercial (CC BY-NC 4.0) 許可證發佈的開放存取文章, 該許可證允許他人發佈、改編、非商業性地增強本作品, 並以不同條款許可其衍生作品, 但前提是必須適當引用原作, 且使用屬於非商業性。請參閱: <http://creativecommons.org/licenses/by-nc/4.0>。