



臺灣社交距離App

疾病管制署 X 台灣人工智慧實驗室



衛生福利部疾病管制署

Taiwan Centers for Disease Control



AI Labs.tw

台灣人工智慧實驗室

衛生福利部疾病管制署

- 上班時間(周一~周五)：02-23959825 分機 3044
- 非上班時間(六、日或國定假日)：02-23510982



App背景介紹 (1/3)

- 「**臺灣社交距離App**」是由台灣人工智慧實驗室開發，並與行政院及疾病管制署合作的防疫App。
- 此App以**保護隱私且尊重使用者意願**為最高原則。由使用者**自主下載及隨時刪除**，程式中相關接觸編碼資料僅**儲存於手持裝置14天**。
- 運用先進技術**無須註冊任何個人資料**，不會有任何個人資料被上傳，且政府和程式開發商均無資料庫儲存個人資料。



App背景介紹 (2/3)

告警啟動：

- 此App會定期自動呼叫CDC確診資料庫取得程式編碼值。
- 若確診者同意分享本身之程式編碼值，且App用戶符合程式設定之接觸者定義（2公尺+2分鐘），則該用戶於呼叫CDC資料庫後出現告警畫面。
- 用戶可利用此告警得知自己為確診個案之可能接觸者，自主向衛生單位通報。



App背景介紹 (3/3)

限制：

- 用戶人數需達一定量 ($\geq 50\%$) 使具效益。
- 因自主性高，無法確保用戶隨時攜帶手機、同意分享本身確診之程式編碼值、或刻意忽略告警。



App設計脈絡



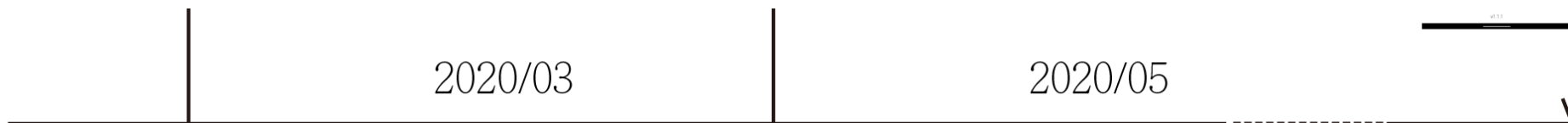
行政院
Executive Yuan



衛生福利部疾病管制署
Taiwan Centers for Disease Control



AI Labs.tw
台灣人工智慧實驗室



2020/02

2020/03

2020/04

2020/05

2021/04



Google

Apple | Google



App設計要點

- ✔ 保障個人隱私
- ✔ 減少經濟衝擊
- ✔ 透過減少互動數量，降低暴露風險
- ✔ 降低傳染風險
- ✔ 在自願的基礎上使用
- ✔ 拯救生命



歐盟GDPR適足性

GDPR (General Data Protection Regulation, 一般資料保護規範)

Taiwan AI Labs

相關APP之開發應進行資料保護影響評估，並建議公開原始程式碼 (source code)，以利公眾瞭解其運作機制。

公開原始碼，且開放各國政府使用。

相關APP不應追蹤、蒐集個別使用者之定位資訊，因其功能係在於發現與確診者接觸之事件。

無須註冊，且無定位功能。

相關APP所蒐集資料之儲存方式可採集中式 (centralised) 或分散式 (decentralised) (即資料儲存於各用戶手持裝置) 等方式，惟皆應確保適當安全維護措施避免資料外洩，EDPB則建議分散式之資料儲存方式較符合資料最小蒐集原則。

資料採分散式儲存於各使用者手持裝置。

當事人雖係自願下載相關APP，惟因各會員國係基於公共利益之執行法定職務，而為相關個人資料之處理，爰應以執行法定職務為其資料處理之合法要件，而非當事人同意，惟基於尊重當事人權益，相關個資係以當事人自願提供之方式為之，不應給予不願使用相關APP之當事人任何不利影響。

所有操作完全尊重使用者意願。

應確保相關APP發出之確診者資訊之正確性。

與國家疾管單位合作，確保正確性。

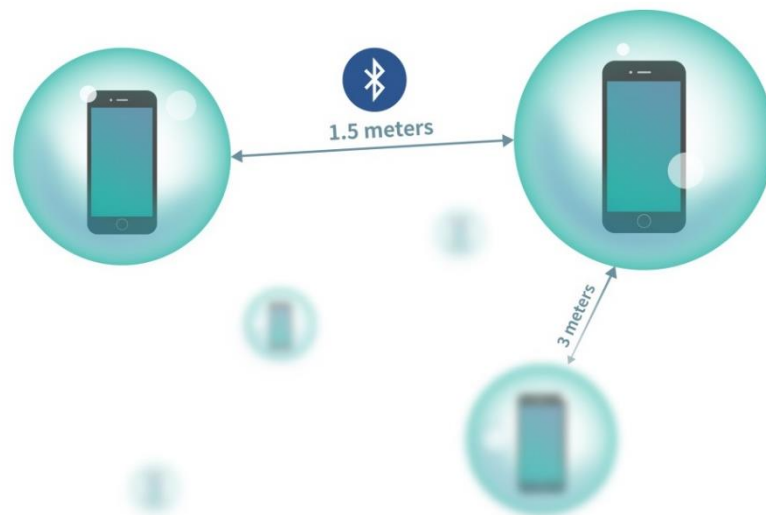
有關APP提供之衛教指示應避免以自動化決策方式，而仍應具有「呼叫機制 (call-back mechanism)」，如提供專線或連結專人提供詢問與建議。

無任何自動化決策機制。



架構設計

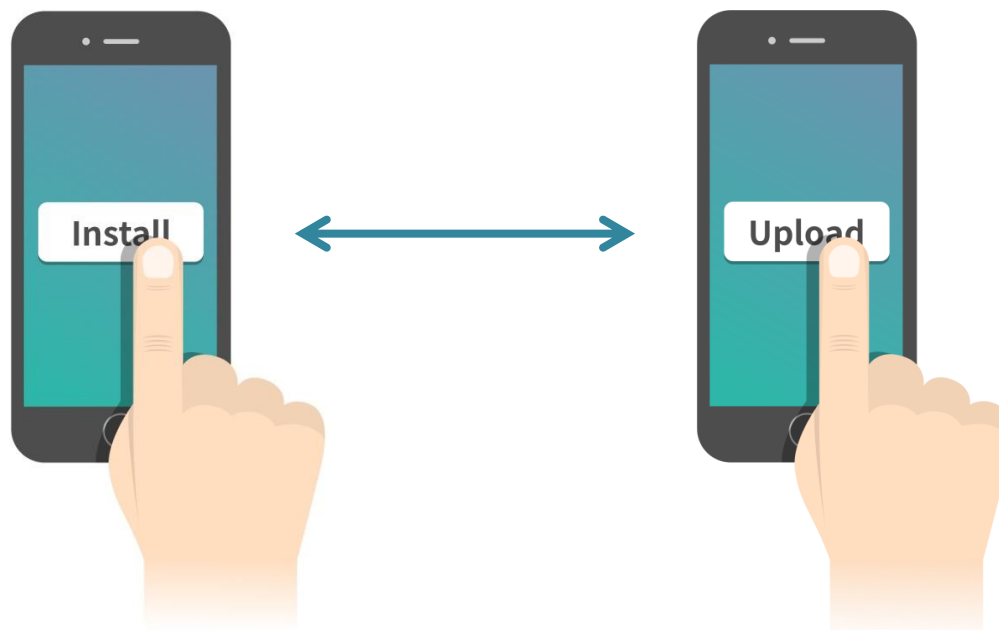
- 去中心化的設計讓使用者無須註冊也無須上傳資料，減少個資蒐集疑慮。
- 利用App本身每10-20分鐘產生一個雜湊值（Hashed ID/**隨機 ID**），在用戶互相接觸時，雙方的手持裝置會透過**藍牙偵測**身旁裝置的隨機 ID，同時**紀錄接觸的時間長度與距離**。
- 分散儲存在個別用戶的手持裝置中，只**儲存14天內的資訊**。





使用者優先

- 除一般使用者可自行選擇是否下載，若有使用者**確診**，可透過醫生或疾管署人員主動詢問，是否願意**上傳**過去手持裝置所生成的**隨機 ID** 資訊。
- 使用者能掌握自己想分享的資訊，且上傳的資料，會由疾管署來維護，**10天後將自動從伺服器中刪除**。





每日更新

- 透過App每4小時的自動更新，App將會自動查看是否有資料上傳，並下載於手持裝置端自行比對接觸史。
- 曾經與確診者在2公尺內，接觸長達2分鐘以上的用戶，系統會提醒他注意最近的身體狀況。
- 用戶收到提醒後，就能主動與防疫人員聯繫。



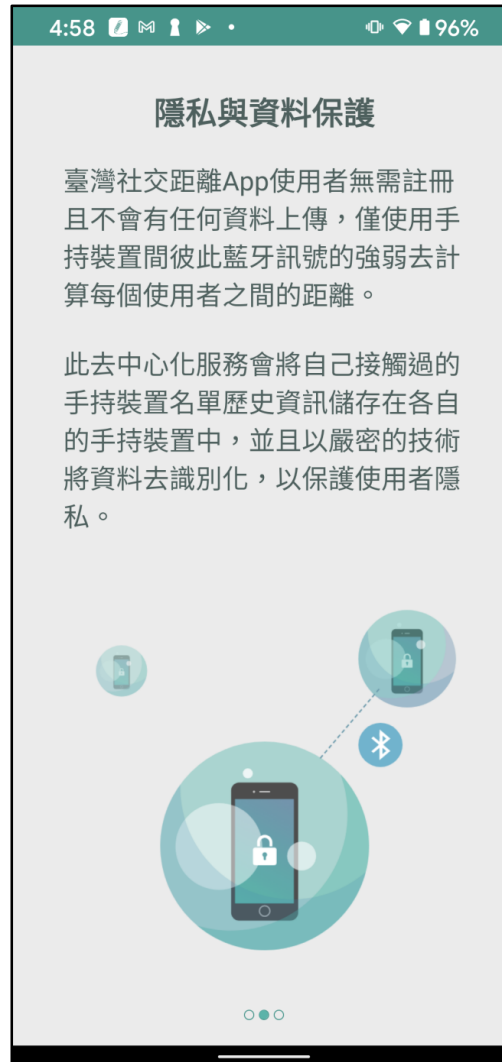


App起始畫面



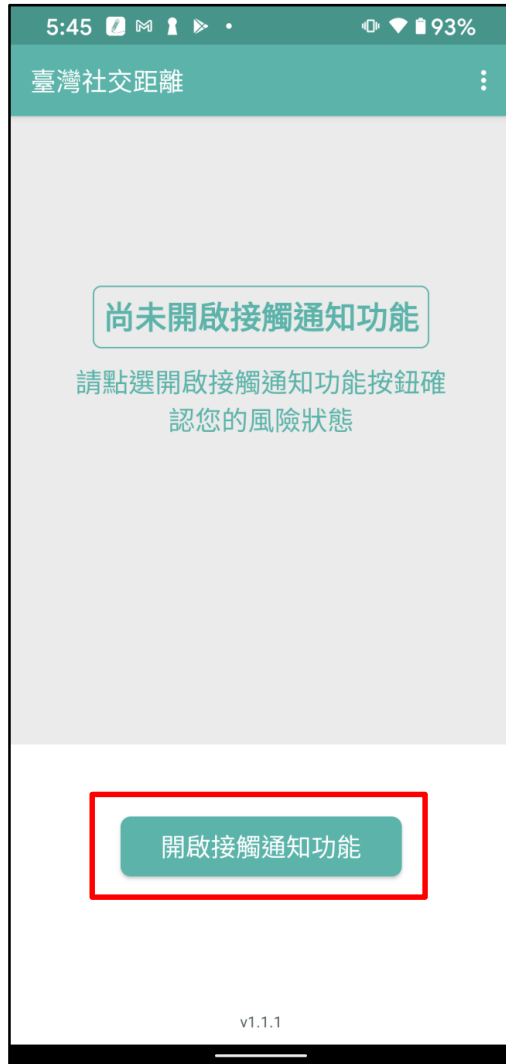


App說明畫面

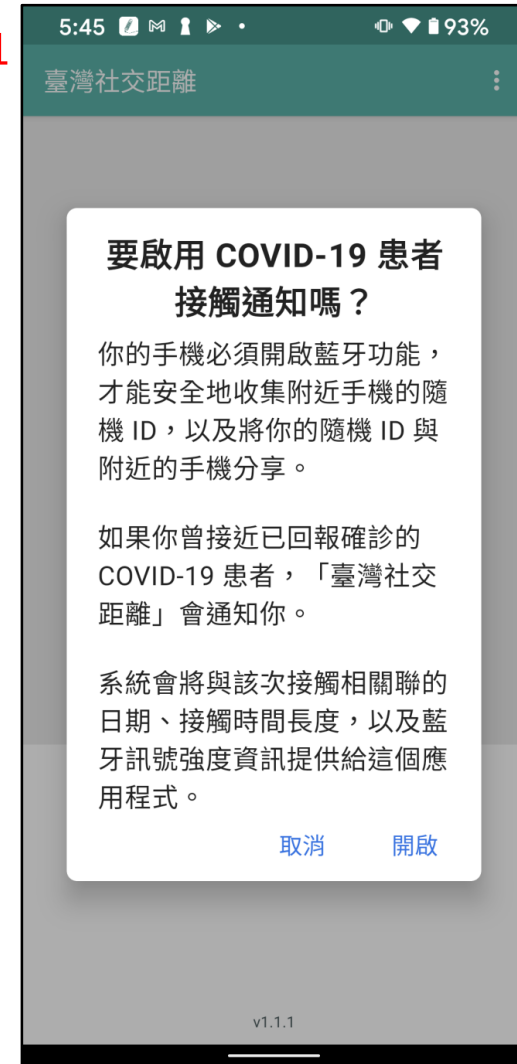




App畫面-啟用接觸通知功能



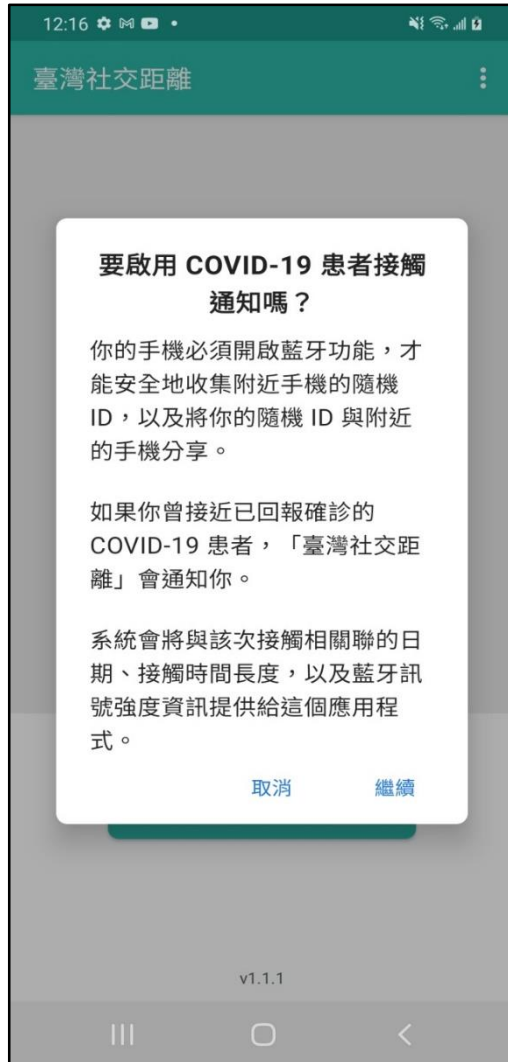
Android 11
以上畫面



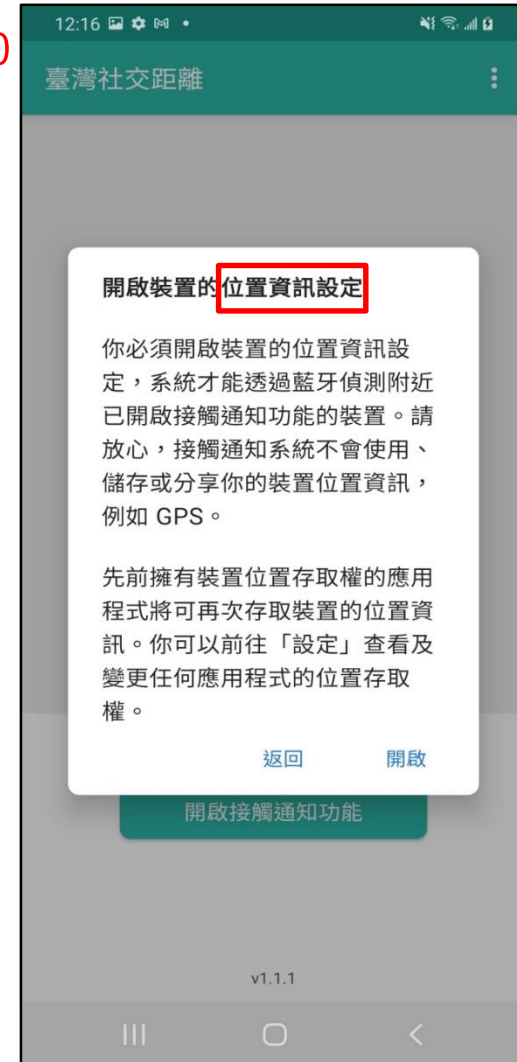


App畫面-啟用接觸通知功能

Android 10
以下畫面



Android 10
以下畫面





Google-位置資訊設定說明

2021/3/31

關於接觸通知系統和 Android 位置資訊設定 - Android說明

關於接觸通知系統和 Android 位置資訊設定

在 Android 10 以下版本中，[接觸通知系統](#)會使用手機的位置資訊設定和藍牙功能。你可以透過多種方式管理使用該系統期間的隱私權。

在 Android 11 中，手機不必開啟位置資訊設定，接觸通知系統即可正常運作。[瞭解如何查看及更新 Android 版本](#)。

接觸通知系統不會使用你的位置資料

我們不允許使用接觸通知系統的應用程式要求存取裝置的位置資訊。

為何手機必須開啟位置資訊設定

接觸通知技術會使用裝置的藍牙掃描功能偵測附近的裝置。在搭載 Android 6.0 到 10 版本的手機上，接觸通知系統會使用藍牙掃描功能。如果你只為內建接觸通知系統的應用程式開啟[位置資訊設定](#)，藍牙掃描功能將無法正常運作，因此請務必替裝置上的所有應用程式開啟這項設定。

Google 和 Apple 都在手機中內建了相關保護措施，可確保政府使用 ENS 製作的患者接觸追蹤應用程式無法推測你的所在位置。系統會定時變更指派給裝置的隨機 ID，防止開啟這項功能的裝置遭人追蹤。請放心，隨機 ID 中不含任何位置資訊，因此裝置透過系統交換隨機 ID 時，你的位置資訊不會因此外洩。

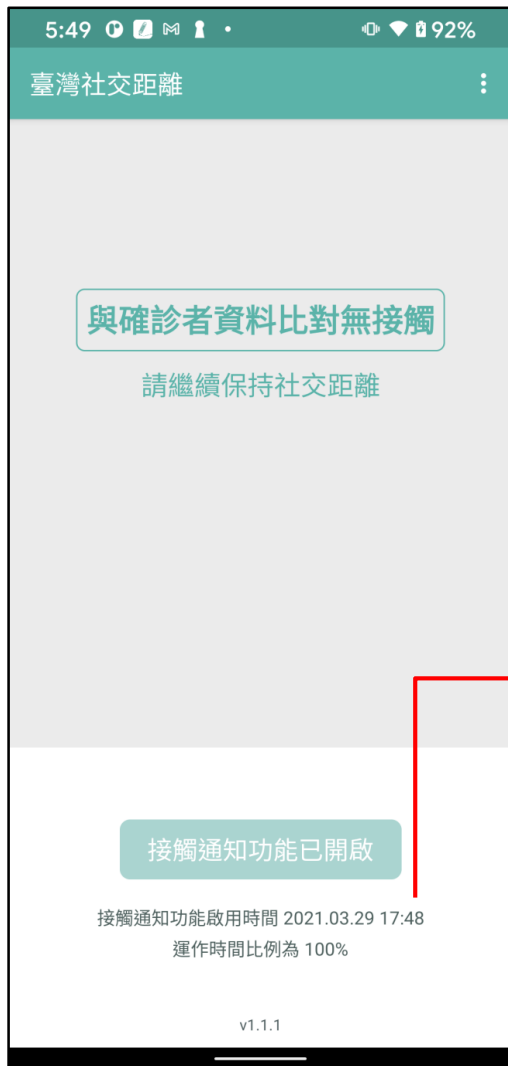
控管位置資料的使用方式

接觸通知系統不會使用裝置的位置資訊，我們也禁止使用 ENS 的公共衛生主管機關應用程式要求存取裝置位置資訊。

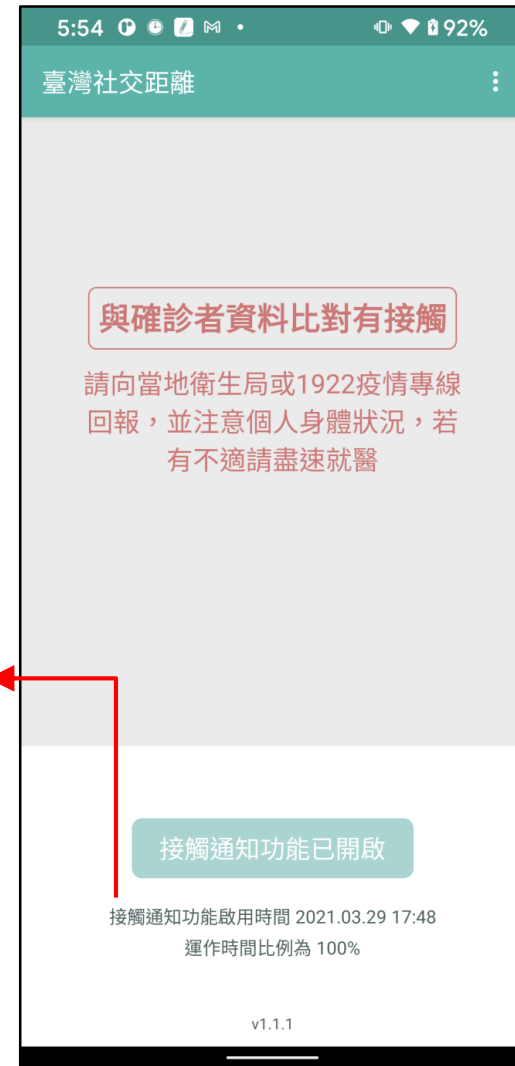
<https://support.google.com/android/answer/9930236>



App畫面-比對無/有接觸畫面



安裝App並啟用
接觸通知功能時起算





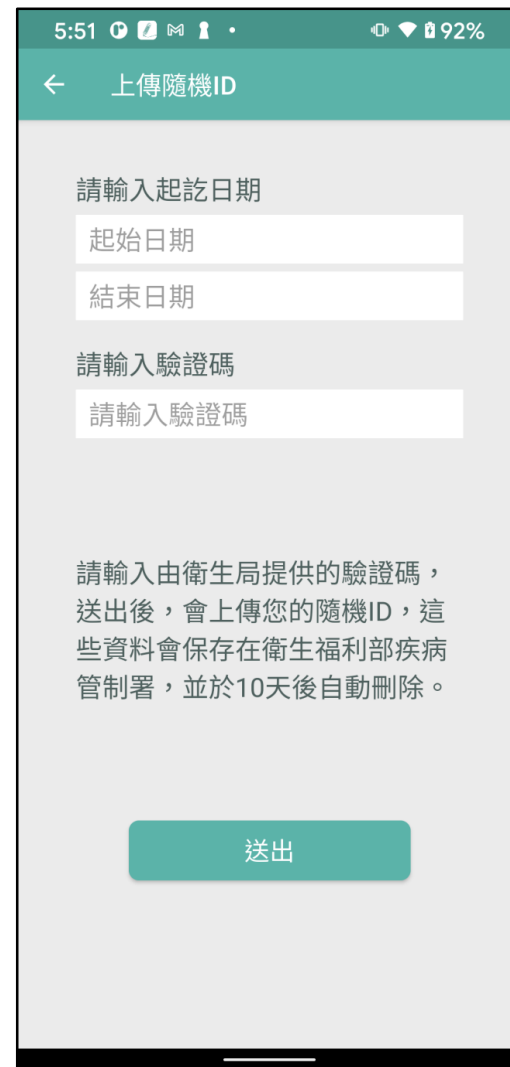
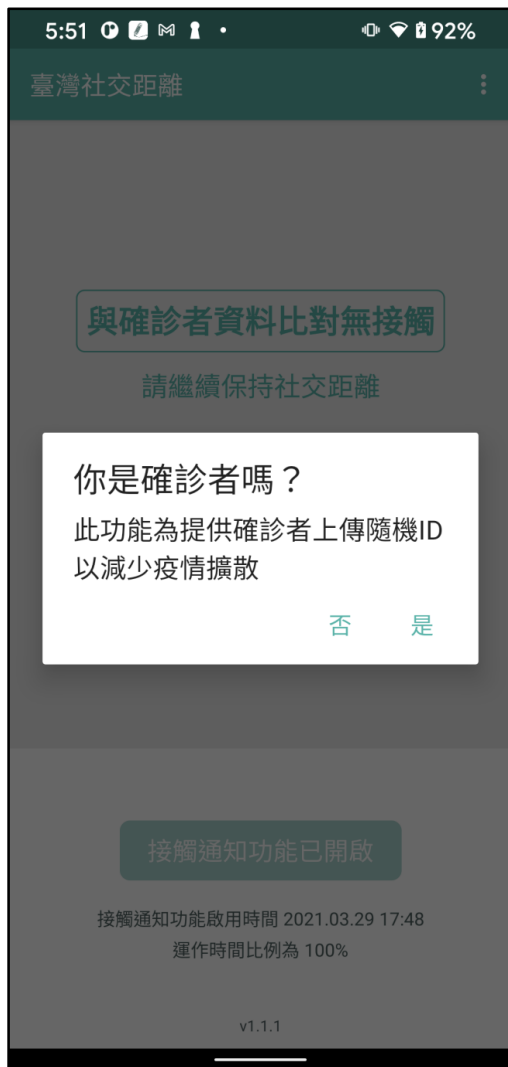
App畫面-比對無/有接觸畫面



比對有接觸
才會出現

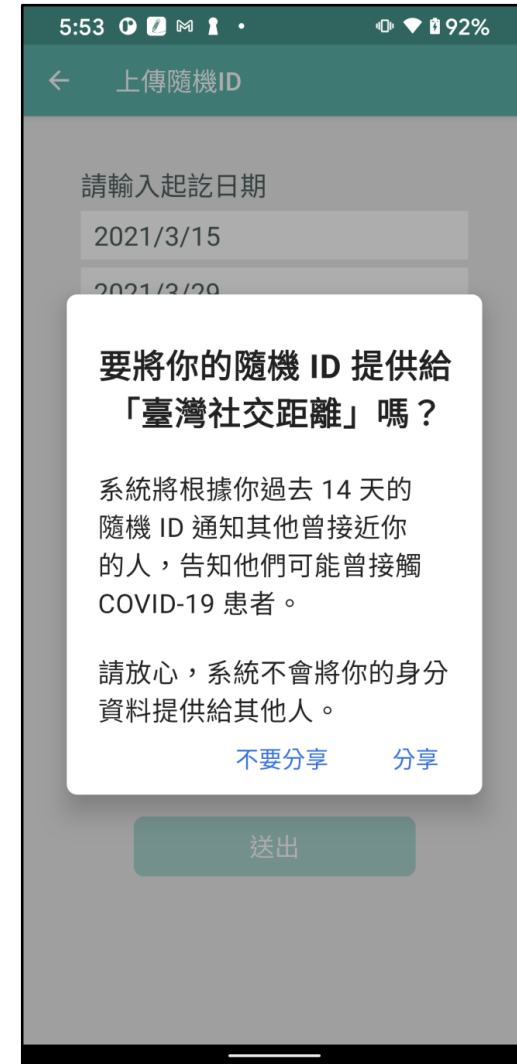


App畫面-確診者上傳隨機ID



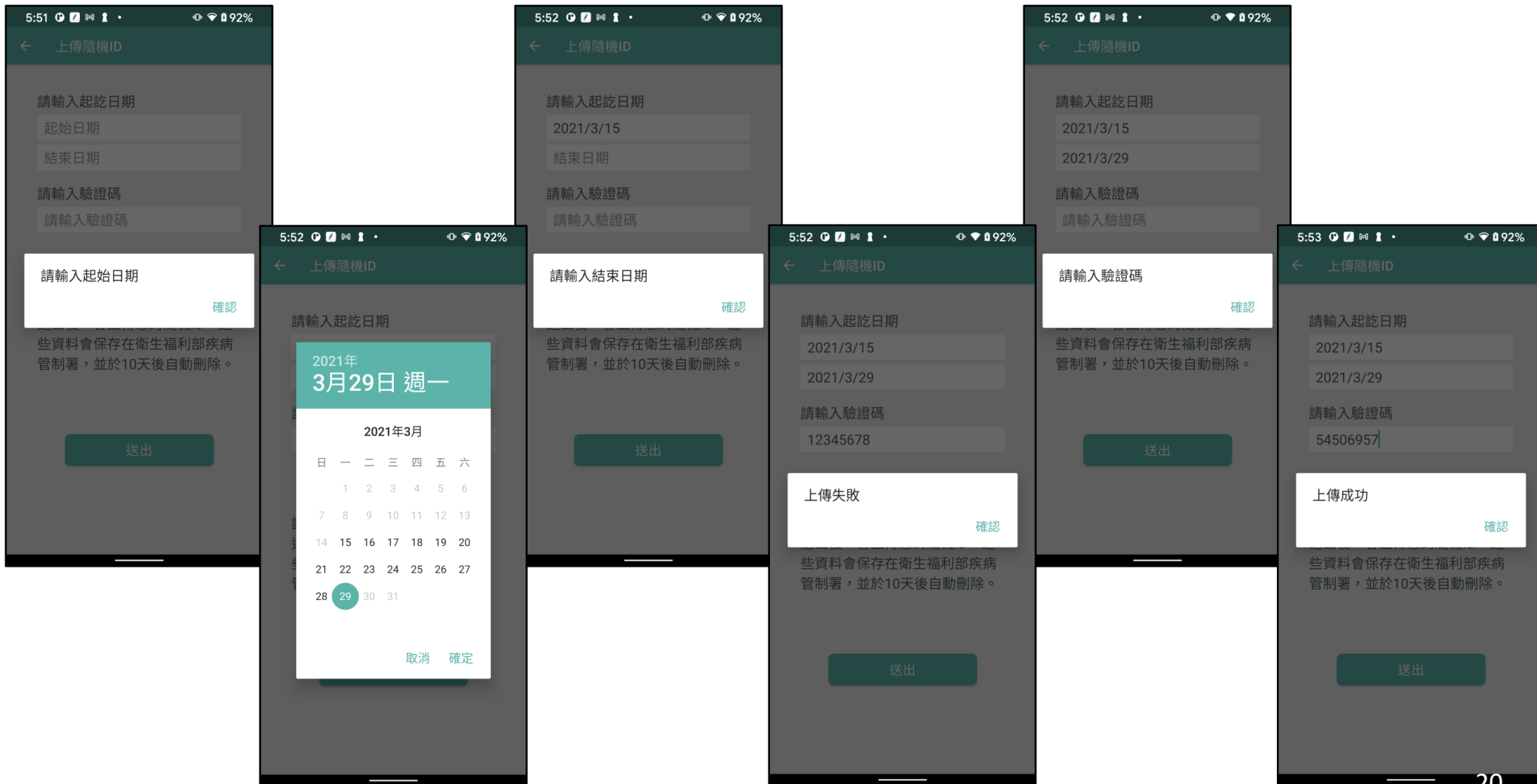


App畫面-確診者上傳隨機ID



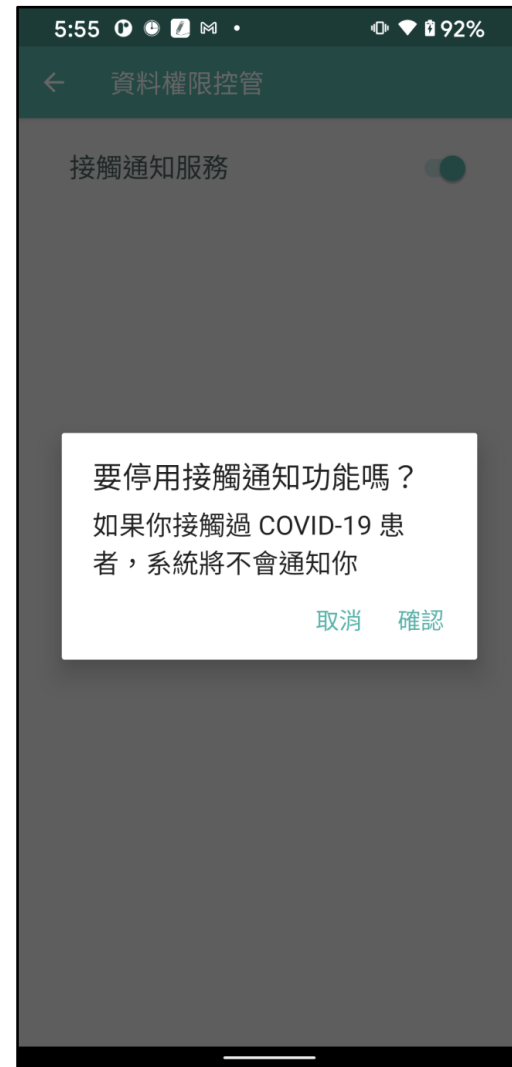
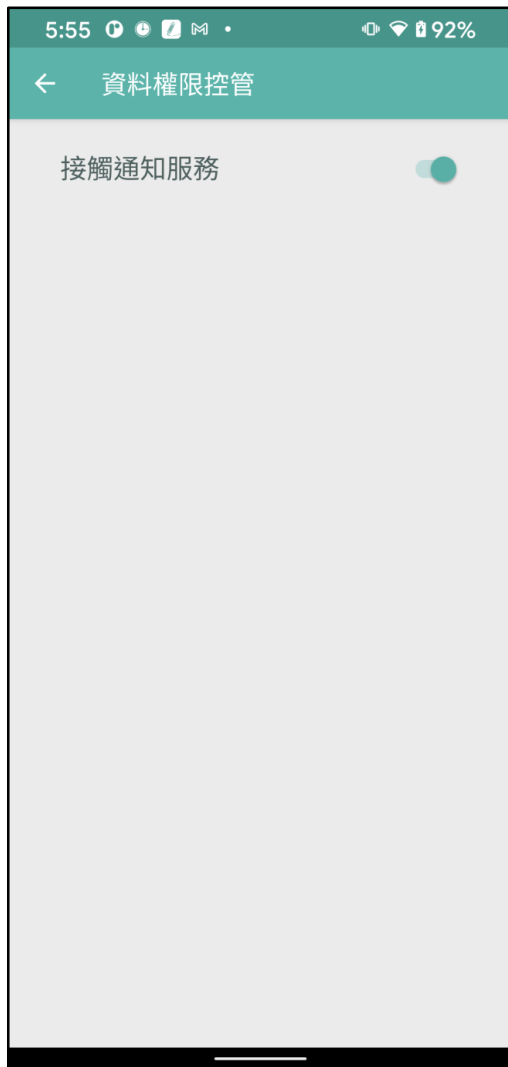


App畫面-確診者上傳隨機ID



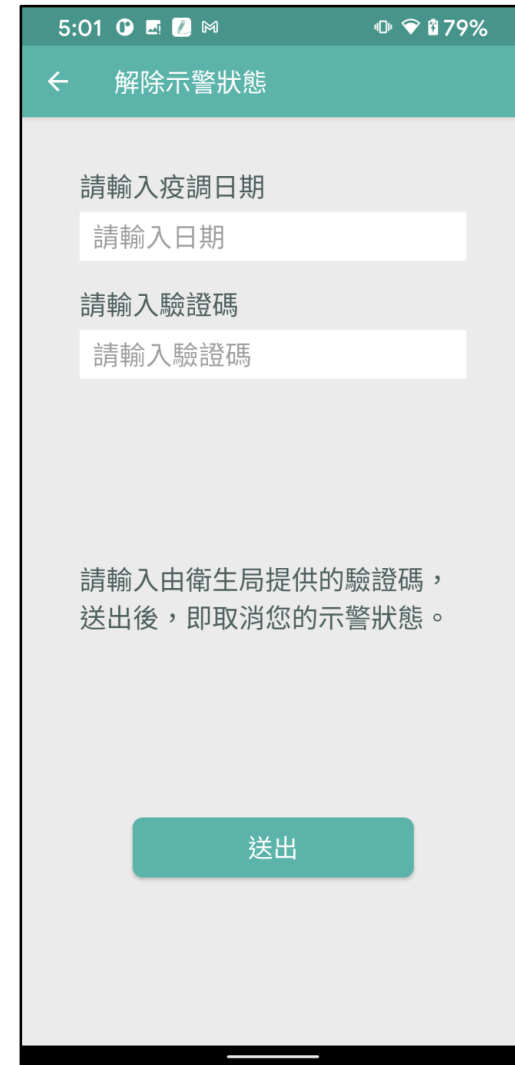
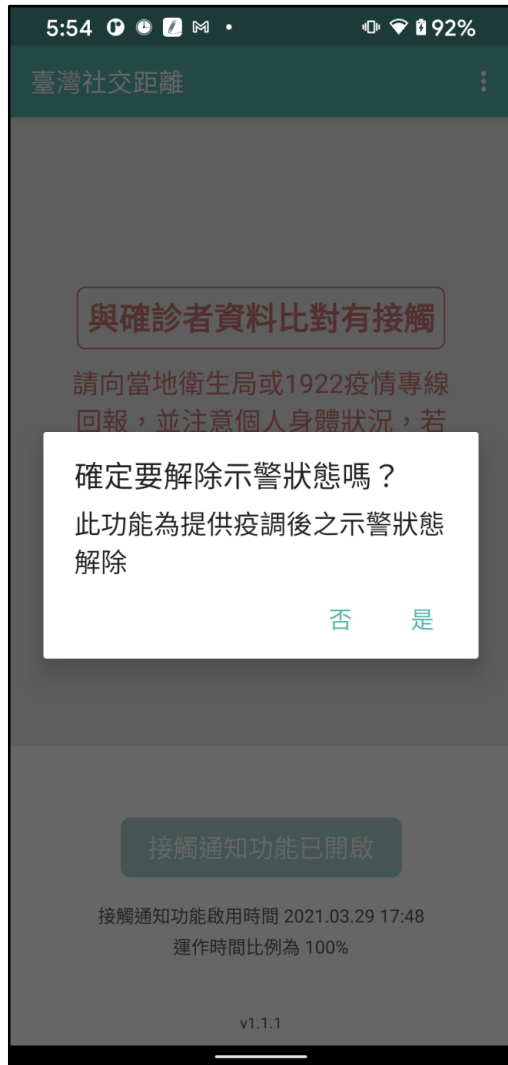


App畫面-接觸通知權限控管



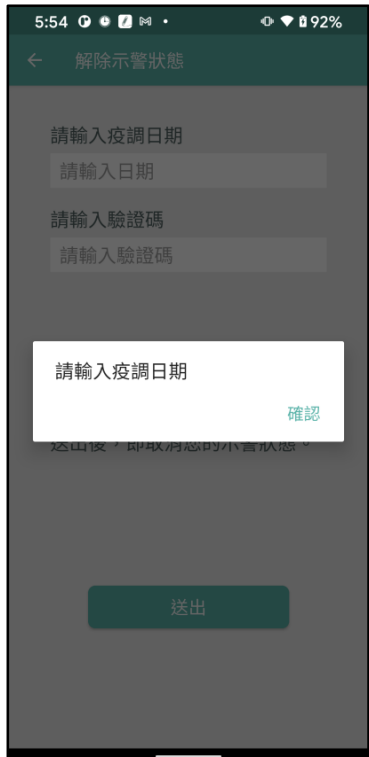


App畫面-解除示警功能



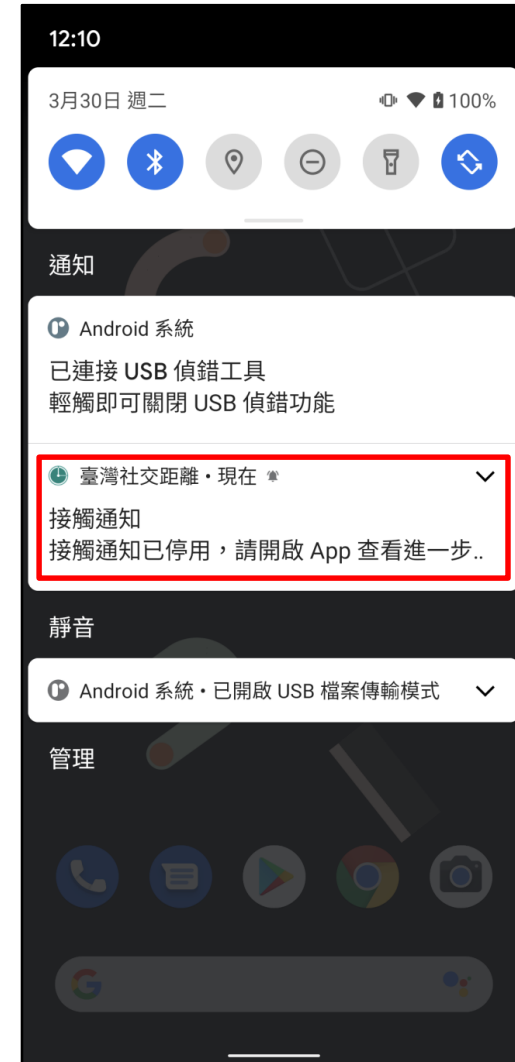


App畫面-解除示警功能





APP推播通知-已開啟/停用功能





APP推播通知-比對有無接觸風險



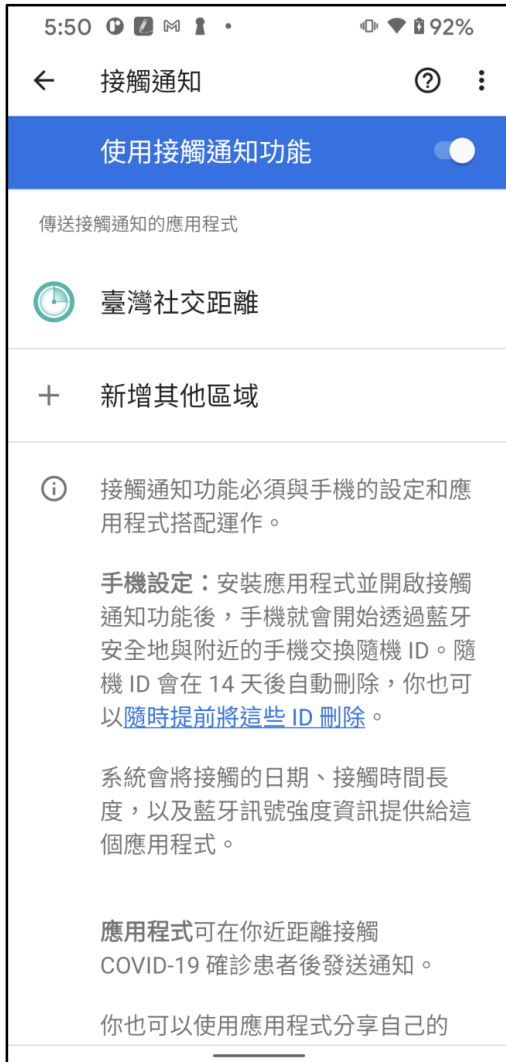


手機系統畫面

※ 以下手機系統畫面為 Android/iOS 內建設定



手機系統畫面-開啟藍牙功能

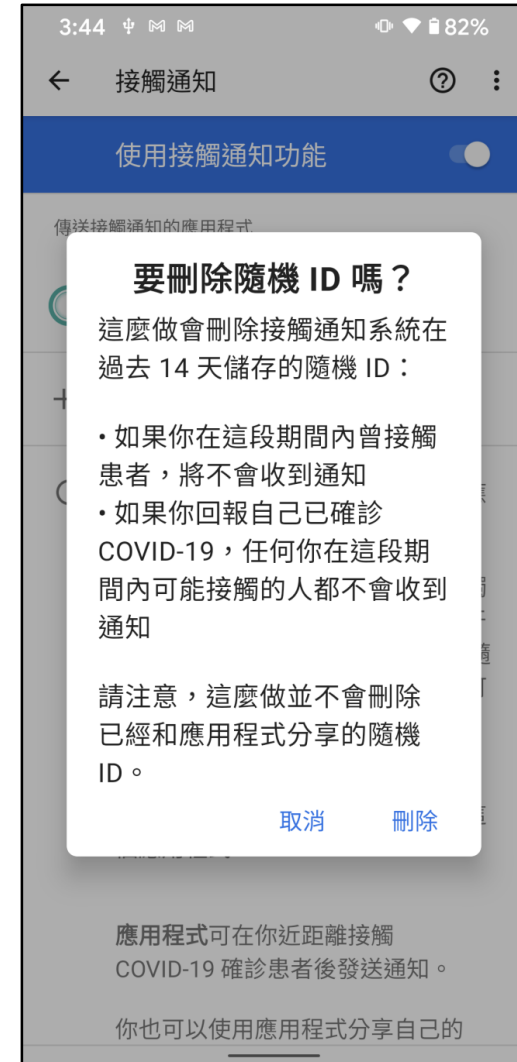




手機系統畫面-刪除隨機ID

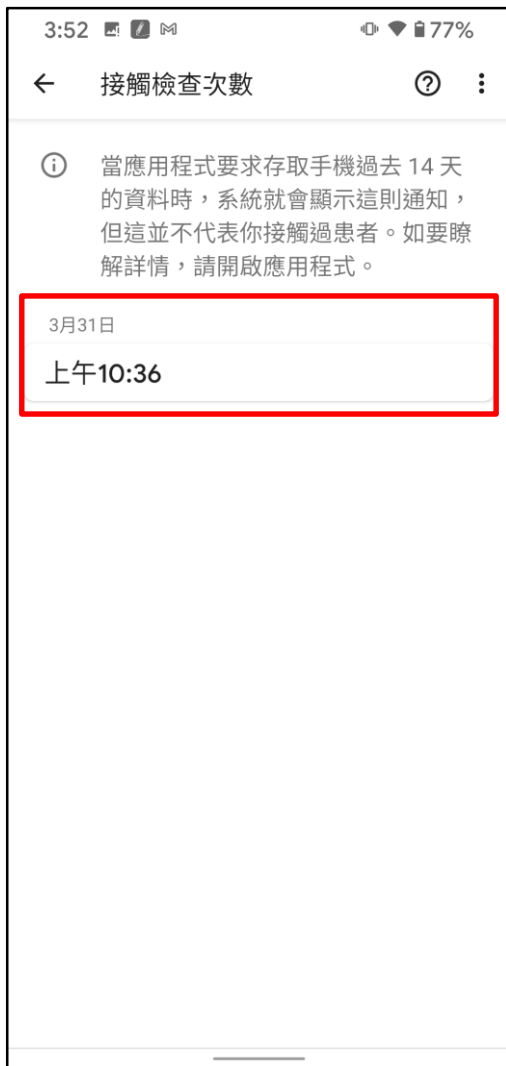


刪除手持裝置本身之隨機ID，非風險狀態





手機系統畫面-接觸檢查次數



當伺服器推播新資料時
之時間

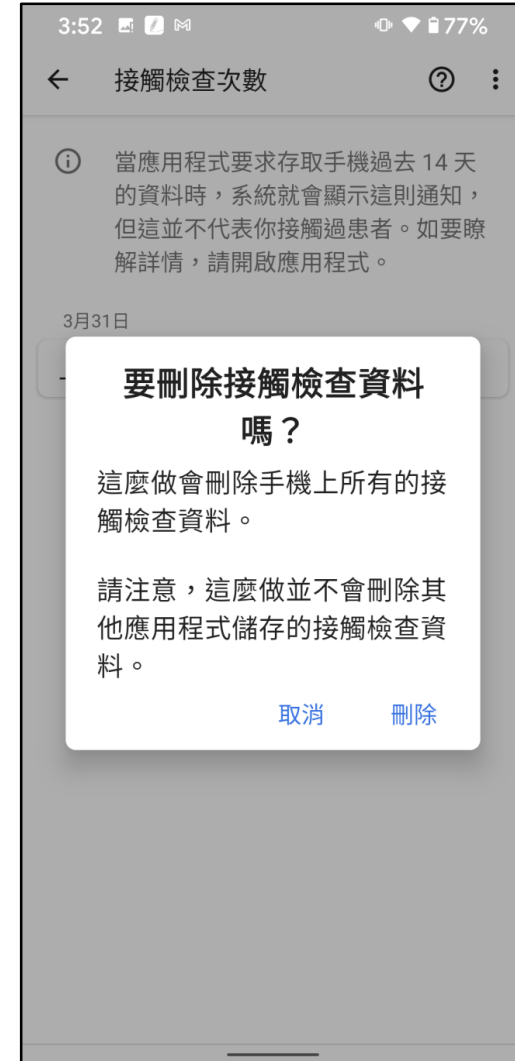




手機系統畫面-匯出/刪除檢查資料



此為文字檔，內容為
當伺服器推播新資料時
之時間





手機系統畫面-自動通知其他人



此為無須App之內建系統功能啟用選項，因臺灣地區已有接觸通知App，故無法選取。





報告完畢
敬請指教