

The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University

Advisor: Chun-I Fan

May 11, 2021

Outline

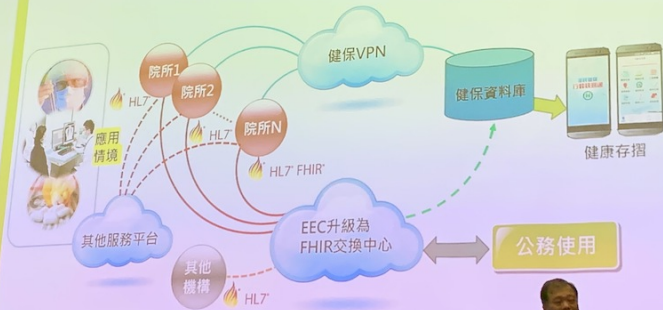
Background

Background

Researching takes time.



電子病歷交換架構及平台的改革



Research

2017衛生福利部電子病歷資訊安全檢查表

Change password?

19	具特殊權限公用程式之使用	<p>目的： 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。</p> <p>合格項目： 特權的公用程式應造冊，每次抽查時，未限制不得超過3件。</p> <p>[註]未有使用特權的公用程式者，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
----	--------------	--	--	--

Parallel permission

19	具特殊權限公用程式之使用	<p>目的： 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。</p> <p>合格項目： 特權的公用程式應造冊，每次抽查時，未限制不得超過3件。</p> <p>[註]未有使用特權的公用程式者，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
----	--------------	--	--	--

Without encryption?

六、密碼學				
21	密碼控制措施	<p>目的： 資訊系統設定加解密演算機制有否符合院內規定，且機密資訊應加密儲存。</p> <p>合格項目： 訂有加解密機制之規範與落實執行。</p> <p>[註]醫院之資訊系統若無設定加解密機制，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格

2017衛生福利部電子病歷資訊安全檢查表

FTP? SFTP?

36	資訊傳送政策 /程序與協議	<p>目的： 應訂有資訊傳送協議(內外部)、政策、程序及控制措施，以保護經由使用所有型式通訊設施或電子(例如電子郵件、即時通訊或FTP資料傳輸等)等資訊傳送。</p> <p>合格項目 訂有相關規範與落實執行。</p>	<input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
----	------------------	--	---	---

Without certificate?

項次	項目	必要	評量項目	自評結果	檢查結果
22	金鑰		<p>目的： 金鑰管理(如軟體憑證等)須符合院內規定。</p> <p>合格項目： 訂有金鑰管理之規範與落實執行。</p> <p>[註]醫院若無軟體憑證等金鑰，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格

嚴重懷疑沒有經過資安專家審核

Linux source code

static __latent_entropy struct task_struct *copy_process

- fork.c L1851-2399
- 549

task_struct

- sched.h L649-1401
- 753

Key part - *copy_process

Key part - task_struct

Formal verification

- Abstract Interpretation
- Formal Model Checking
- Theory Prover

λ -calculus

Privacy

Privacy is not only federated learning

