正本

臺中榮民總醫院　書函

地址：407台中市西屯區台灣大道四段1650號
承辦人：林欣誼
電話：(04)2359-2525#4781
電子信箱：ivy87088@vghtc.gov.tw

受文者：台灣藥物臨床研究會

發文日期：中華民國105年11月30日
發文字號：中榮研字第1054300197號
速別：普通件
密等及解密條件或保密期限：
附件：如說明

主旨：檢具「電子病歷系統調查表」乙份，惠請查收。

說明：

一、覆貴協會105年09月13日(105)台臨研字第105091301號函。

二、檢附資訊室協助完成電子病歷系統調查表乙份。

正本：台灣藥物臨床研究會
副本：本院資訊室、臨床試驗中心

臺中榮民總醫院

台灣藥物臨床研究協會
Taiwan Clinical Research Association

中華民國開發性製藥研究協會
INTERNATIONAL RESEARCH-BASED PHARMACEUTICAL MANUFACTURERS ASSOCIATION

電子病歷系統調查表
Electronic Medical Record System Survey Form

機構名稱 Institution name	臺中榮民總醫院
系統名稱及版本 System name & version	不適用 (本院自行開發)
填寫單位 Survey form completed by (Department)	臺中榮民總醫院-資訊室及臨床試驗中心
填寫人/職稱 Completed by / Title	資訊室 / 臨床試驗中心-林欣誼
聯絡電話 Contact number	(04)2359-2525分機4781
電子郵件帳號 Email address	ivy87088@vghtc.gov.tw

問題 Questions:

1. 電子病歷系統是否有經過認證?
Is the electronic medical record certified?

■ 是Yes ☐ 否No

若有，此認證的相關條件為何 (例如ISOXXXXX):
If yes, which criteria of certification have been followed (ex. ISOXXXXX):

ISO 27001:2013

2. 是否有系統確效記錄文件可供檢視?[a]
Are the system validation documents available for review?[a]

■ 是Yes ☐ 否No

說明Comments: 使用者填寫「電腦功能增改申請單」，功能完成後經使用者測試通過，才准予上線

3. 系統是否定期確效，且系統確效記錄是否於保存期間內妥善儲存並可即時取得?
Is the system validated on a regular basis and the validation information readily retrievable and retained throughout the retention period?

■ 是Yes ☐ 否No

若是，多久進行一次確效? 每年進行稽核至少一次
If yes, how often will the validation been performed again?

4. 資料是否曾傳輸到其他的媒介? 如果是，是否有品質控制流程以確保傳輸的資料正確無誤? **Are data ever transferred to other media? If yes, is there a QC process to ensure that the data are correctly transferred?**

■ 是 (請勾選) Yes (please tick)
- ☐ 曾傳輸到其他的媒介 Transferred to other media
- ■ 有品質控制流程 QC process is available
- ☐ 無品質控制流程 QC process is not available

☐ 否 No

說明Comments: 存放至備份媒體，進行抽測確認備份資料完整

5. 是否備有系統產生的稽核追蹤紀錄 (audit trail)?
Is there a system generated audit trail?

■ 是Yes ☐ 否No

說明Comments: 系統紀錄存放於 Log Server

6. 病歷修改後，原始資訊是否仍可供檢閱?
Is the original information still available for review after the change is made?

■ 是Yes ☐ 否No

說明Comments: 保存病歷修改紀錄

7. 稽核追蹤記錄是否可於監測及查核時檢閱?
Is the audit trail available for monitoring and inspection?

■ 是Yes ☐ 否No

若是，請說明檢閱流程:
If yes, please describe the review process:

病歷管理會定期檢視調閱人員紀錄

8. 是否有防止稽核追蹤紀錄及其他安全設定被使用者修改或被關閉之措施?
Are the audit trail and other security settings protected from modification or being turned off by users?

■ 是Yes ☐ 否No

說明Comments: 使用者無法關閉稽核追蹤紀錄

9. 稽核追蹤紀錄是否能記錄所更改的日期、時間、內容以及修改人員?
Is the audit trail available to capture the date/ time/ details/ person of record change?

■ 是Yes ☐ 否No

說明Comments: 以上欄位皆有紀錄

10. 稽核追蹤記錄之保存期間為多久?
How long is the retained period for the records of audit trail?

保存期間 Retention period: 依 ISO 27001:2013 標準：系統紀錄保存 3 個月，病歷存取記錄保存 7 年

11. 電腦日期與時間有進行管制嗎?[b]
Are the computer date and time controlled? [b]

■ 是Yes ☐ 否No

說明Comments: 每日與 NTP 自動校正時間

12. 系統是否包含完整的記錄 (資料、中介資料、稽核追蹤以及電子簽章 [適用時])?[c]
Does the system contain complete records (data, metadata, audit trail, and, as applicable, e-signatures)? [c]

■ 是Yes ☐ 否No

說明Comments: 包含以上完整紀錄

13. 對於資料與中介資料，是否備有適當的備份、復原與緊急應變的程序?[d]
Are there adequate backup, recovery and contingency procedures for data and metadata? [d]

■ 是Yes ☐ 否No

說明Comments: 設有備份復原程序及緊急應變程序

14. 備份的設備是否儲存在一個安全的地方，且備份資料儲存、運行於與主資料不同處，以防萬一與主資料一同損壞? (應該異地備份)
Are backup media stored in a secure location, and the backup and main databases stored and functioned separately in order to avoid any damage in one crash? (The backup media should be kept off-site in a secure location).

■ 是Yes ☐ 否No

說明Comments: 設有異地備份設備

15. 備份系統是否即時備份資料?
Is the backup system backup the data on a real-time basis?

■ 是Yes ☐ 否No

說明Comments: 設有備份系統，每日備份資料

16. 是否有測試過備份資料的還原情況?
Has the restoration of backup data been tested?

■ 是Yes ☐ 否No

說明Comments: 不定期抽測確認備份資料完整性

17. 如果電子病歷系統無法使用，是否有緊急的應變計畫 (如:紙本病歷)
Is there a contingency plan (e.g. paper record) in place in case the system becomes unavailable

■ 是Yes ☐ 否No

說明Comments: 設有緊急應變程序

18. 是否有最新的緊急應變程序，描述如何將硬體、軟體及資料數據恢復?
Is there an up-to-date disaster recovery plan in place, describing how hardware, software and data will be restored?

■ 是Yes ☐ 否No

說明Comments: 設有緊急應變程序，每年檢討更新

19. 是否備有實體的保全程序與管制措施，以確保環境控管?[e]
Are there procedures and controls for physical security, ensuring a controlled environment?[e]

■ 是Yes ☐ 否No

說明Comments: 設有門禁管制與錄影監控機制

20. 是否備有確保使用者帳號及密碼安全的程序與管制措施?[f]
Are there procedures and controls for the security of user account and password?[f]

■ 是Yes ☐ 否No

說明Comments: 設有帳號密碼登入管控機制

21. 是否有流程確保任何已不具權限的人其權限會及時被移除?
Is there a process to ensure that individuals who should no longer have access are removed in a timely manner?

■ 是Yes ☐ 否No

說明Comments: 離職或調職者移除其權限

22. 是否備有管理和記錄系統變更的程序?[g]
Are there procedures to manage and document changes to the system?[g]

■ 是Yes ☐ 否No

說明Comments: 程式上線設有申請與管理程序

23. 是否備有針對病毒、駭客等的防護措施?[h]
Is there protection from viruses, hackers, etc.? [h]

■ 是Yes ☐ 否No

說明Comments: 設有防火牆、防毒牆等防護設備

24. 是否備有適當的裝置檢查及/或作業檢查?[i]
Are there Device and/or Operational Checks as appropriate? [i]

■ 是Yes ☐ 否No

說明Comments: 設有無線網路管控機制，未核准設備無法使用

25. 系統記錄文件是否進行妥善保存?[j]
Is the system documentation maintained appropriately? [j]

■ 是Yes ☐ 否No

說明Comments: 存放於 Log Server

26. 是否使用專屬且受管制的電子簽章?[k]
Are unique and protected electronic signatures used? [k]

■ 是Yes ☐ 否No

說明Comments: 使用衛生福利部核發醫事人員憑證進行電子簽章

27. 如果使用電子簽章，有任何書面程序可讓人員對其簽章負責嗎?[l]
If e-signatures are used, are there written procedures to hold people accountable for their signature? [l]

■ 是Yes ☐ 否No

說明Comments: 電腦使用人員均需填寫帳號密碼申請單及保密切結書

28. 如果使用電子簽章，電子簽章是否包含個人姓名、日期、時戳，以及簽章的意義?[m]
If e-signatures are used, do e-signatures include individual's name, date, time-stamped and meaning of signature? [m]

■ 是Yes ☐ 否No

說明Comments: 包含以上各欄位

29. 若一段時間內未使用，系統是否會自動登出?
Does the system automatically log off a user after a specified period of inactivity?

■ 是Yes ☐ 否No

說明Comments: 三十分鐘未使用即自動登出

30. 臨床試驗電子記錄的蒐集與保存做法與相關法規(例如醫療法及GCP) 要求一致嗎?[n]
Are clinical trial electronic record collection and retention practices consistent with regulatory requirements, such as Medical Care Act and GCP? [n]

■ 是Yes ☐ 否No

說明Comments:_____

31. 當依照GCP規定執行監測、稽核或查核時，是否有流程或政策可檢視或複印特定臨床試驗之電子病歷?[o]
Is there a process and management policy to access or copy the electronic medical record for specific clinical study while conducting monitoring, auditing and inspection under the compliance of GCP? [o]

☐ 有Yes ■ 否No

若有，請說明檢閱流程:
If yes, please describe the review process:

_____

32. 是否有提供監測人員申請臨時使用且獨立的電子病歷帳號密碼的流程?
Is there a process to provide a temporary and independent EMR account and password to Monitor / CRA?

■ 是Yes ☐否No

說明Comments:_____

33. 監測人員的電子病歷帳號權限是否只限於閱覽，且僅能閱覽特定案件的受試者病歷?
Will the monitor's EMR access be read only and be limited to the medical records of a specific trial's subjects?

■ 是Yes ☐ 否No ☐ 不適用NA

說明Comments:_____

34. 監測人員是否可閱覽受試者所有的電子病歷資料?
Will the monitor access all the electronic medical records of a clinical trial subject?

■ 是Yes ☐ 否No

說明Comments: _____

35. 是否提供外部使用者有關系統訓練的手冊或標準作業程序?
Does site have EMR user manual and SOP for external user?

☐ 是 (請勾選) Yes (please tick)
- ☐ 提供訓練手冊 User manual is available
- ☐ 提供標準作業程序 SOP is available

■ 否No

說明Comments:_____

36. 是否有使用及維護系統的人員之訓練證明文件? [P]
Are there documented training records for persons that use and maintain the system? [P]

☐ 是Yes ■ 否No

說明Comments:_____

37. 是否有提供監測者使用EMR的相關訓練?若有，是否有提供訓練紀錄或證書?
Does site provide EMR training to monitors? If yes, is training record or certificate available?

☐ 是(請勾選) Yes (please tick)
- ☐ 無提供訓練紀錄或證書No training record nor certificate
- ☐ 提供訓練記錄 Training record is available
- ☐ 提供訓練證書 Training certificate is available

■ 否No

說明Comments:_____

填寫人:
Completed by

簽名: 賴秉勳
Signature

日期: 25 / 11 / 2016 (dd/mmm/yyyy)
Date

臨床試驗中心(任鑑)
契約暨務管理師員 林欣誼

30 / 11 / 2016

備註Note:

[a] 軟體確效記錄文件係用於呈現軟體是否符合試驗中心的所有要求與使用者期望的「信心水準」建立程度。確效記錄文件的「標準套件」包含系統應該達到的要求、用於測試系統應執行項目的一套計畫、測試結果評估、錯誤評估/解決方式，以及最後的總結報告等。證明系統已針對「確保準確性、可靠性、一致的預期性能，以及能偵測無效或變更的記錄」等目的而完成確效的所需記錄文件，將視系統是否由機構購買或自行建立而定。

Software validation documentation is the demonstration of the developing "level of confidence" that the software meets all the site's requirements and user expectations. A "typical set" of validation documentation includes requirements for what the system is supposed to do, a plan to test what the system is supposed to do, test results evaluation, error evaluation/resolution, and a final summary report. Depending on if the system is purchased or "built" by the institution, the documentation required to show that the system has been validated "to ensure accuracy, reliability, consistent intended performance and the ability to detect invalid or altered records" will vary accordingly.

[b] 電腦的日期與時間也必須來自可靠的來源，而且使用者無法變更該來源。同時，也應該準確、清楚且可控制的。中心應備有書面程序，說明誰負責設定並定期檢查系統時脈(system clock)。附註說明，網路化的系統，其螢幕上的時間不得為系統/軟體的時間來源。中心應能告知時間來自何處以及由誰確保其準確性。產生的所有資料應可進行追蹤且系統使用的日期可支援這個動作。在您討論有關稽核追蹤及/或電子簽章時，您應該詢問日期來自何處，由誰確保這個日期的正確性，以及有任何差異時，由誰負責處理?

The date and time of the computer should be taken from a reliable source that cannot be modified by the users. It should also be accurate, unambiguous and controlled. Written procedures should be located at the site stating who is responsible for setting and periodically checking the system clock. Just as a note, for networked systems the time on the screen may not be the source of the time for the system/software. The site should be able to tell you where the time is coming from and who makes sure it is correct. All data generated should be traceable and the date that the system uses supports this activity. In your discussions about the audit trail and/or electronic signatures, you should ask where the date comes from and who makes sure that this date is correct and who addresses any discrepancies?

[c] 換句話說，如果資料是移轉自另一個系統、更舊的軟體版本或另一個位置，您是否能夠檢視完整的記錄? 如果答案是否定的，那麼機構必須讓您能夠檢視原始記錄，以便確認 CRF 上面的資訊。以下則說明有關資料與中介資料所代表的意義：

Or another way to ask this question, are you able to view a complete record if data has been transferred from another system, an older version of the software or another location? If not, the institution is required to allow you to look at the original record to verify information on the CRF. To clarify what is meant by data and metadata:

資料：代表適合以人工或自動化的方式來傳達、解讀或處理的事實、概念或指示。

Data: Representations of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or automated means.

中介資料：是指和資料有關的資料。所謂中介資料是指無法實際納入記錄的一部份，但是對於賦予該記錄意義、達到文件需求仍有其必要性的資料 (根據《美國聯邦法規》第

21 篇第 11 節或相關之既有規定，如：cGMP、GLP 以及 GCP 等定義)。
Metadata: This is data about the data. Meta-data is that data that may not be physically included as part of a record but is still necessary to give that record meaning to fulfill documentation requirements (based on 21 CFR Part 11 or applicable predicate rules, e.g., cGMP, GLP, GCP, etc.).

「具體而言，可能與電子紀錄相關的中介資料類型可包含：記錄的建立、作者、建立日期、所有權、可用來分類文件的搜尋關鍵字、文件內找得到的資料類型等細節，以及不同資料組成之間的關係等。中介資料必須儲存成所描述之電子文件所必需的部份。」(21 CFR Part 11) "
In practical terms, the types of metadata that can be associated with an electronic record may include: details of the record's creation, author, creation date, ownership, searchable keywords that can be used to classify the document, details of the type of data found in the document, and the relationships between different data components. Meta-data must be stored as an integral part of the electronic document it describes." (21 CFR Part 11)

d. 應將備份與重建程序正規化。此一重要程序應予以合格化並備有包含各步驟被執行的證明文件。系統無法使用時的緊急程序也應該納入恢復正常作業前採取的行動，以及針對系統停機時產生的資料所採取的行動(如適用)。應定期執行電子記錄與中介資料的備份，以免遺失資訊。應在系統所有人核准的系統要求與系統程序內，制定備份的頻率，因為這會影響到災害時可能遺失的資料數量。舉例而言，eDM 電子資料管理系統被認定為對公司營運致關重要的系統，而我們每天都有累積備份外，每週均有完整備份，以免試驗資料遺失或損毀。另外針對在中心以外儲存的備份與檔案庫媒體，也應該有保護程序的存在。
A backup and restore process should be formalized in a procedure. The procedure is critical and should be qualified and documented to include proof that the steps were performed. Referring to a time when the system is not able to be used, contingency procedures should also include action to be taken until normal operation is restored and what actions are taken to the data generated during the system downtime, as applicable. Backups of electronic records and meta-data should be performed regularly to prevent loss of information. The frequency of backups should be defined in the system requirements and system procedures approved by the System Owner since this impacts the amount of data that could be lost during a disaster. For example a system like eDM is determined to be critical to sponsor's operation and we have periodical full backups with daily incremental backups to protect study data from loss or corruption. Procedures should exist to protect backup and archive media when stored off-site.

e. 系統必須位於一個提供實體保全與營運完整性(符合系統功能需求者)的環境內。應有實體的保全與營運程序。保全應擴及試驗中心內所有人，含訪客、委託者代表、清潔人員等。電腦設施(包含控管室與儲藏櫃)，應有實體的保全並控管使用權(門鎖、出入登記簿、刷卡等)。應視需要控管並監督環境條件，以維持營運完整性。環境條件應符合廠商規定。也應將確保備份記錄的實體保全列入考量。
Systems must be located in an environment that provides physical security and operational integrity, as appropriate to the system function. Physical security and operational procedures should exist. Security should extend to all roles at the investigator site, including visitors, sponsor representatives, cleaning people, etc. Computer facilities including control rooms and storage closet should be physically secure with controlled access (locked doors, log books for entry and exit, key card access, etc.). Environmental conditions should be

controlled, as appropriate, and monitored, where needed, to maintain operational integrity environmental conditions should meet manufacturers' specifications. Consideration should also be taken to ensure the physical security of backed up records.

f. 所管制的系統應有一致性的程序及/或管制措施來管理使用者名稱與密碼。(如：處理一般過期不會超過 90 天的密碼、發放識別資訊、定期檢查使用記錄，以及停用系統使用權的程序。) 如果系統及/或營運系統的功能不包含密碼過期，則應執行需要定期變更密碼的程序管制。使用中的系統不應處於未被監控的狀態，系統應具備密碼管控的螢幕保護(逾時保護)來防止未被授權的人員於系統非使用時段對於資料的取得。
If system and/or operating system functionality does not include password aging, procedural controls should be implemented that require periodic password changing. Procedures and or controls should be established to manage user ID and passwords consistently across regulated systems. (e.g., procedures addressing password aging typically not exceeding 90 days, issuance of identification information, periodically checking access logs, and termination of system access). An active system should not be left unattended. The system should have a password controlled screen-saver ("timeout" feature) to prevent unauthorized access during periods of inactivity.

g. 對系統進行的變更，必須控管並加以記錄。應備有程序可確保系統所有人已評估所有的變更(含供應商建議的變更)。若為了持續使用軟體，而需要進行變更或保證會進行變更，則變更核准的審查記錄、測試/重新確效(如需要)、最後變更的評估，以及將發行的消息告知系統使用者等事項也應與其他系統記錄文件同時備妥。
Changes made to the system must be controlled and documented. Procedures should be in place to ensure that all changes are evaluated by the owner of the system (even those recommended by a vendor). If a change is needed or is warranted for the continued use of the software than a documented review of the change approval, testing/revalidation (as necessary), evaluation of final change and communication to the users of the system about the release should all be present with other system documentation.

h. 電子病毒、蠕蟲、惡意程式、駭客等會威脅資訊完整性與系統可用性。應該安裝防毒軟體 (如：McAfee、Norton 防毒軟體、BitDefender 等)，隨時更新並主動執行/掃描網路或非網路內的任何類型的系統。有開放使用網際網路的系統也應該採取額外的防護措施，如：防火牆與惡意程式偵測等。作業系統也應該隨時更新，以減緩系統受到的攻擊。
Electronic viruses, worms, malware, hackers, etc. are a threat to information integrity and system availability. The site should have virus software installed (e.g. McAfee, Norton antivirus, BitDefender, etc.), kept up-to-date, and working/scanning actively for any type of system networked or non-networked. Additional precautions should be taken for systems open to the internet, for example firewalls and malware detection. Operating systems should also be kept up-to-date to mitigate an attack on the system.

i. 應有裝置檢查以確保只有特定裝置被選作資料輸入或指令的合理來源。確效可用於證明特定的終端或工作站在技術上能從某個點將資訊傳送到另一個點。然而單靠確效本身，並無法處理此類裝置是否有取得執行此類工作的授權 (《美國聯邦法規》第 21 篇第 11 節；前文#85)等細節。
Device checks are warranted where only certain devices have been selected as a legitimate source of data input or commands. Validation may demonstrate that a given terminal or workstation is technically capable of sending information from one point to another, however validation alone would not be expected to address whether or not such device is

authorized to do so. (21CFR Part 11; Preamble #85)

「適當的」一詞表示並非所有情況下都需要進行裝置檢查。此類檢查應該只適用於特定已經選作資料輸入或指令的合理來源的裝置。舉例而言，在網路環境下，可能基於保全考量需要限制發出至授權工作站的重要指令。而在實驗室的環境下，可能需要確保資料只來自特定校準過的儀器。
The term "appropriate" suggests that device checks are not required in all cases. These checks should be used when certain devices have been selected as legitimate sources of data input or commands. For example, in a network environment it may be necessary for security reasons to limit issuance of critical commands to an authorized workstation. In a laboratory environment it may be necessary to ensure that data only comes from a specific calibrated instrument.

系統所有人與開發商應在定義與設計系統時評估器材檢查的適用性 (如：電腦系統必須能夠區分作業來源與有效性)，進而決定資料輸入或作業指示來源的有效性。此類評估應包含在系統記錄文件內。整體而言，主持人不會執行此類評估，因為此類評估屬於系統設計的一部分，是由供應商決定。
System owners and developers should evaluate the suitability of device checks (e.g., the distinction the computer system can make regarding the source and validity of an operation) during system definition and design to determine the validity of the source of data input or operational instructions. Such evaluations should be included in the system documentation. In general, the investigator would not do this type of evaluation as it would be integral to system design and determined by the vendor.

裝置檢查：裝置檢查確保電腦系統有接收來自合理來源的資料。
Device checks: device checks ensure that the computer system is receiving data from legitimate source

作業檢查：作業檢查可確保輸入資料時事件的排序正確。例如，如果 A、B 與 C 事件必須按照順序發生，則系統會確保 A 事件在 B 事件之前發生，而 B 事件在 C 事件之前發生。
Operational checks: Operational checks ensure proper sequencing of events when entering data. If events A, B, and C have to occur in order, the system ensures that Event A occurs before Event B which occurs before Event C.

j. 系統記錄文件是說明系統如何作業與維護的記錄。必須適當地管制(保全、變更控管、使用權等)記錄文件，才能確保系統的運作一致。除了管制外，同樣重要的是系統記錄文件必須隨時更新，並由變更管理的系統進行控管(針對記錄的內容、變更歷史記錄等設定版本)。系統記錄文件包含：標準作業程序、系統維護記錄、使用者手冊、說明檔、系統開發記錄文件、功能要求、設計規格、使用記錄文件、使用者訓練記錄、緊急計畫，以及其他確效資料等。來源碼也視為是系統記錄文件的一部分。
System Documentation are records describing how a system operates and is maintained. Adequate controls (security, change control, access rights, etc.) over the documentation are necessary to ensure the consistent operation of the system. In addition to control, it is important that the system documentation be kept up to date and controlled under a system of change management (versioning of the documented, history of change, etc.) System documentation includes standard operating procedures, system maintenance documentation, user manuals, help files, system development documentation, Functional Requirements, Design Specifications, User Documentation, User Training Records, Contingency Plan and

other validation materials. Source code is also considered to be part of the systems documentation.

k. 電子簽章是指針對個人執行、採用或授權、當作該個人手寫簽名且具有相同法律約束力的任何符號或一系列的符號所建立的電腦資料。電子簽章一般不是個人手寫簽名或打印在 WORD 文件上的一行字。舉例而言，如果記錄遭到變更，必須備有管制措施，能用於確保初始的簽名已經不再與已簽署的記錄有任何連結，並要求針對修改的記錄重新簽署。以電子各案報告表來說，電子簽章將永遠與記錄連結，直到這些記錄不復存在為止。
Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. An electronic signature tends not to be an image of an individual's handwritten signature or a line typed into a Word document. For example, if the record is changed, controls must be in place to ensure it is clear that the initial signature is no longer linked to the signed record, and to require re-signing of the modified record. As in electronic data capture (EDC) system, an electronic signature should be forever associated with the records until those records no longer exist.

l. 使用電子簽章時，個人必須對其電子簽章下採取的行動負責。電子簽章視為具備與手寫簽名同等的法律約束力。試驗中心應備有書面程序，讓人員對其在電子簽章下執行的行為負責，而且就這個觀念應備有可透過記錄文件證明的訓練。
When electronic signatures are used, individuals are held accountable and responsible for action taken under their electronic signatures. Electronic signatures are considered to be the legally binding equivalent of handwritten signature. Investigator site should have written procedures to hold people accountable for their actions conducted under electronic signatures and there should be documented training on this concept.

m. 是否可同時以紙本和印出的形式進行檢視?不管簽署的記錄何時被檢視或列印，已簽署的電子記錄(電子版或紙本)都應顯示簽署者的全名。這個名字必須是唯一的。如果該完整的姓名並非唯一，則應該另有一個識別依據(如：中間名的字首縮寫、使用者編號等)。
Can this be viewed both in paper and printed? Electronic records that are signed (either electronically or on paper) should manifest the signers' full name whenever the signed record is viewed or printed. This name should be unique. An additional identifier (e.g., middle initial, User ID, etc.) should be added if the full first and last name is not unique.

記錄上的簽名表示特定的重要等級或狀態的變更(如：已獲核准)。在電子環境下，必須能判斷簽名的時間。日期/時間應該明顯。一般只仰賴「隱埋式」(buried)資料來判斷記錄簽署的時間是不夠的(如：需透過進一步詢問才可察看的稽核紀錄)。
Signatures on records indicate a certain level of importance or change in status (e.g. approved). In the electronic environment it is important to be able to determine when the signature was applied. This date/time should be obvious. It is generally not sufficient to rely on "buried" data (e.g. audit trails only available through advanced queries) to determine when a record was signed.

簽章的目的在於表示特定的行動，如審閱人員、核准人等採取的行動。在簽署一份記錄以及顯示一份已簽署的記錄時，簽名的意義應該明顯。若不清楚簽名所表示的行動，可能難以判斷簽名所連結的資料以及具法律約束力的意涵。
Signatures are used to indicate specific actions such as reviewer, approver, etc. When signing

a record and when displaying a signed record the meaning of the signature should be apparent. When it is not clear what action the signature represents, it may be difficult to determine what data the signature is linked with and what are the legally binding implications.

n. 系統上的資料及稽核追蹤(audit trail)既被當做來源資料(source document)，則必須依照來源資料的保存期限來保存，且必須在主管機關要求審閱時能夠取得。電子型態的來源資料應被保存在未來仍能讀取的傳播媒介上。
System data and audit trails, being source documents, must be retained for a period as agreed for all source documents and must be available for regulatory review. Electronic source should be retained on a media that will allow credibility in the future.

根據醫療法第 70 條規定，人體試驗之病歷，應永久保存。
According to Article 70 of Medical Care Act, medical records for human trials shall be retained indefinitely.

o. 陳述這個問題的另一個方式：您是否能夠從系統中取得記錄，供主管機關以電子或書面格式檢視(僅檢視我們的試驗)?是否備有這類的流程?對於用於臨床試驗的記錄或報告，試驗中心必須為主管機關(以及試驗委託者代表) 提供存取、複製及驗證其正本/認證副本的權限。系統應該能夠產生電子記錄、電子簽章以及對應的中介資料之完整副本，例如以人類可閱讀形式呈現的稽核追蹤記錄等 (亦即能夠列印出來而且可能的話，在螢幕上檢視)。
To state this question another way - Can you get records out of the system for the Agency to review in electronic or paper format just for our studies? Is there a process for this? The site is required to provide the Agency (and to sponsor representatives) access to, copy and verify any original/certified copy of records or reports used to support the clinical trial at that site. The system should be able to generate complete copies of an electronic record, electronic signature, and the corresponding meta-data such as audit trail in human readable form (e.g., be able to print it and if possible, view it on screen).

p. 文件必須可證明以下事項：開發(視需要)、維護或使用系統的人員(系統管理員、研究人員、藥劑部人員等)具備執行其工作所需的教育、訓練與經歷。被交付重要工作項目(系統管理、資料備份、資料輸入等)的人員，必須接受充分的訓練後才能勝任。製造供應商可能已提供此類訓練，但中心至少應該有文件記錄顯示曾經教導過的內容、由誰負責教導，以及教導的對象與時間等。
Documentation must exist to show that the people that developed (as necessary), maintain or users of the system (system administrators, research staff, pharmacy staff, etc.) have the education, training, and experience to perform their tasks. Personnel entrusted with important functions (system administration, backing-up data, data entry, etc.) must have sufficient training to do their jobs. The vendor could have given this training but at a minimum there should be documentation at the site as to what was taught, by whom, to whom and when.