

個人情報保護に対応したシステム運用のあり方、 および、電子カルテ安全対策ガイドライン

2005年 1月27日

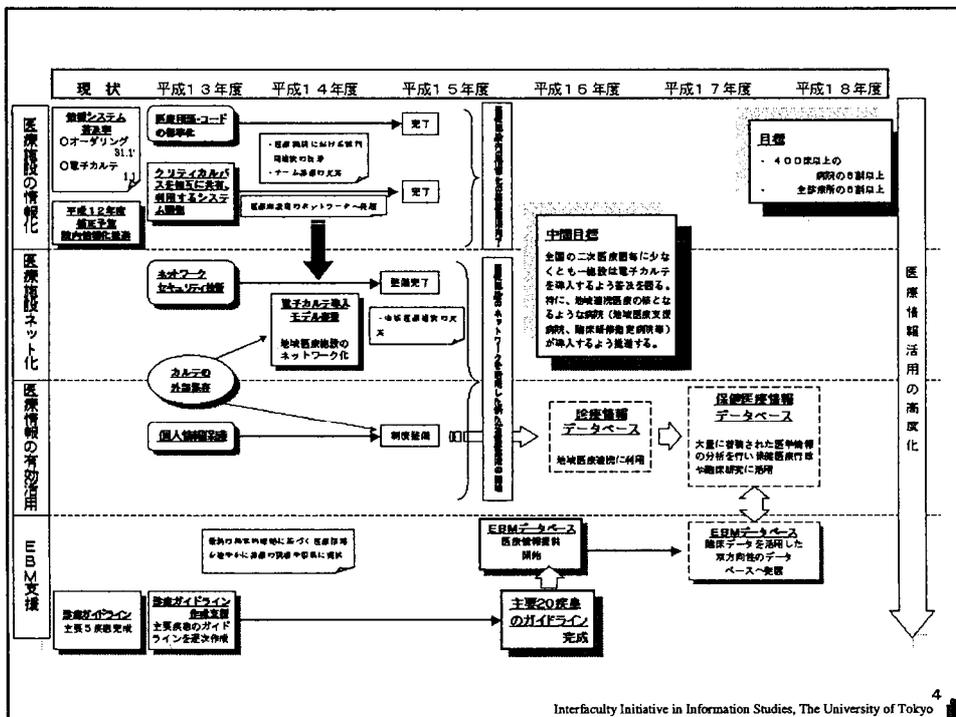
東京大学大学院情報学環 山本 隆一

医療情報の規制緩和

- ＞ S63 診療録等のOA機器による入力
- ＞ H6 医療画像の電子媒体への保存
- ＞ H11 診療録および診療諸記録の電子媒体への保存
- ＞ H14 外部保存容認(制限付き)

診療録の電子保存

- > 平成11年4月22日通知
- > 健政発517号、医薬発587号、保発82号
- > 平成6年の医用画像の保存に関する通知は廃止
- > 真正性、見読性、保存性の確保
- > 自己責任、運用規則の制定
- > プライバシー保護
- > 署名・捺印の必要な書類は保留



外部保存容認通知(H14. 4. 3)

- ＞ 原則は平成11年の電子保存と同じ
 - 真正性・見読性・保存性・プライバシー保護・自己責任・運用規程
- ＞ 事故等があった場合の責任の所在の明確化(契約等)
- ＞ オンライン電子保存は限定的
 - 個人情報保護法が未整備
 - 安全性の実証が必要
 - 見直しを明記
- ＞ 紙・フィルム媒体に関しては現状追認？

医療情報ネットワーク基盤検討会とは

- ＞ 平成15年6月に医政局長の私的検討会として設置された
- ＞ 安全に情報を伝達・参照できるような環境整備を図る必要性
- ＞ 医療情報を取り扱う際の運用面においても適正を期する必要性
- ＞ 上記確保のための基盤整備のあり方について、患者・国民の視点を重視しつつ検討する

E-文書法(161国会提出)

- > 通則法
民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律

- > 整備法
民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律の実施に伴う関係法律の整備等に関する法律

今後の医療情報ネットワーク基盤のあり方について 医療情報ネットワーク基盤最終報告

- > I はじめに
 - フリーアクセスを担保し、情報セキュリティの確保及び個人情報保護を前提とした情報伝送の技術的及び運用管理上の基盤が必要
- > II 医療における公開鍵基盤について
 - 電子署名法に適合した電子署名
 - 国際的標準を念頭に置いたヘルスケアPKI認証局開設を目指す
 - 医療の公的資格台帳の電子化とICカードによる資格認証
- > III 医療に係る文書の電子化
 - 放射線の照射録、臨床修練外国医師の診療録、及び様々な制度下に交付・運用される診断書等は電子署名で可
 - 処方箋は現状では不可であるが、処方情報の電子化を進める
 - E-文書法への対応
- > IV 医療に係る文書の電子保存
 - ガイドライン等の見直し(わかりやすく、個人情報保護法に対応)
 - オンライン外部保存に、公的機関等を追加
- > V おわりに

医療介護関係事業者における個人情報の適切な取り扱いの
ためのガイドライン III 医療・介護事業者の責務 4

＞ 安全管理・従業者の監督

- 組織的、人的、物理的、および技術的安全管理措置。
- リスクに応じ、必要かつ適切な措置。
- 従業者には理事や派遣労働者を含む。
- 規定の整備と公表。
- 組織体制の整備(CPO, 委員会)。
- 一定期間毎の監査。(必要に応じて外部監査)
- 問題発生時の報告連絡体制。苦情処理との連携。
- 雇用契約、就業規則での個人情報保護規定の整備。
- 派遣労働者を含めて教育研修の実施。
- 入退室管理、盗難の予防、機器・装置の物理的保護。
- アクセス管理、アクセス記録の保存、ファイアウォール。
- 媒体劣化の防止、検索可能性の維持。
- 不要な場合の復元不可能な破棄(機器も含む)。
- 医療情報システムに関しては別に指針を定める。

標準的電子カルテ推進委員会
中間論点整理メモ

＞ 電子カルテの現状と普及のための課題

＞ 課題解決に向けた検討の視点と方向性

標準的電子カルテ導入の目的や目標の明確化

標準的電子カルテ導入の効果を評価する方法の明確化

標準的電子カルテが備えるべき機能等

- ・ 個人情報保護の観点からのシステムの運用のあり方について、何らかの標準的な指針等を作成することが求められている。
- ・ 電子カルテシステムのセキュリティ基準を明確にし、特に医療の継続のための可用性の確保に関して具体的手法を含めた指針を示すとともに、前二項の対策と一体化した安全対策をとれるようにすることが求められている。

標準的電子カルテを普及させるために必要な基盤整備

＞ 論点検討にあたっての考慮すべき事項

サブワーキンググループの編成

電子保存・外部保存ガイドラインサブワーキング

電子保存および外部保存のガイドライン・解説資料の編集等
トレンドテクノロジーを押さえつつ、
医療現場の担当者が理解しやすい内容にする
既存のガイドラインの問題点の把握と方向性決定
実質的に診療情報システムの安全管理をカバー

PKI基本ポリシーサブワーキング

保健医療分野での認証基盤の整備に関連した、
認証局証明書ポリシー標準化やガイドライン等の作成
国際的な標準に準拠して作業を進める
当初は署名用ポリシーのみ

医療情報システムの安全管理のためのガイドライン

- > 1. はじめに
- > 2. 本ガイドラインの読み方
- > 3. 本ガイドラインの対象システムおよび対象情報
- > 4. 自己責任について
- > 5. 情報の相互利用性と標準化について
- > 6. 医療情報システムの基本的な安全管理
- > 7. 電子保存の要求事項について
- > 8. 診療録および診療諸記録を外部の保存する際の基準
- > 9. 診療諸記録をスキャナ等で電子化して保存する場合について
- > 10. 運用管理について
- > 付表1. 一般管理における運用管理の実施項目例
- > 付表2. 電子保存における運用管理の実施項目例
- > 付表3. 外部保存における運用管理の実施項目例

構成

- > A. 制度上の要求事項
法律・通知・他の指針など
- > B. 考え方
要求事項の解説および原則的な対策
- > C. 最低限のガイドライン
Aの要求事項を満たすためにかならず実施しなければならない事項
- > D. 推奨されるガイドライン
実施しなくても要求事項を満たすことはできるが、説明責任の観点から実施したほうが理解が得やすい対策

6. 医療情報システムの基本的な安全管理

- > A. 個人情報保護法
方針の制定、情報の把握、リスク分析
- > 組織的安全管理対策
B. ---、C. ---、D. ---
- > 物理的安全管理対策
B. ---、C. ---、D. ---
- > 技術的安全管理対策
B. ---、C. ---、D. ---
- > 人的安全管理対策
B. ---、C. ---、D. ---

脅威例

- > 診療情報システムに格納されている電子データ
権限のない者による不正アクセス、改ざん
権限のある者による不当な目的でのアクセス、改ざん
コンピュータウイルス等の不正なソフトウェアによるア
クセス、改ざん
- > 入力の際に用いたメモ・原稿・検査データなど

- > データを格納した可搬型媒体など

- > -----

技術的安全対策

- > B. 考え方
 - (1) 利用者の識別および認証
 - ・ 認証強度の考え方
 - ・ ICカード等のセキュリティ・デバイスを配布する場合の留意点
 - ・ バイオメトリックスを利用する場合の留意点
 - (2) 情報の区分管理とアクセス権限の管理
 - (3) アクセスの記録
 - (4) 不正ソフトウェア対策

技術的安全対策

> C. 最低限のガイドライン

- (1) 利用者の識別および認証
- (2) 動作確認等での漏洩への留意
- (3) 職種による権限の設定とアクセス管理
- (4) アクセスの記録と定期的な確認
- (5) 時刻情報の要件
- (6) ウイルスなどの不正ソフトウェア対策

> D. 推奨されるガイドライン

- (1) 情報の区分管理、区分単位でのアクセス管理
- (2) ウイルスなどの不正ソフトウェアの対策の実効性の確認
- (3) 離席の場合のクローズ処理

6. 医療情報システムの基本的な安全管理

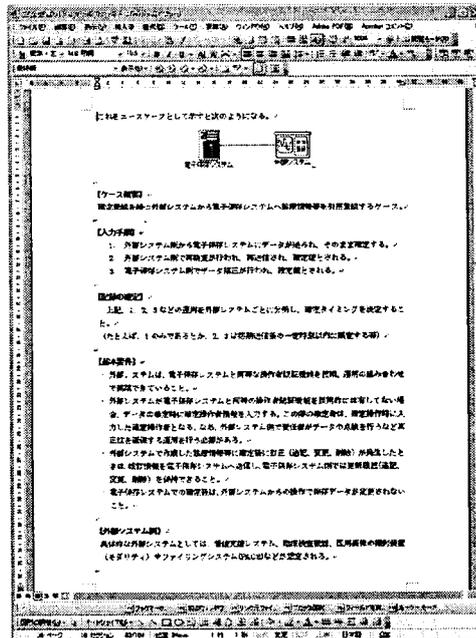
> 人的安全管理対策

- 従業者に対する人的安全管理対策
- 委託事業者に対する人的安全管理対策

> 情報の破棄

> システムの改造・保守

7. 電子保存の要求事項について



19

8. 外部に保存する際の基準

＞ 外部保存を受託する施設の限定

医療機関・医療法人等が適切に管理する場所

行政機関等が開設したデータセンター等

危機管理上の目的のために医療機関等が外部に自らが所有する機器を用いて保存する場合

20

9 E文書法への対応

- 都度発生する書面(フィルム)のスキャン原則は可。

技術的に診療に差し支えない精度。

文書は300DPIフルカラーレスキャナ

日本医学放射線学会電子情報委員会の指針

電子署名による責任の所在の明確化。

- すでに蓄積された書面(フィルム)のスキャン原則は不可。

技術的に診療に差し支えない精度。

電子署名等による責任の所在の明確化。

計画から監査まで第三者監査に相当する

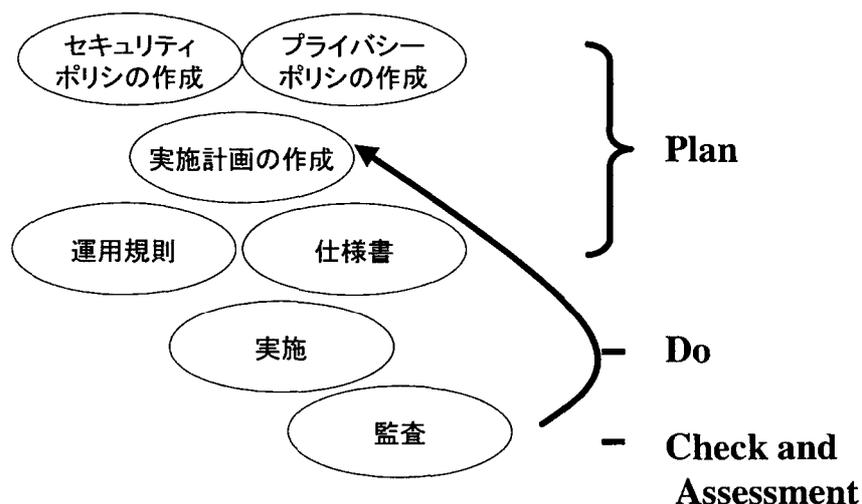
厳格な監視。

項目	実施内容	実施場所	実施時期	実施責任者	実施状況	実施結果
1	1. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
2	2. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
3	3. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
4	4. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
5	5. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
6	6. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
7	7. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
8	8. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
9	9. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
10	10. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
11	11. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
12	12. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
13	13. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
14	14. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
15	15. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
16	16. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
17	17. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
18	18. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
19	19. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		
20	20. 文書管理の現状を把握し、必要に応じて改善策を講ずる。	院内	随時	院長		

付表

- > 1. 運用管理項目
安全管理上の要求事項で多少とも運用的対策が必要な項目
- > 2. 実施項目
上記管理項目を実施レベルに細分化したもの
- > 3. 対象
医療機関の規模の目安
- > 4. 技術的対策
技術的に可能な対策、ひとつの実施項目に対して選択可能な対策を列挙した
- > 5. 運用的対策
4. の技術的対策をおこなった場合に必要な運用的対策の要約
- > 6. 運用管理規程文例
運用的対策を規定に記載する場合の文例

セキュリティとプライバシー保護の実現方法



PDCAサイクル（通常ポリシーは参照されるだけ）