患者に優しい個人情報保護

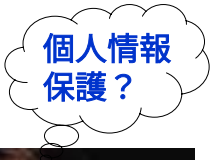
東京工業大学　像情報工学研究施設
IT都市創造（NTTコミュニケーション）工学
寄附研究部門
特任教授　喜多　紘一

（2005年2月26日　第3回　IHE　ワークショップ　in　札幌）

何か気になる、何で騒ぐのだろう

個人情報保護法が2005年4月に施行される耳にしたけれど、
個人情報を保護すればよいのだから、個人情報を洩れなくすればよいのだろう！

それなら医療機関は、すでに守秘義務を守っているし、
コンピュータの正確性･安全性にも配慮しているから特に問題ない、
特に4月を気にすることはない、
自分の病院は特に新規に対応する必要はない、問題ない筈・・・・・。



でも、新聞や仲間から洩れ聞くところに寄れば、
何か同意をとらないといけないとか、
利用目的を明確にしろとか、
目的外の利用はダメとか、
要求があったら開示しなくてはならないなんて
聞こえてくるけど、これは何なんだろう、
自分のところはどうしたらよいのだろう、
なんて不安になってきておられるところもあるのではないでしょうか。

個人情報を保護するには守秘義務だけではなく新観点による作業が必要！

個人情報保護法

（個人情報の保護に関する法律（平成十五年法律第五十七号））

第一章 総則（第一条－第三条）（目的）（定義）（基本理念）
第二章 国及び地方公共団体の責務等（第四条－第六条）
第三章 個人情報の保護に関する施策等
　第一節　個人情報の保護に関する基本方針（第七条）
　第二節　国の施策（第八条－第十条）
　第三節　地方公共団体の施策（第十一条－第十三条）
　第四節　国及び地方公共団体の協力（第十四条）
第四章　個人情報取扱事業者の義務等
　第一節　個人情報取扱事業者の義務（第十五条－第三十六条）
　第二節　民間団体による個人情報の保護の推進（第三十七条－第四十九条）
第五章　雑則（第五十条－第五十五条）
第六章　罰則（第五十六条－第五十九条）
附則

第四章第一節
個人情報取扱事業者の義務

- （利用目的の特定）
- （利用目的による制限）
- （適正な取得）
- （取得に際しての利用目的の通知等）
- （データ内容の正確性の確保）
- （安全管理措置）
- （従業者の監督）
- （第三者提供の制限）
- （委託先の監督）
- （保有個人データに関する事項の公表等）
- （開示）
- （訂正等）
- （利用停止等）
- （理由の説明）
- （手数料）
- （報告の徴収）
- （勧告及び命令）
- （主務大臣の権限の行使の制限）
- （主務大臣）

個人情報保護のパラダイム･シフト

医療スタッフの
コントロール

患者の
コントロール (利用目的･･･)

個人情報保護法施行前

個人の守秘義務

個人情報保護法施行後

個人情報取扱業者の義務

パラダイム･シフトの背景

- 一人にしておかれる権利

  1890年代の米国

  ←ゴシップ記事が背景

- 自己に関する情報の流れを自身でコントロールする権利

  1980年ＯＥＣＤ　ガイドライン

  ←　情報･ネットワーク技術の進展が背景

個人情報保護法の背景

- ＯＥＣＤプライバシーガイドラインの採択：1980.9
  「プライバシー保護と個人データの国際流通 についてのガイドラインに関する理事会勧告」
  - 情報の自由な流れとプライバシー保護の調和
  - ＯＥＣＤ8原則

- ＥＵ指令の採択：1995.10、98年10月発効
  「個人データ処理に係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州会議及び理事会の95/46/EC指令」
  - ＥＵ域外への個人データの移転禁止（第２５条）
  - 第三国にもＥＵ諸国と同等の「十分なレベルの保護措置 adequate level of protection」を求める

わが国の取り組み

- 1997.3 ： METI個人情報保護ガイドライン(改訂)
  → 業界ガイドライン
- 1998.4 ： JIPDECプライバシーマーク制度
- 1999.3 ： ｺﾝﾌﾟﾗｲｱﾝｽ･ﾌﾟﾛｸﾞﾗﾑ要求事項の JIS 化
- 1999.8 ：「住民基本台帳法の一部を改正する法律」公布「附則第１条第２項:この法律の施行に当たっては、政府は、個人情報の保護に万全を期するため、速やかに、所要の措置を講ずるものとする。」住民基本台帳カードは、2003年8月の運用開始
- 2003.5 ： 個人情報の保護に関する法律

OECD8原則

利用目的

③目的明確化の原則

収集目的を明確にし、収集目的に合致したデータ利用

収集したデータの目的外に利用禁止

①収集制限の原則

適法・公正な手段、情報主体に通知または同意を得て収集

④利用制限の原則

適切管理

⑤安全保護の原則

紛失・破壊・使用・修正・開示等から保護

②データ内容の原則

利用目的に沿い正確・完全・最新

実施管理

データの管理者は諸原則実施の責任

⑧責任の原則

⑥公開の原則

実施方針、データの存在、利用目的、管理者の公開

データの所在及び内容の確認、異議申立

⑦個人参加の原則

第四章第一節 個人情報取扱事業者の義務

- (利用目的の特定)
- (利用目的による制限)
- (適正な取得)
- (取得に際しての利用目的の通知等)
- (データ内容の正確性の確保)
- (安全管理措置)
- (従業者の監督)
- (第三者提供の制限)
- (委託先の監督)
- (保有個人データに関する事項の公表等)
- (開示)
- (訂正等)
- (利用停止等)
- (理由の説明)
- (手数料)
- (報告の徴収)
- (勧告及び命令)
- (主務大臣の権限の行使の制限)
- (主務大臣)

プライバシーマーク制度

個人情報保護JIS Q 15001に適合したコンプライアンス・プログラムを整備し、個人情報の取扱いを適切に行っている事業者を、第三者機関であるJIPDEC（及びその指定機関）が評価・認定し、その証としてプライバシーマークと称するロゴの使用を許諾する制度。

プライバシーマーク制度

目　的

医療機関には：
個人情報の保護に関する信頼獲得へのインセンティブを提供
→ 個人情報保護システムの確立促進

患者には：
事業者の個人情報の取扱いの適切性を容易に判断できる材料（マーク）を提供
→ 個人情報を自分で守る意識の向上

プライバシーマーク取得の意義

- 個人情報保護はこれからの病院経営者の義務
  - 2005年4月1日実施
  - 特定の個人の数が5千以上／6ヶ月のいづれの日
  - 守秘義務のみではない。(利用目的・公開等)
  - コントロール権(目的外使用禁止・開示)
  - 説明責任
- 個人情報保護は電子カルテ導入と両輪
- 個人情報保護法施行で情報活動を狭めない：ルールを明確にし、収集・活用しやすくする
- プライバシーマーク取得は個人情報保護法対応へのよりどころ
- 取得活動による業務フローの改善と職員の活性化

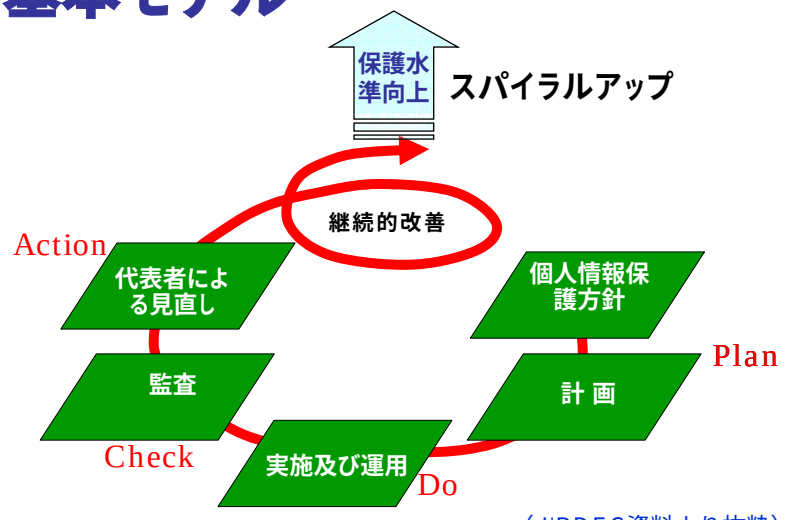
プライバシーマーク付与の効果

- 個人情報保護の動きへの対応
  - 「私的自由、私生活、人目をさけること」の意識からの切替
  - 中待合室・6人部屋をなくすことのみではない
- 電子カルテ導入で社会的・経済的損失を防ぐために必須
- 自分の情報を誰が知っているのかに対する説明
- 患者さんの治療に対する積極的参加意識
- 診療スタッフの患者情報に対する意識向上
- 情報管理の明確化と業務改善
- 情報管理レベルの向上

JIS Q 15001と個人情報保護法の関係

比較項目	Pマーク制度	個人情報保護法
個人情報保護方針	○	
計画	○	
体制及び責任	○	
個人情報の収集に関する措置収集の原則	○	○
個人情報の利用及び提供に関する措置	○	○
個人情報の適正管理義務	○	○
個人情報に関する情報主体の権利	○	○
教育	○	
苦情及び相談	○	○
監査	○	
事業者の代表者による見直し	○	

JIS　コンプライアンス・プログラムの基本モデル



（JIPDEC資料より抜粋）

個人情報保護法との関連

- プライバシーマーク制度はJIS15001に沿って2面を審査
  - 現在の保護レベルが適切か
  - PDCAを継続できる体制にあるか
- 個人情報保護法はDoの目標を記述
- 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」はPDCAも記述

コンプライアンス・プログラム要求事項（JIS Q 15001）

- 一般要求事項　（CPの作成・規程化）
- 個人情報保護方針（基本方針）
- 計画　（Plan）
- 実施及び運用　（Do）
- 監査　（Check）
- 見直し　（Action）

計画（Plan）

- 個人情報の特定（手順の確立とリスクの認識
- 法令及びその他の規範
- 内部規定
- 計画書

実施・運用（Do）

- 体制及び責任
- 個人情報の収集に関する措置
- 個人情報の利用及び提供に関する措置
- 個人情報の適正管理義務
- 個人情報に関する主体の権利
  （開示・訂正・削除・拒否）
- 教育
- 苦情及び相談
- コンプライアンス/プログラム文書
- 文書管理

監査/見直し（Check&Action）

- 監査
- 事業者の代表による見直し

JIS Q 15001 の要求事項一覧

1．適用範囲
2．引用規格
3．定義
4．コンプライアンス・プログラムの要求事項
4.1 一般要求事項
4.2 個人情報保護方針
4.3 計画
4.4 実施及び運用
4.4.1 体制及び責任
4.4.2 個人情報の収集に関する措置
4.4.2.1 収集の原則
4.4.2.2 収集方法の制限
4.4.2.3 特定の機微な個人情報の収集の禁止
4.4.2.4 情報主体から直接収集する場合の措置
4.4.2.5 情報主体から間接的に収集する場合の措置
4.4.3 個人情報の利用及び提供に関する措置
4.4.4 個人情報の適正管理義務
4.4.5 個人情報に関する情報主体の権利
4.4.6 教育
4.4.7 苦情及び相談
4.4.8 コンプライアンス・プログラム文書
4.4.9 文書管理
4.5 監査
4.6 事業者の代表者による見直し

医療機関の認定指針の構成

- A．JIS Q 15001の要求事項
- JIS Q 15001の要求事項を原文通りに記載し、四角の枠で囲んでいる。
- B．医療機関としての解釈
- 医療機関にJIS Q 15001を適用する場合の要求事項の解釈を記載している。
- C．最低限のガイドライン
- 最低限実施しなくてはならない方策の指針を記載している。
- D．推奨されるガイドライン
- 最低限のガイドラインに医療機関の実情を配慮し、追加した方が望ましい方策を含めた指針を記載している。

コンプライアンス・プログラム実現のステップ

1：個人情報保護方針を定め文書化
2：ＣＰ策定のための組織の発足
3：ＣＰ策定の作業計画の立案
4：個人情報保護方針を組織内に周知
5：個人情報の特定
6：既存の個人情報取扱いシステムの評価
7：ＣＰの構成の検討
8：ＣＰの基本となる規程の策定
9：ＣＰの詳細規程の策定
10：ＣＰの文書化
11：ＣＰに準じた体制の整備
12：ＣＰを周知するための研修の実施
13：ＣＰの運用状況の監査
14：ＣＰの改善の実施

個人情報保護方針

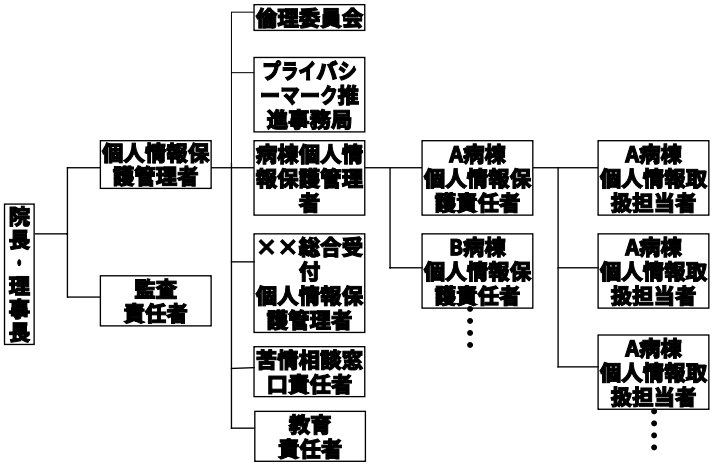
a) 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること。

b) 個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること。

c) 個人情報に関する法令及びその他の規範を遵守すること。

d) コンプライアンス・プログラムの継続的改善に関すること。

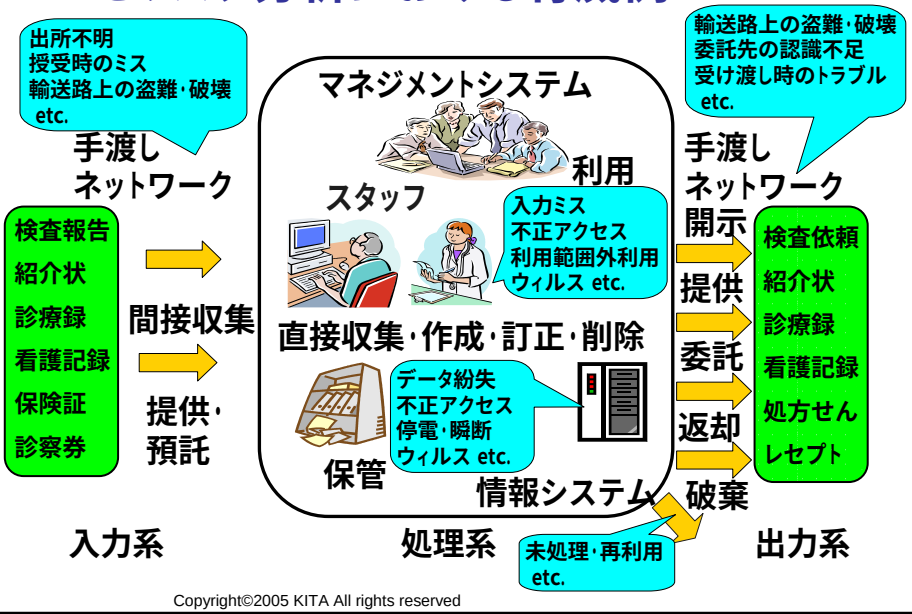
ＣＰ策定のための組織作りとＣＰ運用の体制



医療機関における個人情報を含む書類の例

診察申込書	検査依頼伝票	請求書／領収書
保険証	検査結果報告書	薬歴情報
紹介状	ー生化学検査	退院証明書
診察券	ー生理検査	院療養計画書
予約票	ー超音波検査	手術管理情報
入院申込書	ー内視鏡検査	給食管理情報
入院療養計画書	ー放射線検査	行政官庁への報告
診療録	看護記録	のための各種届出書等
処方せん	レセプト	

医療機関における個人情報の特定とリスク分析における脅威例



脆弱性に対する対策例

- 保管
  - アクセス制限
  - ユーザ認証
  - 鍵管理
  - 記録, ログ
  - バックアップ/リカバリ
  - 電子保存の基準遵守
  - 災害管理
- 提供・預託
  - 出所確認
  - 受け渡しエリアの確保
  - 輸送路上の注意
  - 授受記録
- 委託・返却
  - 輸送路上の注意
  - 授受記録
- 処理・利用
  - 正確性の確認
  - 利用範囲の確認
  - ユーザ認証
  - アクセス制限
  - 入退出管理
- 破棄
  - 破棄確認
  - 再利用時の確認

(JIPDEC資料より抜粋・追加)

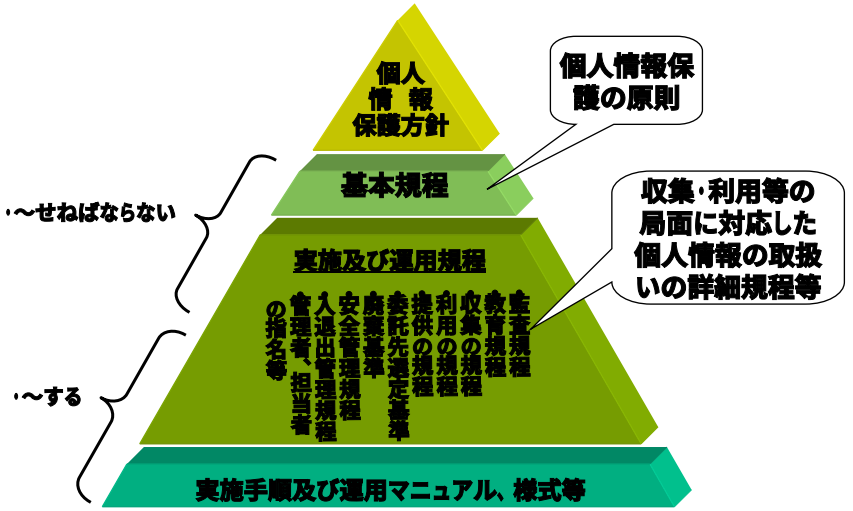
個人情報特定の例

業務	情報資産	個人情報	入手先	入手形態	取扱経路	情報の形態	処理内容 (利用目的	保管場所	保管期間	提供先	提供経路	廃棄方法
放射線部業務	検査依頼書	氏名 生年月日	依頼科	紙	患者持参	紙	撮影指示 (診療)	撮影台 保管棚	3年	自部門		溶解
	撮影画像	氏名 病態画像	自部門	デジタル	診断機器	デジタル	撮影 (診療)	サーバ	3年	依頼科	院内ネット	disk 消去
	読影レポート	氏名 診断名										
	照射録											

リスク分析の例

業務	情報資産	資産価値（損失）	脅威	現状の対策	脆弱性	現状のリスク	追加対策	対策後の残存リスク	対策後の規定番号
放射線部業務	検査依頼書								
	撮影画像								
	読影ポート								
	照射録								

規程の階層構成



（JIPDEC資料より抜粋）

規定作成の留意事項

- 業務の文書化は慣れていないのでスキルが必要
- 一律でなくても良い（法令・ガイドライン遵守以外は医療機関のポリシーによる）
- ポリシーを決めて公開
- 誰でも場面に応じ同じ行動
- 倫理委員や個人情報保護責任者の活用（独断で決定しない）

収集する場合は情報主体から以下の同意必要

a）医療施設の内部の個人情報に関する管理者名、所属、連絡先

b）収集目的（診療・経営・診療報酬請求・研究・教育）

c）提供：個人情報の提供目的、当該情報の受領者、個人情報の取扱いに関する契約の有無

d）個人情報の預託を行うことの予定（外注検査・診療報酬計算の外注）

e）情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に生じる結果

f）個人情報の開示を求める権利、当該情報の訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法

利用及び提供の原則

- 個人情報の利用及び提供は、情報主体が同意を与えた収集目的の範囲内で行わなければならない
- 診療・医学教育・病院管理・各種報告・支払い請求・福祉への協力・介護保険関連・外部からの照会等に対する各医療機関としてのポリシーの規程化

個人情報の適正管理義務

- 個人情報の正確性の確保

  個人情報は、収集目的に応じ必要な範囲内において、正確、かつ、最新の状態で管理しなければならない。

- 個人情報の利用の安全性の確保

  個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなど）に対して合理的な安全対策を講じなければならない。

適正管理の留意事項

- 個人情報の特定（伝票単位）
- リスク分析（ワークフロー分析）
- 出来心を芽生えさせない
- 裁判での説明責任（ガバナンス・監査証跡）
- 作業マニュアルレベルでの規定

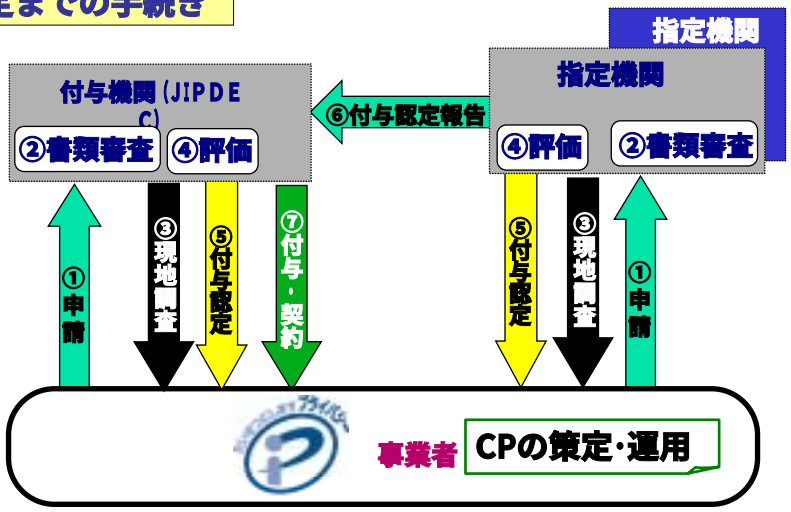
教育・監査・苦情処理・見直し

- 定期的フォロー体制
- 臨時事項に対する対応

プライバシーマーク制度

JISA（情報サービス産業協会）
JMRA（日本ﾏｰｹﾃｨﾝｸﾞ・ﾘｻｰﾁ協会）
JJA（全国学習塾協会）
MEDIS-DC（医療情報システム開発センター

認定までの手続き



プライバシーマーク制度

認定に係る費用2004年12月より改定

	規模別料金（消費税別）		
	小規模	中規模	大規模
申請手数料	50,000	50,000	50,000
審査料	200,000	450,000	950,000
使用料	50,000	100,000	200,000
合計	300,000	600,000	1,200,000

この他、現地調査に係る旅費、宿泊費を請求

1．大規模事業者：中規模事業を超える事業者
2．中規模事業者：資本金、従業員数何れか一方を満たす事業者

	製造業その他	卸売業	小売業	サービス業
資本金	3億円以下	1億円以下	5千万円以下	5千万円以下
従業員	300人以下	100人以下	50人以下	100人以下

3．小規模事業者：常時使用する従業員数が20人以下（商業、サービス業は5人以下）

プライバシーマーク制度

審　査

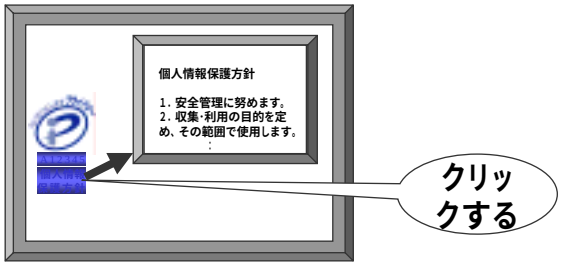
1. **書類審査（JISへの適合性）**
   - ①個人情報保護組織の整備
   - ②研修の規定・計画・実施
   - ③監査の規定・計画・実施
   - ④消費者相談窓口の設置
   - ⑤安全管理の措置
   - ⑥外部委託の基準、保護に関する契約
2. **現地調査（半日程度）**
   - ①経営課題としての認識
   - ②全社的取組みの姿勢
   - ③運用状況（エビデンスによる確認）

プライバシーマーク制度

マークの使用

①有効期限：使用契約 による2年間の使用（更新で継続）
②マークの活用：
　＊店頭　＊契約約款　＊マニュアル　＊広告
　＊封筒　＊レターヘッド　＊名刺　＊ホームページ　etc.

【ホームページで利用する場合】



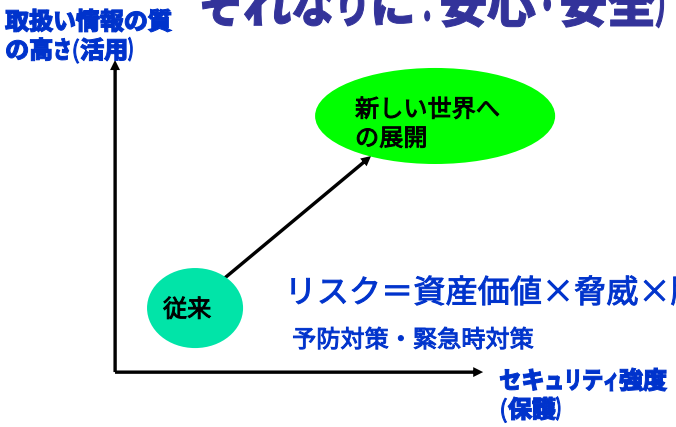
プライバシーマーク付与として適切な体制

- 同意された利用目的の範囲内で利用し保護しているか気をつけている
- あらたに取扱が発生した個人情報を見逃さない
- 患者さんが自分の個人情報の扱いに関心をもち、主体的に診療に参加している
- 上記行動が診療マネージメントに貢献している

保健医療分野のプライバシーマーク付与認定事業者一覧（2004.10.21）

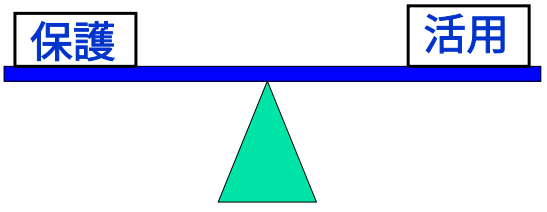
- 医療法人財団　河北総合病院 (JIPDEC)
- 医療法人医誠会　城東中央病院 (JIPDEC)
- （有）コンピュータ・プロダクティビティ・サポート
- （財）日本予防医学協会
- （株）コンピュータービジネス
- 人材派遣健康保険組合
- (社)半田市医師会
- セントケア（株）
- （株）オムニカルテ社

個人情報保護≠情報の塩漬け
⇒情報の活用（利用して欲しいヒトは それなりに：安心・安全）



ハイリスク／ハイリターン⇒許容リスク／ハイリターン

バランスとグレーゾーン



個益と公益

例外事項として判断が必要

(安易にて起用しない：ルール化)

- 法令に基づく場合
- 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- 当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合
- 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合
- 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必　要がある場合であって、当該事務の遂行に支障を及ぼすおそれがあるとき。
- 取得の状況からみて利用目的が明らかであると認められる場合

医療情報の可用性の確保

- 医療情報はアベイラビリティ（可用性）が重要
- 緊急時のマニュアル化が必要
- ガラスブレーク
- 生命維持を優先・後処理で対応

個人情報が保護されないと
(漏洩による2次的被害:目的外利用)

- 不特定多数情報
  - 売り込み、勧誘、脅迫
  - 情報を寄せられ活用・売却・不正アクセス
- 特定個人の情報
  - VIP情報
  - 本人に一生の打撃・影響
  - 差別・・・・後ろめたい？　社会の進歩？　誤情報？
  - 活動の制約・・・・正義の味方？ (エネミー・オブ・アメリカ)
  - 不特定の敵の目にさらされる・・・死亡広告・テロ
- 社会的活動損失
  - アンフェアー・評価に偏り
  - 情報活用に制限 (有効なシステムが構築できない)
  - 組織の評価が下がる・・・・損害賠償責任

個人情報が保護されないと
(患者安全と情報の信頼性)

- 患者安全 (CIAの確保)
  - Confidentiality (機密性)
  - Integrity (完全性)
  - Availability (可用性)
- 信頼性 (真正性:不改ざん＋責任の所在)
  - 証拠力・証明力
  - Autheticity
  - accountability

IHE-Radiology

- **Basic Security（SEC）**
  - セキュア・ノードアクターが既存のアクターとペアーでユーザ認証、ノード認証、監視レコードの送付動作
  - 個人情報保護への対応を支援する、個人情報へのアクセスの記録（何時、誰が、何処で、誰の情報にアクセスしたか）を行うための技術的手段を提供

- **Portable Data for Images（PDI）**
  - CD-Rなどの外部媒体に画像やレポートをDICOMオブジェクトとしての格納や、DICOM以外の標準に準拠したオブジェクトとしての格納。ネットワークを経由しない情報の相互運用が保証
  - 個人情報保護としては画像・レポートの開示の際に利用可能

- **Patient Information Reconciliation (PIR)**
  - 未確認(身元不明)の患者または確認できなかった患者の収集済み画像を患者の受診・オーダ・来歴と照合するための手段を提供。
  - こうした患者の確認は個人情報保護上も正確性を担保する上で重要。意識回復後や家族からの情報収集等なにをもって照合するか、又、どう照合したかの記録をとるなど医療機関で規定化しておくことが必要。

個人情報保護とIT Infrastructureの関係

- **個人情報保護に利用できる統合プロファイル**
  - EUA （「病院全体でのユーザ認証」(Enterprise User Authentication）：Single Sign On
  - CT （「システム全体での時間合わせ」Consistent Time)
  - ATNA（「監査証跡とノード認証」(Audit Trail and Node Authentication)

- **その他のプロファイル**
  - RID「表示のための情報取得」(Retrieve Information for Display)
  - PIX「患者ID情報の相互参照」(Patient Identifier Cross-referencing)
  - PSA「アプリケーション間の患者IDの連動」(Patient Synchronized Applications)
  - PWP「個人別診療情報ディレクトリ」(Personal White Page)
  - PDQ「患者情報問い合わせ」(Patient Demographics Query)
  - XDS 「電子カルテの施設間連携利用」(Cross-Enterprise Clinical Document Sharing、)

  利用目的、情報の連携やアクセス可能者に対し患者の同意が取られているか、認証は確実か、正確性が担保されるか確認。
  プロファイルを使用する仕組みおよびその規定化が必要

- **今後まとめられることが期待されるプロファイル**
  - ATNAのXDSへの拡張
  - 同意の確認
  - 権限管理やアクセス制御ポリシーに関するプロファイル等

システム開発者の留意事項

- 開発･保守時を含め個人情報保護を意識したシステムを開発する
  - 技術的対策と組織的対策を明確に説明
  - 極力個人情報を減らす
  - デモ用･トレーニング用プログラムに注意
  - 予防対策と緊急対策のバランス
  - ネットワーク基盤検討会の動向に注目（外部保存？）
- 開発時はできるだけ擬似データを用いる
- 生データをシステム確認に用いる場合はアクセス者を制限し、記録を残し、使用後直ちに返却、または破棄する
- 個人情報取扱規定を作成･周知させる。

システム保守の場合の留意事項

- 保守先の個人情報保護規程に従う
- 保守先の了解、監視の下に保守をおこなう
- 社内にデータを持ち込む場合はアクセス者を制限し、記録を残し、使用後直ちに返却、または破棄する
- 生データはアクセス者を制限し、記録を残し、使用後直ちに返却、または破棄する
- 説明責任を果たせるように

セキュリティ評価制度

- プライバシ-マーク制度（JIS Q 15001）
  - JIS Q 15001に適合して電子計算機処理に係る個人情報の適切な保護のための体制を整備している事業者に対し、その申請に基づきその旨の認定及びその旨を示す特別の表示であるプライバシーマークの付与を行う制度。
- 情報セキュリティマネジメントシステム適合性評価制度（ISMS：ISO／17799）
  - 組織が保護すべき情報資産について、技術的なセキュリティ対策だけではなく、人間系の運用・管理面のセキュリティ対策などを含めたセキュリティ管理に対する第三者適合性評価制度
- 情報セキュリティ監査制度（ISO／17799）
  - リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から、国際的にも整合性の取れた基準に従って検証または評価し、保証を与えあるいは助言を行う制度
- セキュリティ評価・認証（ISO／15408）
  - 情報システムやそれを構成する機器・ソフトについて、セキュリティ機能全般および目標とするセキュリティレベルをある評価基準に基づいて評価し、その結果を認証する制度