

～今さら聞けない？ まだ知らない??～

個人情報保護法 基本の“き” Stage.1



医療の世界では、守秘義務は当然の義務として存在していた

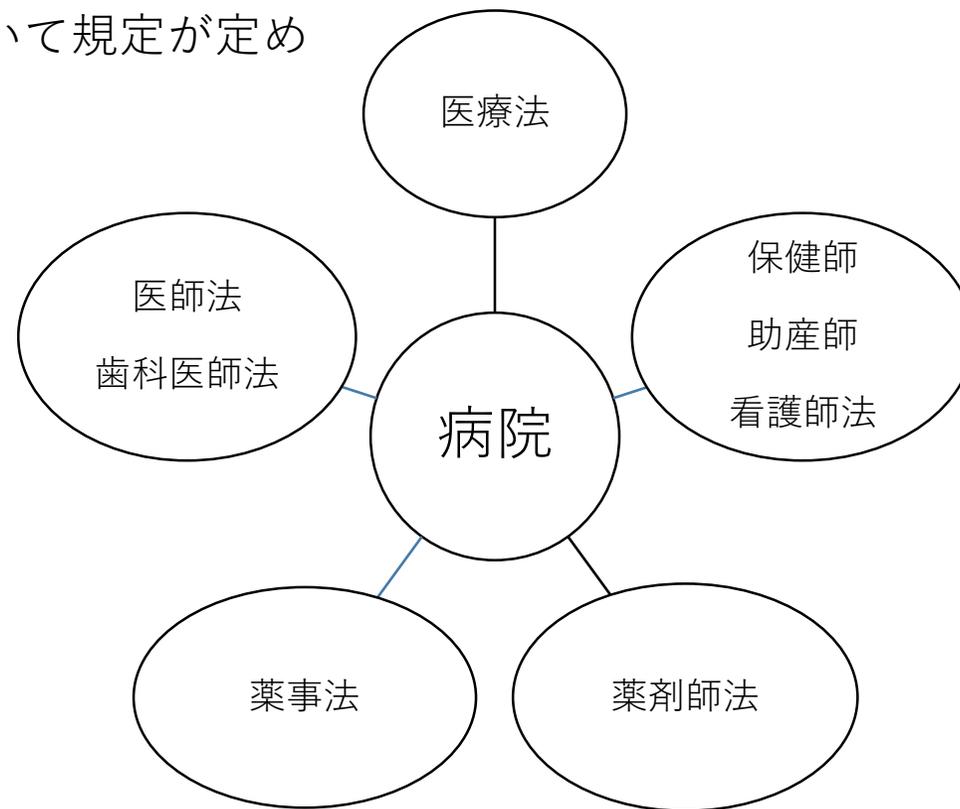
守秘義務を守る、いわゆる“プライバシーの尊重”は、従来から医療の様々な場面における基本だった。



病院を取り巻く様々な法律や規則では、『守秘義務』について規定が定められている。

ヒポクラテスの誓い（抜粋）

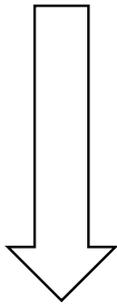
- 7.いかなる患家を訪れるときも、それはただ病者を利益するためであり、あらゆる勝手な戯れや墮落の行いを避ける。女と男、自由人と奴隷の違いを考慮しない。
- 8.医に關すると否とに關わらず、他人の生活についての秘密を守る。



個人情報保護法ができた背景

🔗 個人情報保護法が整備された背景には、インターネットやメールなどを使用した国際的なデータ流通の本格化に伴い、国によって異なる制度が世界的な情報流通の阻害要因として認識されたことに端を発している。

個人情報の取り扱いに起因する、個人の権利・利益侵害に対する不安、懸念等を払拭するために制度が整備された。



2005年（平成17年）に個人情報保護法が全面施行されたことを受けて、医療機関でも改めてプライバシー尊重と個人情報保護が問い直されることになった。

守るべき4つの基本ルールと主な用語の定義

【守るべき4つの基本ルール】

1. 個人情報の取得・利用
2. 個人データの安全管理措置
3. 個人データの第三者提供
4. 保有個人データの開示請求

【主な用語の定義】

- 一. 「個人情報」 …個人情報とは、生存する個人に関する情報であって、氏名や生年月日等により特定の個人を識別することができるものをいう。また、他の情報を容易に照合することができ、これにより特定の個人を識別することができることとなるものも含まれる
- 二. 「個人識別符号」 …その情報だけでも特定の個人を識別できる文字、番号、記号、符号をいう。例えば、公的な番号としてのパスポート番号、基礎年金番号、マイナンバー、各種保険証等
- 三. 「個人情報データベース等」「個人データ」「保有個人データ」
…個人情報をデータベース化したり、検索可能な状態にしたものを「個人情報データベース等」といい、これを構成する情報を「個人データ」という。個人データのうち、事業者に修正、削除等の権限があるもので、6か月以上保有するものを「保有個人データ」という

4つのルール 1. 個人情報の取得・利用

【概要】

個人情報取扱事業者は、「個人情報を取り扱うにあたって、利用目的をできる限り特定しなければならない」とされている（個人情報保護法第15条第1項）。なお、利用目的は、できるだけ具体的に特定すること。また、特定した利用目的は、あらかじめ公表しておくか、個人情報を所得する際に本人に通知する必要がある。

取得した個人情報は、特定した利用目的の範囲内で利用する必要があり、これ以外のことを使用する場合は、あらかじめ本人の同意を得なければならない（個人情報保護法第16条第1項）

=Point=

個人情報を書面で取得する場合は、利用目的を本人に明示する必要がある（個人情報保護法第18条第2項）。なお、取得の状況からみて、利用目的が明らかである場合は、通知・公表の必要はない（個人情報保護法第18条第4項第4号）。

4つのルール 2. 個人データの安全管理措置

【概要】

個人情報取扱事業者は、「個人データの安全管理のために、必要かつ適切な措置を講じなければならない」とされている（個人情報保護法第20条）。

=Point=

個人データの適正な取り扱いの確保に、組織として取り組む必要がある。取り扱いに関する基本方針や個人データの取り扱いに係る諸規定の策定が有効。

区分	概要
組織的安全管理措置	組織体制整備、個人データ取扱いに係る諸規定に従った運用、漏洩等の事案に対応する体制の整備
人的安全管理措置	従業員への教育
物理的安全管理措置	機器及び電子媒体等の盗難等の防止策、電子媒体等を持ち運ぶ場合の漏洩等の防止
技術的安全管理措置	外部からの不正アクセスの防止等

2-1. 個人データの安全管理措置の特例

従業員の数が100人以下の小規模事業者に対しては、事業が円滑に行われるための配慮から、ガイドラインにおいて特例的な対応方法が示されている。

区分	概要
組織的安全管理措置	個人情報取り扱いの基本的なルールを決める
人的安全管理措置	従業員への教育
物理的安全管理措置	紙で管理している場合は、鍵のかかる引き出しに保管する PC等で管理している場合は、ファイルにパスワードを設定する
技術的安全管理措置	PC等で管理している場合は、ファイルにパスワードを設定する PCにセキュリティ対策ソフトウェアを導入する



4つのルール 3. 個人データの第三者提供

【概要】

個人情報取扱事業者は、「個人データを第三者に提供する場合、原則として、あらかじめ本人の同意を得なければならない（個人情報保護法第23条第1項）」。また、「第三者に個人データを提供した場合は、一定事項（いつ、誰の、どんな情報を、誰に等）を記録する必要がある（個人情報保護法第25条、26条）。ただし、以下のような場合は例外的に、第三者提供の本人同意は不要。

- ▶法令に基づく場合（例：警察、裁判所、税務署等からの照会）
- ▶人の生命・身体・財産の保護に必要（本人同意取得困難「例：災害時の被災者情報の家族・自治体等への提供」）
- ▶公衆衛生・児童の健全育成に必要（本人同意取得が困難「例：児童生徒の不登校や、児童虐待のおそれのある情報の関係機関での共有」）
- ▶国の樹可能の法令の定める事務への協力（例：国や地方公共団体の統計調査等への回答）

4つのルール 4. 保有個人データの開示請求

【概要】

個人情報取扱事業者は、「本人から保有個人データの開示請求を受けたときは、本人に対し、原則として当該保有個人データを開示しなければならない（個人情報保護法第28条）」。また、個人情報の取扱いに関する苦情等には、適切かつ迅速に対応するよう努めることが必要（個人情報保護法第35条）。

=Point=

次の①～⑤については、「本人が知り得る状態」においておく必要がある。

①事業者の名称 ②利用目的 ③請求手続き ④苦情申出先 ⑤加入している認定個人情報保護団体の名称・苦情申出先（加入している場合のみ）

信頼関係の構築・事業活動に対する社会の信頼を確保するためには、「個人情報保護を推進するうえでの考え方や方針（プライバシーポリシー等）を策定・公表しておくことが有効。

整理

平成29年（2017年）5月30日から、個人情報保護法の改正が全面施行された。この背景には、情報通信技術の発展や、事業活動のグローバル化等の急速な環境変化があげられる。

改正前は、5,000人以下の個人情報しか有しない中小企業・小規模事業者は適用対象外となっていたが、法改正によりこの規定は撤廃。個人情報を取り扱う「すべての事業者」に、個人情報保護法が適用されることとなった。なお、ここでいう「事業者」は法人に限らず、例えばマンションの管理組合やNPO法人、自治会や同窓会といった非営利組織も含まれている。

今回は、今回基本として挙げた4つのルールを、それぞれ医療機関に充当させて「内容及び例外規定等の確認」をしていきたいと思う。また、医療機関でありがちな失敗例や個人情報保護、および適切なプライバシー保護が医療安全に与える影響についての考察を行う。

参考資料・文献

- 個人情報保護法ハンドブック 「個人情報保護委員会」
- 個人情報保護委員会Webサイト
<http://www.ppc.go.jp/>
- 病院管理の手引き 「東京都福祉保健局医療政策部医療安全課（平成27年3月発行版）」

