「医療情報システムの安全管理に関するガイドライン」とは

「医療情報システムの安全管理に関するガイドライン」は、個人情報の中でも厳重な保護が必要とされる患者の電子カルテなどの医療情報を適切に管理するために国が定めたガイドラインです。
ガイドラインの対象となるのは、医療機関などで電子的な医療情報の取り扱いに関わる責任者ですが、医療情報共有の裾野が広がる中、ヘルスケアに携わる方に一度は目を通していただきたい情報をまとめました。
このガイドラインは、患者さんの個人情報を守るための基礎知識でもあり、個人情報保護法、e-文書法、医療法、医師法等を根拠として作成されています。

患者ファーストの視点で医療情報システムの安全性を確保

インターネットでさまざまな情報が収集され利活用される時代。電子カルテをはじめとした医療情報を活用したシステムも発展を続け、患者にとっての利便性を高めるとともに医療の質を高めることに貢献しています。近年では、一般診療所や歯科診療所、病院、さらに助産所、薬局、介護事業者などとも医療情報を

連携することで「患者中心のヘルスケア」の質を高める取り組みも広がっています。

しかし近年、ソーシャルネットワークやネット通販などさまざまな情報サービス事業において、システムの脆弱性を突いた事件が起きていることを考えると、最も重要な個人情報のひとつである医療情報においては、もっとも安全性の高いシステムを構築しなければいけないといえるでしょう。

そこで、システムの技術や運営管理上の対策について厚生労働省が策定しているのが「医療情報システムの安全管理に関するガイドライン」です。2005年（平成17年）に第1版を策定後、定期的に改正を行い、2017年（平成29年）に改正個人情報保護法が施行されたのに合わせて、同年「医療情報システムの安全管理に関するガイドライン 第5版」を公表しました。

ガイドラインを遵守しなかった場合、個人情報の漏えいといった事故だけでなく、システムの脆弱性を突いて診療録が暗号化や破壊、改ざんされるといったことも想定されます。医療機器が停止し、予定されていた手術ができなくなるおそれもあります。その結果、診療自体を縮小せざるを得ない、もしくは診療そのものができなくなるという深刻な事態を引き起こしかねないのです。

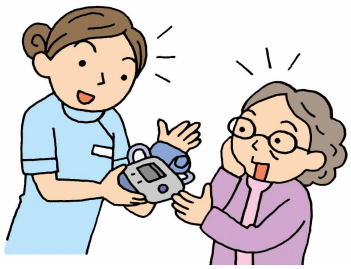
医療機関が行うべき主な内容

ガイドラインには医療情報システム担当者が確認すべきことが詳細に紹介されています。ここではそのポイントを簡単に紹介します。

【1】セキュリティの責任者を置くこと（組織体制の構築）
組織的安全管理対策を組織全体又はシステム毎に責任を持って行うために、責任者を設置する。
最低限のガイドラインとして、情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。
安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。

【2】アクセスを適切に制御
診療記録など集められた医療情報を仕分け、誰がどの情報までアクセスできるかを定め、適切に運用する。医療情報システムの利用者を認証するときは、二要素認証（ID、パスワードに指紋認証を加えるなど）を推奨する。

【3】IoT（モノのインターネット）機器の管理
患者に貸し出される24時間心電図計などのウエアラブル端末や、患者の自宅に設置された医療機器などではインターネットに接続されているものが増えている。機器を貸し出すときには、情報セキュリティ上のリスクがあることを患者に説明し、同意を得る。



【4】パソコンの外部持ち出しに関する方針や規程の整備
組織として保有する情報に対してリスク分析（※）を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定める。運用管理規程には、持ち出した情報及び情報機器の管理方法、情報を格納した可搬媒体若しくは情報機器の盗難、紛失時の対応を定める。
また、運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行う。

（※）リスク分析手法例･･･以下①～③の順に行う方法がある。
①システムで扱う情報を全てリストアップし、重要度毎に分類する。
②分類された情報毎に脅威を列挙する。
③分析した脅威に対して人的組織的に必要な対策を運用管理規程で定めるなどの対策を行う。

【5】BYODの原則禁止

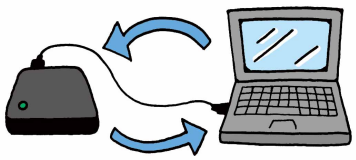
スマホ（スマートフォン）など個人が持ち歩く情報通信機器（BYOD：Bring Your Own Device）が医療情報システムにアクセスすることや、公衆無線LANの利用などは原則禁止。必要とされる場合には、リスクを最小限にするための技術的な対応を行う。

【6】サイバー攻撃などへの対応

従業員に対して標的型メールなどサイバー攻撃に対する教育を行うと同時に、システム障害による個人情報漏洩や医療提供体制に支障が生じる又はそのおそれがあるときには所轄省庁および厚生労働省医政局の下記連絡先に連絡する。
・連絡先：03-3595-2430

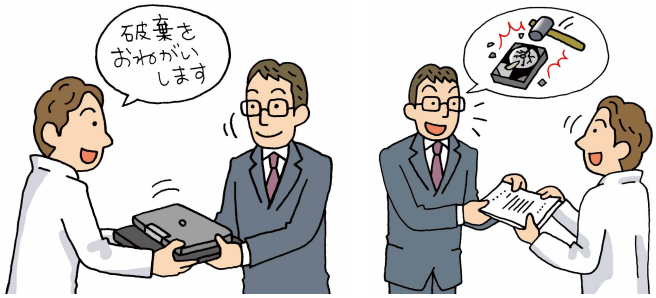
【7】バックアップ

情報を保存している場所で情報の毀損が生じたとき、バックアップされたデータを用いて毀損前の状態に戻せるようにする。不可能な場合は、損なわれた範囲が容易に分かるようにする。



【8】情報の破棄

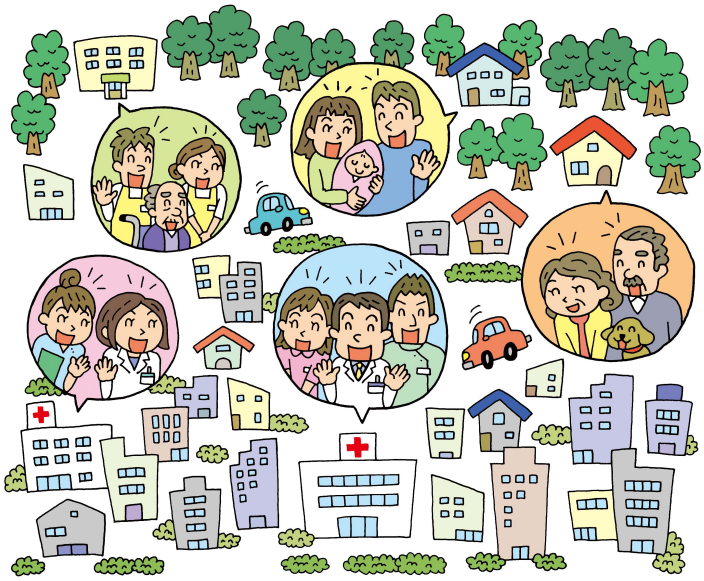
使用している情報処理機器自体を廃棄するときには、必ず専門的な知識を有する者が行い、データが読み出せないことを確認する。



患者の「安全・安心」をサポートするためのガイドライン

IT（情報技術）の発展は、社会のあらゆる分野に大きな変革をもたらしています。医療の世界でも、患者と医師が遠く離れた場所でインターネットを利用して診療を行う「オンライン診療」も行われています。

こうした中で問題となるのがサイバー攻撃などネットワークへの不正アクセスの手口の巧妙化であり、これらに対応するため「医療情報システムの安全管理に関するガイドライン」の改定も順次行われています。ガイドラインを守ることは、患者の安全・安心を守りながら次世代医療を切り拓くために不可欠といえます。



医療情報システムの安全を守るためには、システム担当者や医師だけでなく看護師、薬剤師、介護士などヘルスケアの現場で働くスタッフ全体の協力が欠かせません。医療従事者の皆様はぜひ一度、ガイドラインをご覧ください。

ガイドライン本文、全ての医療機関等の管理者向け読本、用語集、Q&Aなどは、以下よりご覧ください。

・厚生労働省ホームページ　医療情報システムの安全管理に関するガイドライン　第5版（平成29年5月）
・IoTセキュリティガイドライン（経済産業省、総務省）

TOPへ戻る

ページの先頭へ戻る

医療情報連携ネットワークはなぜ必要？
出発点は地域医療を良くしたいという思い
医療情報連携ネットワークの導入効果
利用者の声（導入効果）

医療情報連携ネットワークをどう作る？
医療情報連携ネットワークの構築手順
実施のポイント
利用者の声（苦労した点、成功要因）
ガイドライン、書式例など

医療情報連携ネットワークの具体例を見る

医療情報連携ネットワークとは
データで見る
ピックアップ事例
事例を探す

構築手順
構築手順について
Step1：計画
Step2：構築
Step3：運用
Step4：更改

FAQ
用語集
お役立ち情報
リンク集
資料ダウンロード

プライバシーポリシー・免責事項 | お問い合わせ |