医療情報システムを安全に管理するための
のしおり

医療機関内のセキュリティ対策できていますか？

2010年2月

日本医師会　医療ＩＴ委員会

目次

しおりの目的

- 医療情報システムの導入を検討したり、導入を決定する立場にある、管理者の方（院長や理事長）
- 医療情報システムを既に導入、運用している管理者の方（院長や理事長）

上記の立場にある管理者の方々が、システムを導入する際に、院内の情報技術管理者の先生や取引先の業者に、適切に指示ができる知識を持っているかどうかチェックできます。

正しい知識を持ち、医療機関としてセキュリティ対策を整え、不測の事態に備えましょう。

※「医療情報システム」とは、電子カルテなどに限らず、レセコンや医事会計システム、院内で使用するパソコン、FAX などの通信機器も含みます。決して特別なものではありません。

第１章　電子的な医療情報を取り扱う際の責任のあり方

➢ 考え方

そもそも、医療に係わる行為は医療法などで医療機関や医師の責任で行っています。そのため、そこから発生する情報についても、医師の責任で管理して扱うことが原則です。ただし、近年のパソコンやインターネットの普及に伴って、必ずしも全てが医療機関や医師の責任と言えないことも出てきました。

逆に言えば、全てが医療機関や医師の責任にされないためにも、しっかりした情報保護やセキュリティ対策について正しく理解し、実施しておく必要があります。

Q. なぜセキュリティ対策が必要なのでしょうか？

A. 自宅に鍵をかけてお金や資産を守ることと同じで、医療機関にも大切な情報がたくさんあります。それらを正しいセキュリティ対策で守らないと、情報が漏えいしたり、誰かに改ざん、破壊、盗難されたりする危険性があります。

正しい知識を持ち、さまざまな脅威から、情報資産を守ることが必要です。

Q. 情報漏えい被害が絶えないのはなぜでしょうか？

A. 「情報を守らないといけないという意識がない」「自分だけは被害にあわない、大丈夫だという意識から、適切な対策を行っていない」「インターネットは世界中とつながっていて便利だが、悪意のある人もいる無法地帯であり、対策をしても意味がない」といった意識をもっている方が多いからです。

「自分だけは大丈夫！」と思っていませんか？ 自分自身や医療機関スタッフの方が、情報を漏えいしていないと断言できるでしょうか。セキュリティの知識を持たないと、ウイルス入りのファイルやメールを周囲にばら撒くなど、ご自分が加害者になる可能性の方が、今は高くなっているのです。

Q. 医療情報が漏えいした場合には法的責任が課せられることを知っていますか？

A. 下記の情報を公表し、それに対する対処法を説明することが必要です。

- ✓ 何のデータ（例：患者さんの個人情報：氏名、患者番号）
- ✓ 何の媒体や手段（例：USB メモリ）
- ✓ どうして漏えいしたか（例：紛失した）
- ✓ どこで（例：JR 車内で落とした）
- ✓ どうなったか（例：USB メモリは回収済み。取得者にも内容の非公開を誓約済み）
- ✓ 今後どうするか（例：院内委員会でマニュアルの見直しを行い、教育する）

第２章　電子的な医療情報を扱う際の考え方

➢ 考え方

以下の４つの安全管理対策を取りましょう。

●**組織的**安全管理対策
医療機関の組織として、どのように情報を保護するのか、院長を中心として方針を立てます。

●**物理的**安全管理対策
情報が入ったパソコンやUSB メモリなどを物理的にどのように保護するかの対策です。鍵のかかった金庫にしまうということも対策のひとつです。

●**技術的**安全管理対策
ウイルス対策ソフトを導入したり、ID とパスワードを定期的に変更したり、暗号化したりする対策です。パソコンに入っている情報を技術的に保護します。

●**人的**安全管理対策
医療機関で雇用している従業者にセキュリティに関する教育をしたり、注意を促したりする対策です。雇用時に、情報の取り扱いについて契約を取り交わしたり、罰則を付けたりすることも考えられます。

Q. 医療機関として、組織的安全管理対策を行わなければどうなりますか？

A．例えば、こんな事故が起こります。

●医療機関内部の人間が患者情報を、勝手に外部に持ち出す。

●情報セキュリティに対する考え方が徹底できておらず、従業者のモラルが低いので、漏えい事件が起こる。

【対策】組織的安全管理とは・・・

従業者との責任権限を明確にして、セキュリティ対策の規定・手順書の整備運用を行い、実施状況を確認することです。経営責任者（院長）が危機意識を持って、主体的に取り組む必要があります。

Q. 医療機関として、物理的安全管理対策を行わなければどうなりますか？

A．例えば、こんな事故が起こります。

●情報機器の管理ができておらず、USB メモリを紛失して（盗難されて）しまう。

●情報にアクセスできる人が誰か把握しておらず、情報が漏えいした時に責任の所在がわからない。

【対策】物理的安全管理とは・・・

医療機関内部の入退館（室）の管理や、個人データの盗難の防止、情報機器の管理等の措置を行うことです。

Q. 医療機関として、技術的安全管理対策を行わなければどうなりますか？

A．例えば、こんな事故が起こります。

●ID/パスワードが全員同じで、利用者の識別がなく、アクセスの記録を取っていない。

●Winny（ファイル共有（交換）ソフト＝インターネットを通じて不特定多数の相手とファイルを共有／交換するためのソフトウェア）などの問題があるソフトウェアを使用しているために、情報漏えいがおこる。

【対策】技術的安全管理とは・・・

パソコンを使用する時に、許可された利用者だけが確実に情報にアクセスでき、許可されていない人はアクセスできないようにすることです。

また、不正ソフトウェア対策、医療情報システムの監視等、個人データへの配慮が必要となります。

Q. 医療機関として、人的安全管理対策を行わなければどうなりますか？

A．例えば、こんな事故が起こります。

●利用者の不注意により、本来入力すべきデータと違うデータが入力されたまま運用される。これにより、例えば処方量のミスが起きて医療安全が脅かされる。

●利用者が確認を怠り、データを本来送信すべき相手とは異なる相手に送信してしまい、送信先から情報が大量に漏えいしてしまう。

【対策】人的安全管理とは・・・

従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練を行うことです。

Q. セキュリティの危機対策はどうしたらいいか解りますか？

A．最悪の事態を想定して、対策をきちんとしましょう。

まず、規約（手引き）を作って、医療機関としてきちんとした対応をしていることをアピールしましょう。アピールすることは、漏えい対策にも有効です。

また、定期的に従業者への研修会の実施（いつ実施したか、誰が出席したかなど書類を残しておくこと）や誓約書等の整備をしましょう。

第３章　電子的に医療情報を交換もしくは提供する際の考え方

➢ 考え方

電子的に医療情報を交換もしくは提供するには、USB メモリを使ったり、ネットワーク（安全なインターネットも含む）を使ったりすることが考えられます。

この場合、USB メモリの紛失やネットワークからの情報漏えいにも注意する必要がありますが、一番身近な問題はパソコンへのウイルス感染です。ウイルスに感染すると、意図せず情報が漏えいしたり、パソコンが破壊されたりして診療に影響がでることもあります。

まずは、パソコンへのウイルス感染防止を基本として対策を講じましょう。

Q. パソコンにウイルスが感染した時の症状はご存じですか？

A．基本的に下記の２つの操作をする時に、注意してください。

①ファイルを取り込んだとき

②画面を表示するとき

次のような症状がでます（ただし、目立った変化が全然なく、感染していることが分かりにくいケースもあります）。

●パソコンのソフトが頻繁に動かなくなったり、起動しなくなったりする。

●ファイルがなくなったり、知らないアイコンが増えたりする。

●全てのファイルを表示させず、自身を隠す。

●C や D ドライブ、USB メモリがまともに開かない。

●インターネットに勝手に接続したり、メール送信が知らない間に行われたりしている。

Q. パソコンにウイルスが感染した時の感染原因は何でしょうか？

A．感染原因には、下記のようなケースがあります。

●USB メモリなどの外部媒体からの感染。

●メールからの感染。

●悪意ある Web ページを閲覧して感染。

●インターネット上からダウンロードしたファイルからの感染。

●インターネットに接続しただけで感染。

★ウイルス感染や情報漏えいにはこんな事例があります★

（事例１）ウイルス対策ソフトがパソコンに入っていなかった時の被害

【対策】ウイルスに感染した場合の対処方法

もしウイルスに感染したような兆候が現れたら、第一にウイルス感染の被害拡大を防ぐために、ネットワークケーブルを抜くなどして、感染したパソコンをネットワークから切り離し（隔離し）ましょう。そのあと、下記の解決策を検討します。

●パソコンの管理者に相談して、指示に従う。

●業者に相談する（費用が必要）。

●（解決後）業務に使用するパソコンにはすべて事前にウイルス対策ソフトを導入し、日々更新作業を実施する。

（事例２）メールからウイルス感染する被害

【対策】もし添付ファイルがあったら、下記の点に注意して対処しましょう。

●差出人が知人かどうかに限らず、内容が不審なメールは開かない。
⇒差出人（From アドレス）は偽装されている可能性があります。

●不審な添付ファイルは実行しない。

●添付ファイルを開く必要がある場合には、ファイルを一旦フォルダに保存し、ウイルス対策ソフトでチェックを行う（チェックのやり方はソフトによって異なります）。

また、メール使用上の注意点は下記のとおりです。加害者にならない様に、発信する場合も注意が必要です。

●発信元が不明なメールは取り扱い注意。

●添付ファイルに注意。

●発信元が明らかであっても不審なメールに注意。

●自分から発信する際にも、添付するファイルに注意。

（事例3）USB メモリからウイルス感染する被害

【対策】USB メモリから感染するウイルスが非常に増えています。USB メモリを使用する時には、下記の点に気をつけましょう。

●「パソコンに接続するだけで自動実行する機能」を停止する。
（Windows の場合：キーボードの Shift キーを押しながら USB メモリをつなげると、停止できます）

●出所のわからない USB メモリは使用しない。

●ウイルス対策等ができていないコンピュータで、USB メモリを使用しない。

●USB メモリ、FD（フロッピーディスク）、CD-R、DVD-R などの外部記憶媒体を使用してデータを移す場合には、ウイルスチェックをきちんとしてから移すこと。

●しばらく利用していない外部記憶媒体を利用するときにはウイルスチェックをすること。

●私物の USB メモリなどは使用を控えること。

★アドバイス★　USBメモリの使用について

●USB メモリ自体にウイルスチェック機能が付いたものや、パスワードを入力しないと使えないものなどがあります。紛失や盗難等の危険性もありますので、安心を買う意味で、セキュリティ対策がついている USB メモリを買うことをお勧めします。

●職場内で、使うかどうかルールを決めて徹底しましょう。

●あえて使わない、使わせないといった対策も効果的です。パソコンの USB ポート（差し込み口）を使えないようにする方法もありますので、業者に相談してみましょう。

●ウイルスチェックするための専用のパソコンを設置して、チェックしてから使うようにする方法も検討しましょう。

（事例4）パソコン使用時のユーザーID とパスワードが盗まれて情報漏えいした被害

【対策】ユーザ ID とパスワードが未設定だったり、みんなが同じ ID を使用していたり、パスワードを付箋などでパソコンに貼っていたりして、情報を盗み取られる場合があります。ユーザ ID やパスワードについては、下記の点に注意して設定しましょう。防犯対策と同じだと考えましょう。

●ユーザ ID とパスワードは、利用者ごとに設定をする。

●ユーザ ID とパスワードは、他人に知られないようにする。

●他人に解読されないようなパスワードを作る。

●パスワードは定期的に変更する（退職者が知っていると情報漏えいする可能性も）。

●退職者の ID は速やかに削除する。

●アクセスのログを収集し、定期的にチェックしたり、監視したりしていることを従業者に通知する。

★アドバイス★　解読されにくいパスワードについて

～覚えやすく、かつ他人に解読されにくいパスワードを設定する方法～

1. 「文字置換の作成方法」があります。例：「a → @」「t → +」「o → O」などにします。この例に従って「password」という単語を変換すると、「p@sswOrd」となります。他人が簡単には想像できないような独自ルールを作ってみましょう。

2. 「フレーズからの作成方法」があります。最初にフレーズを決めておき、各単語の頭文字を取ってパスワードを作成します。
   フレーズ：Let's manage the password exactly !
   ↓パスワード：Lmtpe!
   作成者はパスワードをフレーズで覚えられるため、忘れにくくなります。

(事例5)電子メールを利用する際に、誤送信して情報漏えいが起こった被害

【対策】電子メールの宛先アドレスをしっかり確認してから、送信しましょう。宛先や CC、BCC の使い方に注意して作成してください。人が操作する場合は、ケアレスミスがよくあります。送信してしまったメールは取り消しできませんので、ご注意ください。

(事例6)インターネット利用時に不審なホームページを見て、パソコン故障被害

【対策】不審なホームページには、パソコン内のソフトを壊していくウイルスがばらまかれているページもあります。インターネットを利用する時に、下記の点に気をつけましょう。

- ●インターネット接続（ホームページ閲覧、メール送受信）には、ウイルス対策ソフトを導入した専用のパソコンしか使用しないことを推奨。
- ●業務に必要のない Web ページ、不審な Web ページにはアクセスしない。
- ●ネットワークの私的利用はやめる。

●コンテンツフィルタなどで閲覧できるWebサイトを限定し、ルールを守ってインターネットを使用するように指導。

●ログ監視を行っていることを、スタッフに通知。

(事例7)メモ用紙や印刷物の破棄による情報漏えい被害

【対策】患者さんの情報がそのまま放置されていると、誰かに盗み取られる可能性があります。下記のようなケースに注意してください。

●パソコン画面に情報を表示したまま離席。

●電話等で聞きとった情報をメモ用紙に書いたものを放置。

●シュレッダーせずにメモや印刷物をゴミ箱へそのまま捨てる。

●個人情報などをプリントアウトし、そのままプリンタ上に放置。

(事例8)パソコンの処分による情報漏えい被害

【対策】故障や古くなったパソコンを廃棄する場合に、リサイクルセンターやパソコンショップなどに下取りに出して、漏えいすることがあります。

廃棄する前に、患者さんの情報などの個人情報や機密情報が入っていないか、よく確認してください。また、データを削除したからといって、安心してはいけません。専用ソフトなどを使って、削除データを復旧できる場合があるからです。費用がかかっても、以下の対策を取りましょう。

●ハードディスククラッシャーなどの装置を使って、物理的にハードディスクを破壊してから廃棄に出す。

●パソコンからハードディスクを取り外し、傷を付けるなどして物理的に破壊する。
レセコンの場合は、業者に相談して廃棄証明書をもらうようにする。

●フォーマットソフト等を利用して、データが復旧できないようにする。

●パソコンメーカーが証明書を出してくれる廃棄サービスをしている場合は、それを利用する。

(事例9)トラッシング(ゴミから収集)による情報漏えい被害

【対策】ゴミとして個人情報の書類等を廃棄する場合には、清掃業者や侵入者などに盗まれる可能性もありますので、必ずシュレッダーにかけましょう。紙情報だけでなく、USB メモリ、FD、CD-R、DVD-R などの電子媒体を捨てる時にも、壊して読み書きできないようにしてから、捨てましょう。

レセプト請求に用いた電子媒体は、請求業務が終了してしまうと、うっかり置き忘れてしまうこともあります。レセプト情報にも重要な個人情報が含まれているので、保管する場合は鍵のかかった場所に保管し、破棄する場合も十分注意して扱いましょう。

Q. レセプトオンライン請求する時のデータは、暗号化されているので安全だと聞きますが本当でしょうか？

A．実は、オンライン請求に使うレセプトデータは「暗号化」されているわけではななく、「コード化」されているだけです。例えば、傷病名が書いてあるところは、SY5319009 のように書かれており、社会保険庁の Web サイトでコードを調べることができます。

よって、安全なセキュリティの高いネットワークからデータ送信をしないと、漏えいする危険性があります。医療機関は、データを送信するまでが責任範囲となっていますので、それまでの段階で情報が漏えいしない様に気をつけましょう。FD などの電子媒体で受け渡しをする場合は、提出した証明書をきちんともらいましょう。

Q. レセプトオンライン請求する場合は、どこに気を付ければいいのでしょうか？

A．その際に使用するネットワークセキュリティについては、以下の点に注意しましょう。難しい内容を含みますので、よくわからない方は、対応をしてくれる業者に相談しましょう。車を修理する場合と同じく、安心・安全の為に、プロに任せるのも有効な手段です。

- ●セキュリティの高いネットワークを使用してデータ送信を行う（クローズドな手段をとる）。例えば、「専用線」「公衆回線（ISDN）」「IP-VPN」など。
- ●電子証明書等を利用した認証手段で、送信元と受信先の双方で、接続相手を確認してデータ送信を行う。

●施設内ルータを経由した、拠点間の不用意な折り返し通信を許可しない設定等を行う。

●無線 LAN は極力使用すべきではないが、やむを得ず使用する際は、利用者以外に特定、悪用されないよう、しっかり暗号化する。

参 考　レセプトオンライン請求で使用するパソコンについて

【事例】レセプトオンライン請求で使用しているパソコンから、情報漏えい被害

診療用の患者データの入ったパソコンを使用しています。

便利なので、このパソコンでインターネットにも接続して、検査センターからのデータ受信や、時には従業者がネット上での検索にも利用しています。

また、最近はオンライン請求にもこのパソコンを使用しています。いろいろなデータがインターネットで取得できて便利なので、ファイル共有ソフトの Winny を入れていました。

ところが、最近、自分のパソコンデータが外部に流出していることがわかりました。そのため、今まで使用していなかったウイルス対策ソフトを購入、インストールして、ウイルス検索をしたところ、多数のウイルスが見つかりました。どうしてこんなことになったのか解りません。

Q. 患者データの入ったデータをインターネット閲覧と共用してもいいですか？

A. 患者さんのデータの入ったパソコンは、原則としてインターネットにはつながないようにしましょう。

院内で全部のパソコンがつながっているネットワークの場合は、特に注意が必要です。

今回の様に、インターネットを閲覧していると、知らぬ間にウイルスに感染してしまう可能性があります。そうなると、パソコンが不具合をおこしたり、場合によっては、そのパソコンの中身を、外部の人に見られてしまうような状態になってしまうこともあります。

インターネット閲覧だけでなく、

- ✓ 一見まともに見えるフリーのソフトをパソコンにインストールする
- ✓ 自分のものではない外部記憶媒体からデータを読み込む
- ✓ Ｅメールでもらった添付ファイルを開く

といったようなことをする場合、ウイルスに感染してしまうことがあります。**Winny などのファイル共有ソフトは、このようなパソコンには絶対に導入してはいけません。**

通常インターネットに接続しない場合でも、大切なパソコンには、**必ずウイルス対策ソフトを導入、適用し、最新ウィルスに対応するパターンファイルを定期的にアップデートします。アップデートする時にのみ、インターネットに接続しましょう。**

また、インターネットはある意味非常に危険なので、**閲覧専用のパソコンを業務用とは別にもう１台用意することをお勧めします。**最近は、このようなパソコンは 10 万円以下で購入することができます。

まとめると・・・

- ✓ パソコンには必ずウイルス対策ソフトを導入してアップデートする
- ✓ インターネット閲覧と E メールは、専用のパソコンを用意する
- ✓ 患者データの入ったパソコンは、原則インターネット接続をしない
- ✓ Winny のようなファイル交換ソフトは絶対に使用しない
- ✓ 他人からもらった USB メモリのデータは、事前にウイルス対策ソフトでウイルスチェックする

以上のことを考慮して、パソコンの選定をしましょう。

まとめ

「情報漏えい」とは、本来その情報を扱うことができないはずの人に情報が伝わってしまうことです。情報漏えいの対策を行うには、外部からの侵入を防ぐことはもちろん、組織内のひとりひとりが意識を持ってセキュリティ対策に取り組むことが重要です。

上記の内容を踏まえて、医療機関の管理者の方（院長や理事長）が、セキュリティ管理者として、しかるべき対策を行ってください。

また、情報漏えいが発生してしまった場合を想定して、さまざまな対応を考えておいてください。

完璧な対応はなかなか難しいとは思いますが、万一の際に、どれだけ手を尽くしたか言える様にしておきましょう。

「安全管理責任」は、あなたにかかっています。

情報漏えいによって医療機関の信頼を損ねるような

事態になれば、経営の危機が来ます。

信頼は、お金では解決できません。

未然に防ぐ対応を今日から始めましょう。

付　録　医療機関従業者向けのしおり

個人情報とは

生存している患者さん等の個人を特定することのできる情報のすべてです。

例えば氏名、生年月日、住所等の基本的な情報から、既往症、診療内容、受けた処置内容、検査結果、それらにもとづいて医師等が行った診断や投薬内容、病状の経過等のことです。

従業者にも責任が及ぶ可能性が

医師、薬剤師等には、罰則規定のある刑法 134 条により秘密漏示の規定があります。

> （秘密漏示）第 134 条　医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、６月以下の懲役又は 10 万円以下の罰金に処する。
> 宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときも、前項と同様とする。

また、医療機関管理者である院長には、個人情報保護法 21 条で、個人情報の安全管理が図られるよう従業者に対する必要かつ適切な監督義務が課されています。

個人情報保護法は医療機関組織全体を「個人情報取扱業者」として扱う法律なので、医師のみでなく医療機関のすべての従業者に対する個人情報の保護義務が求められます。これによって従業者が故意や重大な過失で患者の個人情報を第三者に漏えいすることで医療機関が損害賠償の対象となった場合は、医療機関が従業者に対して求償するだけでなく、医療機関に対して指導・勧告があり、組織全体の信用低下を招きます。

個人情報保護法 58 条では、医療機関に対しても罰金を科することが記載されており、雇用主たる管理者としては、従業者に直接損害賠償請求をする可能性もあります。

目に見える患者情報

●カルテの表紙に病名記載がある場合、他の患者さんの目に触れないように注意。

●患者さんのことを記載したメモ用紙などに注意。

●ホワイトボードなど、患者さんから見える位置に患者情報を記載しない。

●検査データは他の患者さんから目の触れない位置に。

●廃棄する患者情報の記載された紙は、そのまま捨てずに必ずシュレッダーにかける。

●患者情報の記載された書類を FAX 送信する際は、誤送信しないよう注意。
⇒誤ったところに送信すると患者情報漏えいになります。

目に見えない患者情報の代表がレセコン、パソコン、外部記憶媒体

●フロッピーディスク（FD）等のレセプト電子媒体を保管する際は、鍵のかかる場所に。

●レセコンやパソコンには第三者が使用できないように各個人の ID・パスワードを設定。

●適宜更新されるパソコンのセキュリティ・アップデート（Windows の場合、「Windows Update」）を確実に行う。

●パソコンにはウイルス対策ソフトを導入し、日々更新（アップデート）する。

●インターネットの閲覧やメールのやり取りには専用のパソコンを使用し、決して患者情報の入った業務用パソコンは使用しない。
⇒インターネット閲覧やメール送受信によりウイルス感染する可能性があり、これによってパソコン内の情報が知らぬ間に第三者に渡る可能性があります。

●Winny（インターネットを通じて不特定多数の相手とファイル共有／交換するためのソフトウェア）などは決してパソコンに導入しない。

●電子メールでの患者情報のやり取りには患者さんが特定されない工夫が必要。
⇒電子メールは第三者に内容を読まれる可能性があります。

●患者情報の入ったパソコンは普段はインターネットには接続せず、ウイルス対策ソフトの更新時のみ接続し、更新が終了したら LAN ケーブルははずしておく。

●医療機関のパソコンに、私的な USB メモリは使用しない。
⇒最近は USB メモリを介するウイルス感染事例が増加しています。

●管理者の許可なく、医療機関のパソコン内のデータを家に持ち帰らない。

●院内で使用した FD、MO、CD-R、USB メモリ等を廃棄する場合は粉砕して廃棄する。
⇒パソコン上でデータを削除しても、専門家の手にかかると消去されたはずのデータが復元できることがあります。

●レセコンやパソコン、外付けハードディスクなどを廃棄する場合には、専門業者に依頼して内部情報を完全に消去する。または、パソコン内のハードディスクを取り出して、物理的に破壊する。

（医療機関名）

院長殿

患者さんの個人情報の保護に関する誓約書（例）

私は、当院の従業者として、患者さんの個人情報の保護に関する院内規則を十分に理解し、これを遵守いたします。

私は、在職中はもちろん、退職後においても、職務上知り得た患者さんの個人情報を、正当な事由なく第三者に漏らしません。

以上、誠実に遵守することを誓います。

年　　月　　日

（医療機関名）

氏名

※従業者を雇用する際に、このような誓約書を交わしておくことも情報漏えいの取り組みとしては重要です。参考にしてください。

平成 20・21 年度　日本医師会　医療ＩＴ委員会

委 員 長	佐伯　光義	愛媛県医師会常任理事
副委員長	藤井　純司	京都府医師会理事
委　　員	石井　　出	神奈川県医師会理事
委　　員	石川　広己	千葉県医師会理事
委　　員	内田　一郎	大分県医師会常任理事
委　　員	大橋　克洋	東京都医師会理事
委　　員	小澤　孝好	兵庫県医師会常任理事
委　　員	笠井　英夫	岡山県医師会専務理事
委　　員	川出　靖彦	岐阜県医師会副会長
委　　員	河本　英敏	埼玉県医師会理事
委　　員	末松　哲男	福井県医師会理事
委　　員	富田　雄二	宮崎県医師会副会長
委　　員	登米　祐也	宮城県医師会常任理事
委　　員	藤原　秀俊	北海道医師会常任理事 （H.21.3 まで）
委　　員	水谷　匡宏	北海道医師会常任理事 （H.21.4 から）
委　　員	三原　一郎	山形県医師会常任理事

（委員五十音順）

しおり制作協力

山下　さやか　　富士通エフ・オー・エム㈱

非売品