「ＭＣＳ運用ポリシー」

第１.１版

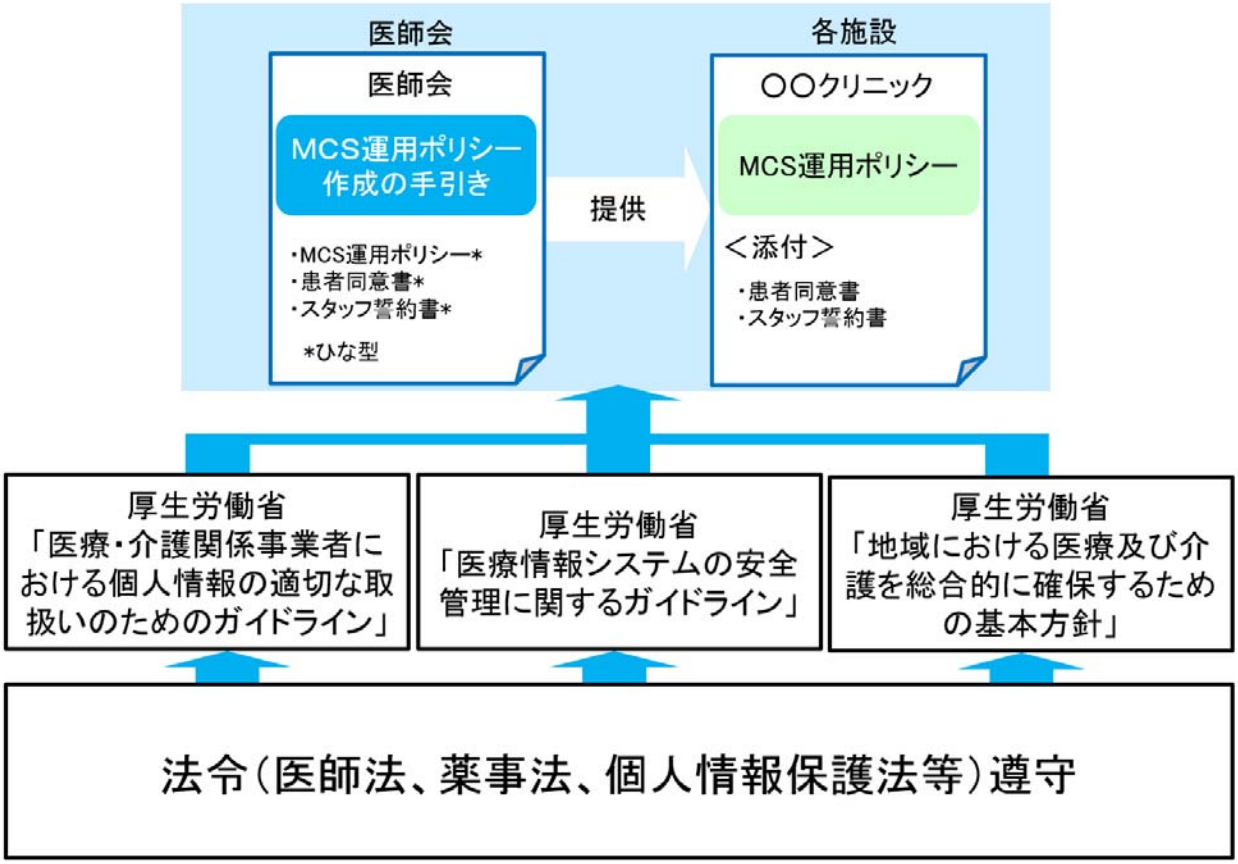
地域包括ケアシステム「あおばモデル」

事務局：青葉区在宅医療連連携拠点

はじめに

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版の「４.１ 医療機関等の管理者の情報保護責任について（１）通常運用における責任について」には、「電子的に医療情報を取り扱うシステムの機能や運用方法が、その取り扱いに関する基準を満たしていることを患者等に説明する責任」を果たすために、「・・・システムの仕様や運用方法を明確に文書化すること・・・」また、「6.1 方針の制定と公表」の「C. 最低限のガイドライン」には、「1. 個人情報保護に関する方針を策定し、公開していること。」、「2. 個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取り扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。」とあります。

医療介護の現場では、これらのガイドラインに則って、システムの適正な運用を行っていく必要があります。



当資料は、株式会社日本エンブレースが提供する医療介護専用のコミュニケーションシステム「メディカルケアステーション」（以下、MCS）を利用するにあたって、病院・クリニック・介護事業者等各施設（以下、施設）にて、医師法、薬事法、個人情報保護に関する法律などの法令遵守はもちろん、厚生労働省の「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」や「医療情報システムの安全管理に関するガイドライン」など医療介護従事者向け各種ガイドラインを考慮しながら、それぞれの施設に合った最適な「MCS 運用ポリシー」を作成するための手引き書です。

各施設は、当資料を参考にして、法令遵守はもちろん、各種ガイドライン等を十分理解したうえで、病院、クリニック、介護施設などそれぞれの施設の特徴、規模等に合わせて、施設の責任のもとに、最適な「MCS 運用ポリシー」を作成し運用してください。

また、施設が作成した MCS 運用ポリシーに基づいて、厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版の「１０運用管理について」の「C 最低限のガイドライン」に記載されている通り、運用管理規定を別途作成及び「システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。」（厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版の付表１　一般管理における運用管理の実施項目例より）が必要となります。

当資料は、ＭＣＳ　Ｖ２．０の機能をベースに記載されています。

当資料は、法令や厚生労働省等の各種ガイドラインの改訂や MCS の機能強化などに伴って必要に応じて改訂される場合があります。

目次

＜参考資料＞

- 患者同意書
- スタッフ誓約書

１．法令及び各種ガイドライン

個人情報の保護に関する法律は、個人情報の有用性に配慮しながら、個人の権利利益を保護することを目的に定められているものですが、医療介護関係事業者が取り扱う患者情報はその特性から、よりいっそう配慮されて取り扱う必要があり、そのためにも、施設は、医師法、薬事法などの各種法令遵守はもちろん、厚生労働省の「医療情報システムの安全管理に関するガイドライン」、「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」を十分理解したうえで、MCS 運用ポリシーを作成する必要があります。

１－１．個人情報の適切な取扱いについて

厚生労働省の「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、個人情報の保護に関する法律に基づき、医療介護関係事業者が行う個人情報の適正な取扱いの確保についてのもので、例えば以下のような記述があります。
（http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000027272.html）

・適用の対象事業者について

『法令上、「個人情報取扱事業者」としての義務等を負うのは医療・介護関係事業者のうち、識別される特定の個人の数の合計が過去６ヶ月以内のいずれの日においても 5,000 を超えない事業者（小規模事業者）を除くものとされている。」が、このガイドラインでは「個人情報取扱事業者としての法令上の義務等を負わない医療・介護関係事業者にも本ガイドラインを遵守する努力を求めるものである。』としています。
（『３．本ガイドラインの対象となる「医療・介護関係事業者」の範囲』より抜粋）

・適用の対象個人情報について

『法令上「個人情報」とは、生存する個人に関する情報であり、個人情報取扱事業者の義務等の対象となるのは、生存する個人に関する情報に限定されている。』が、このガイドラインでは、『当該患者・利用者が死亡した後においても、医療・介護関係事業者が当該患者・利用者の情報を保存している場合には、漏えい、滅失又はき損等の防止のため、個人情報と同等の安全管理措置を講ずるものとする。』としています。（『４．本ガイドラインの対象となる「個人情報」の範囲』より抜粋）

・遺伝情報の取扱いについて

『遺伝情報については、本人の遺伝子・染色体の変化に基づく体質、疾病の発症等に関する情報が含まれるほか、その血縁者に関わる情報でもあり、その情報は生涯変化しないものであることから、これが漏えいした場合には、本人及び血縁者が被る被害及び苦痛は大きなものとなるおそれがある。したがって、遺伝学的検

査等により得られた遺伝情報の取扱いについては、・・・特に留意する必要がある。』としています。（『１０．遺伝情報を診療に活用する場合の取扱い』より抜粋）

上記のとおり、医療介護関係事業者は、小規模事業者であっても、また死亡した後においても、十分配慮して個人情報を取り扱う必要があり、また遺伝情報についても細心の留意によって取り扱っていくべきとしており、医療介護関係事業者ならではの配慮が必要です。

１－２．医療情報システムの安全管理について

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版は、「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」と対になるものとして、医療機関等によって医療情報システムの安全管理の対策が実施されることを目的としており、例えば以下のような記述があります。
（http://www.mhlw.go.jp/stf/shingi/0000026088.html）

・医療情報の価値と重要性について

『4 電子的な医療情報を扱う際の責任のあり方』に、『本来、医療情報の価値と重要性はその媒体によって変化するものではなく、医療機関等の管理者は、そもそも紙やフィルムによる記録を院内に保存する場合と電子化して保存する場合とでは、少なくとも同等の善管注意義務を負うと考えられる。』とあります。つまり、医療情報の価値と重要性は、紙媒体か電子媒体かなど媒体の種類によって変わるものではないので、ＩＴを利用しているかどうかにかかわらず、例えば旧来の紙やＦＡＸ、フィルムなどの場合でも同等の管理をしていく必要があるとしています。

・ＩＤ管理と認証について

『6.5 技術的安全対策』の『C. 最低限のガイドライン』*に『1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。』とし、そのために『2. 本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。』つまり、例えば『ID とパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。』、『パスワードが設定されておらず、誰でもシステムにログインできてしまう。』、『ひとつの ID を複数の利用者が使用している。』ことのないように対策を講じるよう促しています。また、『パスワードは定期的に変更し（最長でも 2 ヶ月以内）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。』等としています。

・情報ごとの区分管理とアクセス制御について

『6.5 技術的安全対策』の『（2） 情報の区分管理とアクセス権限の管理』に、『情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。』とし、『D．推奨されるガイドライン』**に『1．情報の区分管理を実施し、区分単位でアクセス管理を実施すること。』、『2．離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）』等としています。

・人的対策について

『6.6 人的安全対策』の『（1）従業者に対する人的安全管理措置』の『C．最低限のガイドライン』*に『医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。』とし、『1．法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。』や、『2．定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。』等としています。

・ネットワークセキュリティについて

『6.11 外部と個人情報を含む医療情報を交換する場合の安全管理』の『B-2．選択すべきネットワークのセキュリティの考え方』の『C．最低限のガイドライン』*に、『5．送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。』等としています。

*『最低限のガイドライン』は、制度（法律、通知、他の指針等）上の要求事項を満たすために必ず実施しなければならない事項としています。

**『推奨されるガイドライン』は、実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施したほうが理解を得やすい対策としています。

以上のように、医療情報の価値と重要性は、紙媒体か電子媒体かなどそれぞれの媒体によって変わるものではないので、ＩＴを利用しているかどうかにかかわらず、例えば旧来のＦＡＸやフィルムなどの場合でも同等に、必要なユーザーだけが必要な情報に適切な手段によってアクセスするように運用し、またＩＴを利用する場合は、個人によるＩＤ及び適切なパスワードの管理の徹底、ネットワークの暗号化などと合わせて、医療情報の種別、重要性と利用形態に応じた区分ごとのユーザーのアクセス制御を行っていくことが必要となります。また、ＩＴの技術的な安全対策のみならず、人的対策も重要としています。

１－３．地域包括ケアシステム構築のための基本方針

厚生労働省の「地域における医療及び介護を総合的に確保するための基本方針」は、医療介護総合確保法第３条第１項の規定に基づき、地域における医療及び介護の総合的な確保を図るための都道府県及び市町村の事業が、公平性及び透明性を確保しつつ、実施されることを目的としています。
（http://www.mhlw.go.jp/stf/shingi/0000057500.html）

・持続可能なＩＣＴの活用について

『二 医療及び介護の総合的な確保に関する基本的な考え方』の『１ 基本的な方向性』には、『（５）情報通信技術（ＩＣＴ）の活用』について、『質の高い医療提供体制及び地域包括ケアシステムの構築のためには、医療・介護サービス利用者も含めた関係者間での適時適切な情報共有が不可欠であり、情報通信技術（ＩＣＴ）の活用は情報共有に有効な手段である。そのため、医療及び介護に係る情報の特性を踏まえた個人情報保護に十分に配慮しながら、標準的な規格に基づいた相互運用性の確保や将来の拡張性を考慮しコスト低減に努める等、情報通信技術（ＩＣＴ）の活用を持続可能なものとして進めていくことが重要である。』としています。

上記のとおり、地域包括ケアシステム構築のためには、低コストで持続可能なＩＣＴの活用が有効な手段である、としています。

２．患者同意

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４．２版の「6.1 方針の制定と公表の「C. 最低限のガイドライン」には、「1. 個人情報保護に関する方針を策定し、公開していること。」とあります。

したがって、MCS を利用するかどうかにかかわらず、施設は、個人情報保護に関する方針を策定し、その方針を含んだ適切な患者同意が必要です。

２－１．患者同意の方法

患者（介護の利用者を含む）同意方法には、２つの方法があり、病院、クリニックなどの医療機関のみならず、介護などその他の施設においても同様に手続きが必要です。

・オプトアウト方式

個人情報保護方針などを施設内掲示することによって、情報提供停止の申出がない限り、医師の判断で外部医療関係者と情報共有する可能性があることを知らせる方式で、主に外来クリニックで用いられています。掲示内容については様々な団体からひな型が提供されています。

・オプトイン方式

オプトイン方式つまり、事前に個別に本人または家族の同意書を締結する方式です。在宅の場合はこのオプトイン方式つまり患者ごとに患者同意書を交わします。

２－２．患者同意書について

オプトイン方式の患者同意書のひな型を用意しましたので、必要に応じ修正して作成し、最適なもので同意をとるようにしてください。また、患者の希望により同意できない部分がある場合は、その内容を「一部不同意」として追記（例えば、余白部分に「但し、第●項は不同意」と手書きし、手書き部分の上に同意者の印鑑を捺印する等の対応が考えられます。）の上、同意書を交わす方法もあります。

３．ＩＴ機器の安全対策

MCS のみならず、施設のあらゆる医療情報システムは、厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４． ２版を考慮して、安全管理の対策を適切に講じる必要がありますが、ここでは、MCS に関連する対策についてその主なポイントを記述します。

３－１．ＩＤ・パスワードの管理

MCS は、個人ごとに設定及び管理された MCS の ID 及びパスワードによって利用することができます。ID 及びパスワードの管理の推奨事項を記します。

（１） パスワードはメモを残したりせず、人目にふれないように細心の注意を払ってユーザー個人が管理し共有しない。
（２） 一つの ID を複数人で共有しない。
（３） パスワードは、英数混合８ケタ以上とし、定期的（最長で２か月に１回）に必ず変更する。
（４） 利用が終わったら必ずログアウトする。
（５） パソコンの場合、離席時にも必ずログアウトする。
（６） スマホやタブレット、パソコンなど、利用するすべての端末にはロックをかける。

３－２．IT 機器のセキュリティ対策

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４．２版の「6.9 情報及び情報機器の持ち出しについて」の「Ｂ.考え方」では、ノートパソコンやＵＳＢメモリーのみならず、「情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器」についても、「C. 最低限のガイドライン」として、「 1. 組織と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こと。」、「 2. 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を定めること。」、「6. 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。」を勧めています。

ですので、MCS を在宅などモバイルの環境で利用する場合も、上記ポイントに留意しながら、スマートフォン、タブレット等のモバイル端末についても下図ような運用をお勧めします。

また、ＢＹOD（ユーザー個人所有の端末の業務使用）を許可するかどうかは施設ごとの判断となりますが、BYOD であるかどうかににかかわらず、紛失時等の情報漏えいリスク等を考えて、同様の運用をお勧めします。

セキュリティ推奨項目	説明
ナンバーロック	スマートフォン、タブレットなどに他者がログインできないよう、数字列などによるパスワード認証（8文字以上）を設定し、定期的に変更する。
情報機器と情報の取り扱い	持ち出した情報を、定められている以外のアプリケーションがインストールされた情報機器で取り扱わないこと。 また、持ち出した情報機器には、定められている以外のアプリケーションをインストールしないこと。いずれのケースも、例えばファイル交換ソフト（Winny 等）等をインストールしないこと。
ウィルス対策ソフトのインストール	スマートフォンやタブレットに適切なウィルス対策ソフトをインストールしておく。
リモートワイプサービスの利用	スマートフォン、タブレットなどの端末内に残るデータをリモート環境からアクセスし、削除することができるサービス。万一の際に指示することで削除可能となる。
緊急回線停止サービスの利用	万一の際に、スマートフォンやタブレットの回線を遮断することで他者による不正なアクセスを防ぐ。
端末管理・利用者管理（MDM）サービスの利用	利用者側の管理者が一括して、各スタッフの利用状況や各端末の状態を確認、強制設定、ロックできる。
ブラウザ設定（ID等情報の都度入力）	IDやパスワードを記憶する設定にしない。
MCSの操作（コピー等の制限）	定められた手順を守り、情報のダウンロードや、コピー、画面ショットの取得などを行わない。

また、施設内に設置されたサーバー、パソコン、ノートパソコンなどをスタッフが施設外に持ち出すことは禁止する、または持ち出す場合は管理者の承認を事前に得るなどの運用を決めておく必要があります。

そのためには、「情報および情報機器を持ち出す場合は、所属、氏名、連絡先、持ち出す情報の内容、格納する媒体、持ち出す目的、期間を別途定める書式でシステム管理者に届け出て、承認を得ること。」、「システム管理者は、情報が格納された可搬媒体および情報機器の所在について台帳に記録すること。そして、その内容を定期的にチェックし、所在状況を把握すること。」（厚生労働省の「医療情報システムの安全管理に関するガイドライン」より抜粋）といった内容を設けることが考えられます。

３－３．個人情報漏えいの現状について

・ＩＴ機器の紛失・盗難等の実態について

以下は、IT 機器の紛失・盗難等の実態調査結果です。この調査結果では、電子メールや FAX での誤送信の割合がとても高くなっていますので、それらを利用する場合の注意を喚起する必要があります。また、MCS を利用する端末の紛失・盗難時の情報漏えいのリスクを回避するためにも「**３－１．ＩＤ・パスワードの管理**」や、「**３－２．IT 機器のセキュリティ対策**」の徹底が重要になります。

紛失・盗難、誤送信の年間発生確率

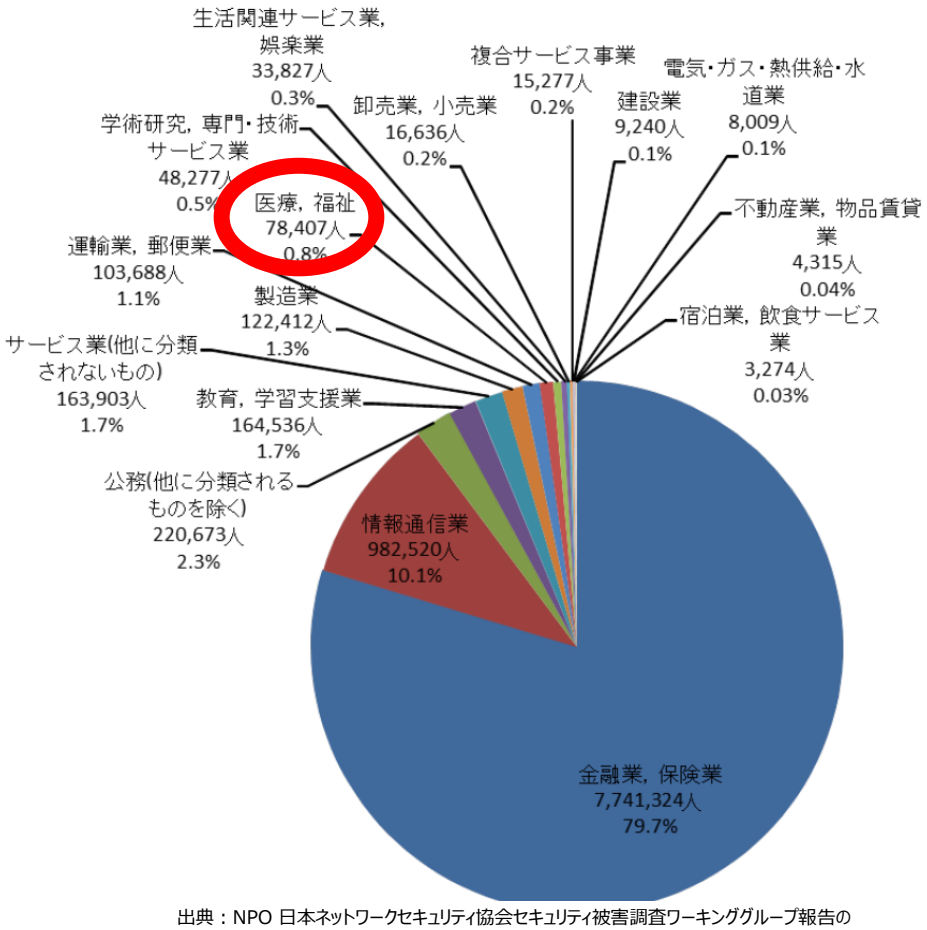
調査対象	2010年	2009年
携帯電話	6．4%	6．6%
パソコン	3．7%	3．1%
USBメモリ	4．7%	4．1%
電子メール（誤送信）	40．3%	17．1%
FAX（誤送信）	39．0%	12．1%

出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の
「情報セキュリティインシデントに関する調査報告書～発生確率編～」

・業種別での個人情報漏えいの人数

以下は、業種別での個人情報漏えいの人数です。「医療・福祉」関連の個人情報漏えい比率は 0.8%です。漏えいしている事実に目を向けて、個人情報管理の運用を日々徹底していく必要があります。

業種別比率（人数）

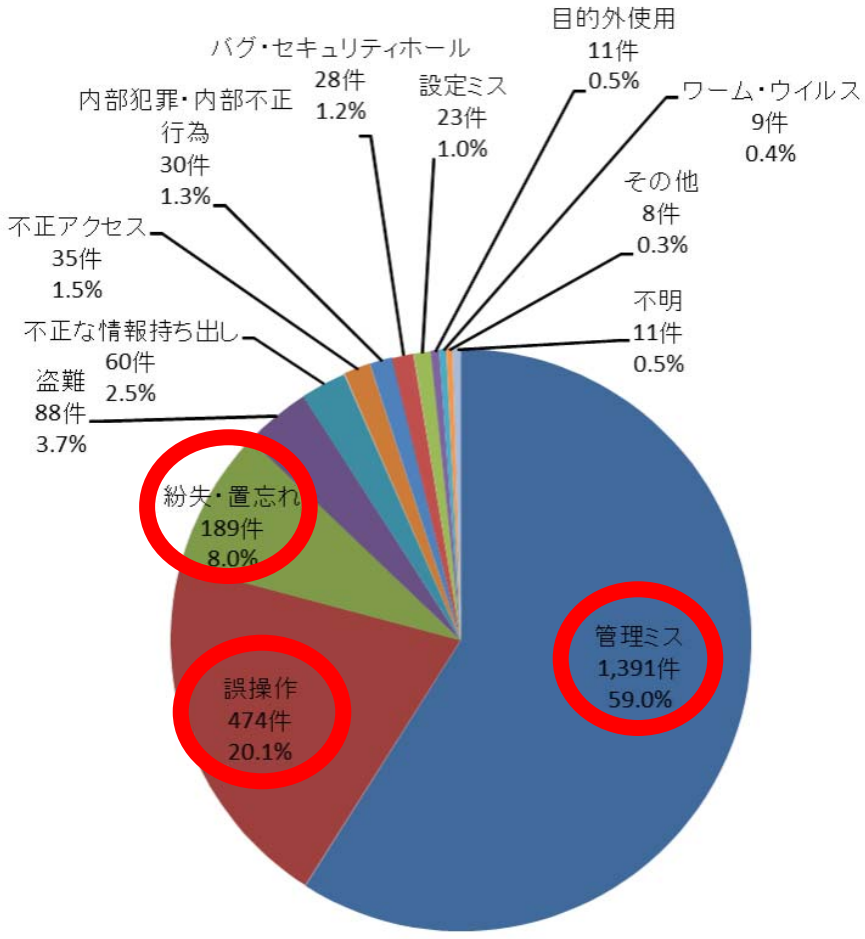


出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の
「2012 年　情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

・個人情報漏えい件数の原因比率

以下は、個人情報漏えい件数の原因比率です。「管理ミス」、「誤操作」、「紛失・置き忘れ」で約 90%を占め、また「管理ミス」の約半分は、信用金庫や信用組合、地方銀行での紛失や誤廃棄であったとのことです。それに対して、バグ・セキュリティホールは、1.2%であり、情報漏えいのほとんどがヒューマンエラー等人的な原因です。ですので、システム提供事業者によるさらなるセキュリティ向上と合わせて、現場での教育等による個人情報管理の運用を日々徹底していく必要があります。

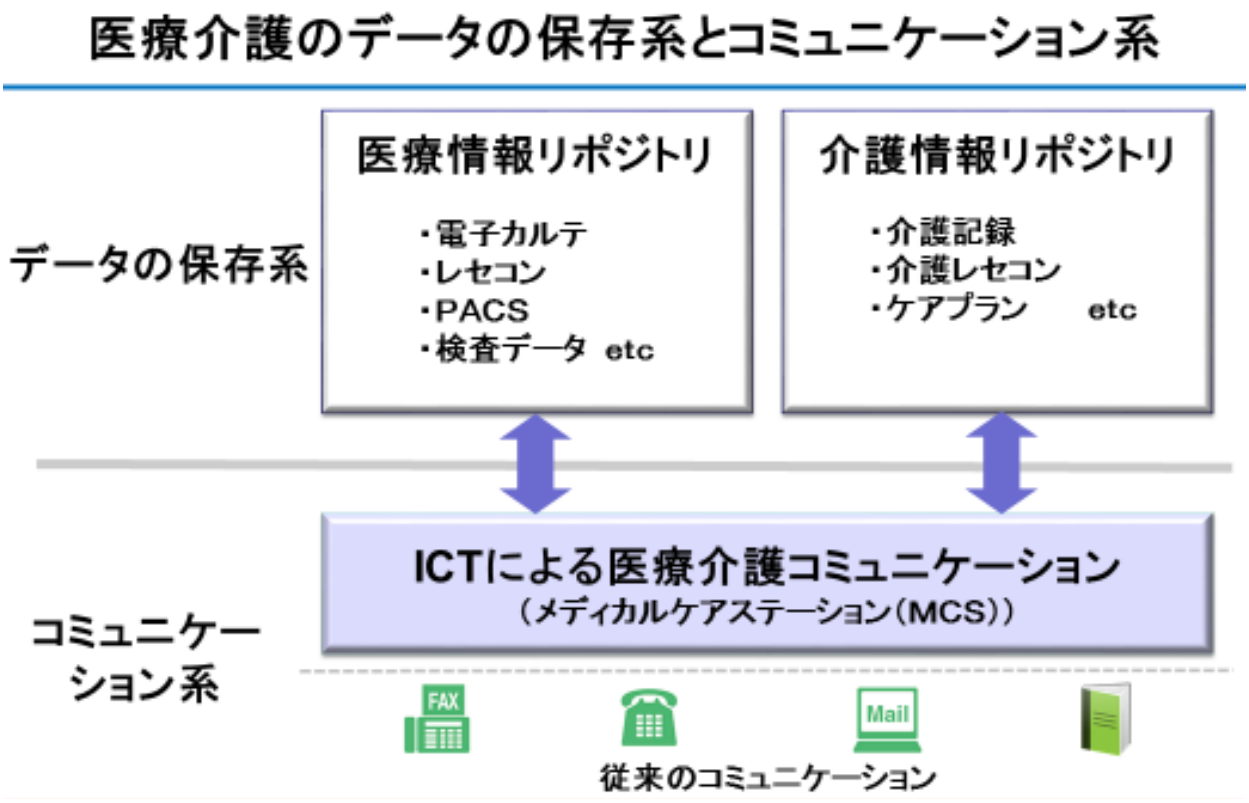
漏えい原因比率（件数）



出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の
「2012 年　情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

４．ＭＣＳの位置づけ

施設のすべての医療情報システムは、MCS を利用するかどうかにかかわらず、厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４． ２版では、「6.5 技術的安全対策」の「（2） 情報の区分管理とアクセス権限の管理」に、「情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。」とし、「C． 最低限のガイドライン」として、「5． 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベ ルに沿ったアクセス管理を行うこと。・・・」、また「D． 推奨されるガイドライン」では「1． 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。」を勧めています。



上図は医療介護にかかわる情報について、データの保存系とコミュニケーション系の位置づけを表した参考図です。データの保存系は、電子カルテや検査データなどの医療情報を保存及び管理する医療情報リポジトリと、介護記録や介護レセコンなどの介護情報を保存及び管理する介護情報リポジトリから構成され、機微なデータの実体はこれらのリポジトリ内に保存・管理されると考えられます。

それに対して、コミュニケーション系は、旧来の電話やファックス、メール、手書きのノートやＩＣＴによる医療介護コミュニケーションシステム（ＭＣＳ）などによって構成され、これらの各種コミュニケーションツールを、それぞれの特

性に応じて臨機応変に利用していく、ということになります。例えば、緊急を要する場合は電話、またデリケートな内容の場合は実際に会って対面で会話する、といった使い分けがされていくことになります。

ＭＣＳは、旧来の電話やＦＡＸなどのコミュニケーションの一部が置き換わっていく新しい形のコミュニケーションツールとして位置づけられ、各種リポジトリと相互補完しながら利用していくということになります。また、MCS は MCS を利用してやりとりする情報について機能的な制限は特に設けられていません。これはＦＡＸや電話を利用する際にも適切な判断をして情報伝達しているのと同じです。

５．ＭＣＳ管理者の設置とアクセス制御

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版の「6.3 組織的安全管理対策（体制、運用管理規程）」では、「C. 最低限のガイドライン」として、「1. 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。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。」とあります。また、施設は、「運用責任者、個人情報保護責任者およびシステム管理者を置き、院長をもってそれに充てること。」、大/中規模病院は、「情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。」また「監査責任者の責務は本規程に定めるものの他、別に定めること。」「情報システムに関する取扱い及び管理に関し必要な事項を審議するため、病院長のもとに情報システム管理委員会を置くこと。」「情報システム管理委員会の運営については、別途定めること。」（付表１　一般管理における運用管理の実施項目例）とあります。

上記からも、規模や必要に応じて、情報システム運用責任者、システム管理者、個人情報保護責任者、監査責任者及び情報システム管理委員会などを設置する必要があります。

MCS を運用するにあたっては、上記担当者のうちのいずれかが、以下に示す MCS 管理者としての役割を担っていただくことになります。

５－１．ＭＣＳ管理者の設置

施設は、必要な情報にアクセスが許可されているスタッフだけがアクセスできる環境を維持するために、施設責任者によって MCS 管理者を設置し、MCS の管理運用をしてください。ここでは、MCS 関連の情報管理内容について記述します。MCS 管理者（どの部署のだれが適切か）は、施設の規模や管理方針等によって異なってきますので、それぞれの施設の特徴や組織形態を踏まえて適切に設置することになります。また、施設の規模や特徴によって、最適な MCS 管理者の人数も決定してください。

MCS 管理者は、MCS 管理者権限ユーザーID を保有し、MCS の適正な利用がされるように MCS を管理運用してください。

- ・MCS の患者情報、個人情報等の管理全般
- ・MCS で利用するＩＴ機器の管理
- ・MCS のＩＤの管理
- ・MCS のグループ登録（患者、自由グループ）及び患者削除管理*
- ・MCS への施設内スタッフ登録及び削除*
- ・MCS へ書き込まれた情報の監視及び削除*
- ・MCS の各グループへ招待された施設内外のユーザーの招待承認及びメンバー解除*

その中でも、*は、MCS 管理者権限ユーザーのみが利用できる MCS の管理機能です。

5－2．お勧めする MCS のアクセス制御方法

適切なアクセス制御のための MCS の利用方法のポイントは以下の通りです。

（1） MCS 管理者権限ユーザー

・MCS で患者単位のグループを作り、それぞれの患者ごとにアクセスする必要のある施設内外の医療介護従事者のみを招待して患者単位のチームを作る。1 つのグループで複数の患者個人情報が混在するような運用は避ける（本来はアクセスする必要のないユーザーが担当していない患者情報にアクセスできてしまうため）。

・MCS の管理者権限ユーザーは、招待された医療介護従事者がその患者へのアクセス権限を持つのにふさわしいかどうかを適切に判断したうえで、「承認機能」で招待を承認する。

・MCS の管理者権限ユーザーは、該当するユーザーが辞めた時や担当から外れた時には、速やかにスタッフ削除やメンバー解除など適切な処理を行う。また定期的に、患者グループごとに、参加しているメンバーが適切であるかどうかの精査を行う。

・MCS の管理者権限ユーザーは、施設として担当しなくなった患者について、「削除機能」を使って速やかに削除する。

・MCS の「管理者権限を設定」の機能を使って、他のユーザーへの権利権限付与する場合は、MCS 運用ポリシーに則って、MCS 管理者権限ユーザーとしての役割を十分説明し、施設の組織上の体制を明確にしてから行う。

・MCS の管理者権限ユーザーは、MCS の安全かつ適正な運用管理を図り、そのためにも不正利用が発生した場合は、MCS の利用を制限もしくは禁止する権限を有する。

・MCS の管理者権限ユーザーは、各書き込みについて監視し、不適正な書き込みなど必要に応じて書き込んだ内容の削除を行う。

・MCS の管理者権限ユーザーも、以下に示す MCS 一般ユーザーの利用方法を遵守する。

（2）MCS 一般ユーザー

・情報セキュリティに十分に注意し、MCS の ID やパスワードを施設スタッフを含む利用者本人以外の者に利用させたり、情報提供してはならない。

・患者グループに招待を受けたユーザーは、自分がその患者グループに参加することがふさわしいかどうかを判断してから、招待の受理を行う。

・各患者グループへの書き込みは、その患者に関することのみとし、別の患者の情報を書き込まない。

・各患者グループへの書き込みは、「４． MCS の位置づけ」を十分理解した上で、適切な範囲内での情報共有の場として利用する。

・MCS のグループごとに常にだれが参加しているのかをわかりやすくするためにも、顔の見える関係をＭＣＳの中でも実現するためにも MCS の個人設定で、スタッフごとにプロフィール、顔写真を登録する。
・自分が担当からはずれた時には、該当する患者グループから、すみやかに「メンバー解除」を行う。
・施設を辞めた時など、MCS を利用する必要がなくなった時は、施設から貸与されている端末があれば返却し、スタッフ誓約書に基づいて、必要な手続きを行う。
・自分自身が書き込んだ情報について責任を持ち、自分自身が書き込んだ不適正な書き込みなどは必要に応じて削除を行う。

また、以下は、厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版の「利用者の責務」から、MCS 用にまとめたものです。これらの点の注意も徹底しましょう。

・MCS ユーザーは、書き込みに際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。
・MCS ユーザーは、与えられたアクセス権限を越えた操作を行わないこと。
・MCS ユーザーは、参照した情報を、目的外に利用しないこと。
・MCS ユーザーは、患者のプライバシーを侵害しないこと。
・MCS ユーザーは、MCS のシステム異常を発見した場合、または使用する機器が紛失もしくは盗難等にあった場合には、速やかにシステム管理者に報告し、その指示に従うこと。
・MCS ユーザーは、不正アクセスを発見した場合、速やかにシステム管理者に連絡しその指示に従うこと。

６．スタッフ誓約書と教育

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４． ２版の「6.6 人的安全対策」の「(1) 従業者に対する人的安全管理措置」の「C.最低限のガイドライン」にて、「医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。」として、「1． 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。」また、「2． 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。」さらに、「３． 従業者の退職後の個人情報保護規程を定めること。」としています。

６－１．スタッフ誓約書

MCS を利用するかどうかにかかわらず、上記ガイドラインに基づいた安全管理のためにも施設内スタッフとの契約は重要です。スタッフ誓約書の記載内容のポイントは以下の通りです。

（１）スタッフは、就業規則やマニュアルなどの諸規定を遵守し、患者等の個人情報のみならず、施設内で知り得た業務に関連する一切の情報をも許可なく漏えいしてはならない、とします。
（２）退職後も漏えいしない、とします。
（３）ＩＴ機器についての取扱い、返却時の注意点などを記載します。
（４）施設が定めた利用目的外での使用を禁止します。
（５）患者その他の第三者のプライバシーその他の権利を侵害するような行為を一切しない。

スタッフ誓約書のひな型を用意しましたので、必要に応じ修正して作成し、最適なもので誓約をとるようにしてください。

６－２．スタッフ教育

施設ごとに作成した MCS 運用ポリシーを徹底するために、施設責任者によって、MCS 管理者およびユーザーに対して、定期的に教育を行っていきましょう。また、MCS の位置づけをユーザー全員で共通認識したうえで、取り扱っている個人情報等の重要性を日々認識し、情報の取扱いに注意していくよう促しましょう。

また、パスワードの管理や離席時のログアウトなど、基本的なことも日々心がけていくことが大切であることを共有しましょう。

７．ＭＣＳ運用ポリシーの作成と運用のポイント

MCS 運用ポリシーは、以下のポイントを踏まえて、施設ごとに最適な運用管理ができるように作成し、作成した MCS 運用ポリシーに基づいて、全ユーザーで運用を徹底するように心がけてください。

７－１．目的の明記

MCS 運用ポリシーの目的を明記しましょう。（以下の例は、厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４.２版に記載されている内容を引用して作成しました。）

例）「この MCS 運用ポリシーは、当施設において、メディカルケアステーション（以下、MCS）で使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取扱い及び管理に関する事項を定め、当施設において、MCS を適正に利用することに資することを目的とします。」

７－２．施設の特徴と規模

MCS 運用ポリシーは、それぞれの施設ごとに取り扱う医療介護情報や、モバイルなどの IT 端末の利用方法、スタッフ数など規模に応じて、管理すべき情報をどのような管理体制で実施するかを考えたうえで作成してください。

７－３．患者同意書、スタッフ誓約書の作成

ひな型を参考に、最適な患者同意書やスタッフ誓約書を作成して、運用してください。

７－４．発表と運用の徹底

作成した MCS 運用ポリシーは、院長や施設長などの責任者によって発表し、MCS 管理者およびユーザーによって運用するように徹底してください。

７－５．情報漏えい発生時の対応について

情報漏えい発生時の対応方法や体制を整え、周知しておくことはとても重要です。情報漏えいによる直接的・間接的被害を最小限に抑えるためにも、また再発防止のためにも適正な措置を行うことができるよう対応方法を準備しておきましょう。

情報漏えいのタイプは、パソコンやモバイル端末、帳票などの紛失・盗難、メールやＦＡＸなどの誤送信、内部犯行、システムへの不正アクセスなどさまざまです。また、関係のない人に患者の情報をうっかり口頭で漏らしてしまうことも情報漏えいの一つといえます。

情報漏えいに関する兆候や具体的な事実を確認した場合は、責任者に速やかに報告することを徹底し、情報漏えい対応のための体制作りを行い必要な方策を講じてください。適切な対応についての判断を行うためにも５Ｗ１Ｈ（いつ、どこで、だれが、何を、なぜ、どうしたのか）の観点で、漏えいした情報の量（件数）と内容、どのような形で保存されていた情報か（暗号化、認証パスワード保護など）などの事実を調査し整理してください。漏えいした情報に個人情報が含まれている場合は、個人情報保護法に準拠した対応が必要となります。

詳しくは、ＩＰＡ（独立行政法人　情報処理推進機構　セキュリティセンター）が発行している「情報漏えい発生時の対応ポイント集」などを参考に準備をしておくことをお勧めします。

７－６．見直し

厚生労働省の「医療情報システムの安全管理に関するガイドライン」第４．２版の「4.1 医療機関等の管理者の情報保護責任について」の「（1）通常運用における責任について　③定期的に見直し必要に応じて改善を行う責任」に、「情報保護に関する技術は日進月歩であるため、情報保護体制が陳腐化する恐れがあり、それを適宜見直して改善するためには以下の責任を果たさなくてはならない。」として、「問題点を洗い出し、改善すべき点があれば改善することそのために医療機関等の管理者は、医療情報保護の仕組みの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行う必要がある。」とあります。

日々進歩しているＩＴ技術、ＩＴを取り巻く環境、法令や各種ガイドラインの改定や施設での業務、患者管理の在り方などの変化や、MCS のバージョンアップ等による機能追加変更などに鑑みながら、作成した MCS 運用ポリシーを必要に応じて見直し、反映して改定していくことをお勧めします。

＜参考資料＞

・患者同意書

ひな型１：最も一般的に利用されているものです。個人情報の利用方法と在宅医療についての説明に加えて、個人情報の利用目的の明細が記述されています。

ひな型２：患者及び家族に読んでいただきやすくするために、個人情報の利用目的の明細を省き、必要最小限の記述にとどめています。

ひな型３：ひな型１に加えて、患者の権利（第２　患者が当施設の保有する個人データに対して有する権利）を追記したものです。より詳しく患者の権利を説明する場合に利用ください。

ひな型４：ひな型１に加えて、MCS の説明を追記したものです。MCS の説明を患者・家族に説明する必要がある場合に利用ください。

・スタッフ誓約書

ひな型１：施設スタッフが誓約する一般的な表記に加え、MCS を意識して、ＩＴ機器取扱いの注意点を加えたものです。

ひな型２：施設スタッフが誓約する一般的な表記のもので、IT 機器について具体的な表記はありません。

表面

在宅医療の開始にあたって
（ご了解いただく事項）

患者の円滑な在宅での療養（医療）を実現するためには、患者をとりまく家族、医療従事者、介護従事者、その他の関係者が適切に連携していく必要があります。そのため適切な連携を行うにあたって下記の事項をご了承いただきますようお願い申し上げます。

記

1） 在宅医療は、医師による継続的な診療が必要であるにもかかわらず、外来受診が困難であるときに行うことができます。
2） 在宅医療は、医療環境が整った病院等で検査及び治療等を集中的に受けることよりも、家族のサポートのもとで住み慣れた自宅で安心して療養を継続することを重視して行われるものです。そのため、患者が在宅での療養（医療）を希望されているのはもちろんのこと、患者をとりまく家族においても意思の統一が図られている必要があります。
3） 在宅医療は、病院診療に比べて十分ではない事項（例えば以下の事項）があります。
　① 訪問（往診）に時間を要すること
　② 検査内容及び診療内容が限られており、かつ検査結果が出るまでに時間を要すること
　③ 衛生面や医療設備等について万全ではない部分があること
4） 在宅医療の開始にあたっては、これまでの担当医からの同意を得ており、診療情報提供書（紹介状）を入手する必要があります。なお、診療情報提供書とは今までの診療経緯や薬の情報（使用禁忌の薬も含む。）等、患者の重要な情報が記載されているものです。
5） 在宅医療の継続にあたっては、患者及び家族と在宅主治医との間に確かな信頼関係を築くことが必要となります。
6） 容態の変化や療養環境の変化を把握するため原則として月二回以上の定期的な訪問診療を受ける必要があります。
7） 円滑な自宅での療養生活を継続していただくため、在宅療養（医療）をサポートする他の病院、診療所、助産所、薬局、訪問看護ステーション、介護事業者その他の関係者と連携を図る目的で、医療従事者や介護従事者その他の関係者が適切と認める通信手段を用いて診療情報を含む個人情報を共有・提供させていただきます。
8） 在宅医療期間中に患者から取得する個人情報の利用目的は、裏面に記載のとおりです。

以上

（西暦）　　年　　月　　日

私は、上記事項について説明を受け、いずれも同意します。

＜患者＞

氏　　名	㊞
住　　所	

＜家族＞

氏　　名	㊞
住　　所	

［注：在宅をサポートする家族１名以上を記載することを想定しています。］

裏面

患者の個人情報の利用目的

1　当施設での利用

（1） 患者に提供する医療サービス
（2） 医療保険事務
（3） 入退院等の病棟管理（もし必要があれば）
（4） 会計・経理
（5） 医療事故等の報告
（6） 患者への医療サービスの向上
（7） 当施設での医療実習への協力
（8） 医療の質の向上を目的とした当施設での症例研究
（9） その他患者に係る管理運営業務

2　当施設外への情報提供としての利用

（1） 他の病院、診療所、助産院、薬局、訪問看護ステーション、介護事業者等との連携
（2） 他の医療機関等からの照会への回答
（3） 患者の診療のため、外部の医師等の意見・助言を求める場合
（4） 検体検査業務等の業務委託及びその他の業務委託
（5） 家族等への病状説明
（6） その他患者への医療提供に関する利用
（7） 保険事務の委託
（8） 審査支払機関へのレセプトの提供
（9） 審査支払機関または保険者からの照会への回答
(10) その他医療・介護・労災保険・公費負担医療等に関する診療費請求のための利用及びその照会に対する回答
(11) 事業者等から委託を受けた健康診断に係る事業者等へのその結果通知
(12) 医師賠償責任保険等に係る医療に関する専門の団体及び保険会社等への相談又は届出等
(13) その他患者への医療保険事務に関する利用
(14) 患者個人を識別あるいは特定できない状態にした上での症例研究、発表及び教育

3　その他の利用

（1） 医療・介護サービスや業務の維持・改善のための基礎資料
（2） 外部監査機関への情報提供

以上

患者同意書（ひな型２）

在宅療養（医療）の開始にあたって
（ご了解いただく事項）

患者の円滑な在宅での療養（医療）を実現するためには、患者をとりまく家族、医療従事者、介護従事者、その他の関係者が適切に連携していく必要があります。そのため適切な連携を行うにあたって下記の事項をご了承いただきますようお願い申し上げます。

記

1）　在宅療養（医療）は、医療環境が整った病院等で検査及び治療等を集中的に受けることよりも、家族のサポートのもとで住み慣れた自宅で安心して療養を継続することを重視して行われるものです。そのため、患者が在宅での療養（医療）を希望されているのはもちろんのこと、患者をとりまく家族においても意思の統一が図られている必要があります。
2）　在宅療養（医療）は病院診療に比べて十分ではない事項（例えば以下の事項）があります。
　①　訪問（往診）に時間を要すること
　②　検査内容及び診療内容が限られており、かつ検査結果が出るまでに時間を要すること
　③　衛生面や医療設備等について万全ではない部分があること
3）　円滑な自宅での療養生活を継続していただくため、在宅療養（医療）をサポートする他の病院、診療所、助産所、薬局、訪問看護ステーション、介護事業者その他の関係者と連携を図る目的で、医療従事者や介護従事者その他の関係者が適切と認める通信手段を用いて診療情報及び療養情報を含む個人情報を共有・提供させていただきます。

以上

（西暦）　　年　　月　　日

私は、上記事項について説明を受け、いずれも同意します。

＜患者＞

氏　　名	㊞
住　　所	

＜家族＞

氏　　名	㊞
住　　所	

［注：在宅をサポートする家族１名以上を記載することを想定しています。］

患者同意書（ひな型３）

表面

在宅医療の開始にあたって
（ご了解いただく事項）

患者の円滑な在宅での療養（医療）を実現するためには、患者をとりまく家族、医療従事者、介護従事者、その他の関係者が適切に連携していく必要があります。そのため適切な連携を行うにあたって下記の事項をご了承いただきますようお願い申し上げます。

記

1） 在宅医療は、医師による継続的な診療が必要であるにもかかわらず、外来受診が困難であるときに行うことができます。
2） 在宅医療は、医療環境が整った病院等で検査及び治療等を集中的に受けることよりも、家族のサポートのもとで住み慣れた自宅で安心して療養を継続することを重視して行われるものです。そのため、患者が在宅での療養（医療）を希望されているのはもちろんのこと、患者をとりまく家族においても意思の統一が図られている必要があります。
3） 在宅医療は、病院診療に比べて十分ではない事項（例えば以下の事項）があります。
   ① 訪問（往診）に時間を要すること
   ② 検査内容及び診療内容が限られており、かつ検査結果が出るまでに時間を要すること
   ③ 衛生面や医療設備等について万全ではない部分があること
4） 在宅医療の開始にあたっては、これまでの担当医からの同意を得ており、診療情報提供書（紹介状）を入手する必要があります。なお、診療情報提供書とは今までの診療経緯や薬の情報（使用禁忌の薬も含む。）等、患者の重要な情報が記載されているものです。
5） 在宅医療の継続にあたっては、患者及び家族と在宅主治医との間に確かな信頼関係を築くことが必要となります。
6） 容態の変化や療養環境の変化を把握するため原則として月二回以上の定期的な訪問診療を受ける必要があります。
7） 円滑な自宅での療養生活を継続していただくため、在宅療養（医療）をサポートする他の病院、診療所、助産所、薬局、訪問看護ステーション、介護事業者その他の関係者と連携を図る目的で、医療従事者や介護従事者その他の関係者が適切と認める通信手段を用いて診療情報を含む個人情報を共有・提供させていただきます。
8） 在宅医療期間中に患者から取得する個人情報の利用目的は裏面第１に記載のとおりです。

以上

（西暦）　　年　　月　　日

私は、上記事項について説明を受け、いずれも同意します。

＜患者＞

氏　　名	㊞
住　　所	

＜家族＞

氏　　名	㊞
住　　所	

［注：在宅をサポートする家族１名以上を記載することを想定しています。］

裏面

第１　患者の個人情報の利用目的

１　当施設での利用
（１）　患者に提供する医療サービス
（２）　医療保険事務
（３）　入退院等の病棟管理（もし必要があれば）
（４）　会計・経理
（５）　医療事故等の報告
（６）　患者への医療サービスの向上
（７）　当施設での医療実習への協力
（８）　医療の質の向上を目的とした当施設での症例研究
（９）　その他患者に係る管理運営業務
２　当施設外への情報提供としての利用
（１）　他の病院、診療所、助産院、薬局、訪問看護ステーション、介護事業者等との連携
（２）　他の医療機関等からの照会への回答
（３）　患者の診療のため、外部の医師等の意見・助言を求める場合
（４）　検体検査業務等の業務委託及びその他の業務委託
（５）　家族等への病状説明
（６）　その他患者への医療提供に関する利用
（７）　保険事務の委託
（８）　審査支払機関へのレセプトの提供
（９）　審査支払機関または保険者からの照会への回答
（10）　その他医療・介護・労災保険・公費負担医療等に関する診療費請求のための利用及びその照会に対する回答
（11）　事業者等から委託を受けた健康診断に係る事業者等へのその結果通知
（12）　医師賠償責任保険等に係る医療に関する専門の団体及び保険会社等への相談又は届出等
（13）　その他患者への医療保険事務に関する利用
（14）　患者個人を識別あるいは特定できない状態にした上での症例研究、発表及び教育
３　その他の利用
（１）　医療・介護サービスや業務の維持・改善のための基礎資料
（２）　外部監査機関への情報提供

［注：以下の通り患者の権利を追記しているものです。］

第２　患者が当施設の保有する個人データに対して有する権利

１　患者は、当施設の保有する個人データについて以下の権利を有しております。
①　当該データの利用目的の通知を求める権利
②　当該データの開示を求める権利及び第三者提供の停止を求める権利
③　当該データに誤りがある場合にその内容の訂正、追加又は削除を求める権利
④　当該データの利用の停止又は消去を求める権利
２　当施設の保有する個人データについてのお問い合わせ先は、下記の個人情報管理責任者までお願い致します。

氏名（　　）、連絡先（　　（　　）　　）

以上

表面

在宅医療の開始にあたって
（ご了解いただく事項）

患者の円滑な在宅での療養（医療）を実現するためには、患者をとりまく家族、医療従事者、介護従事者、その他の関係者が適切に連携していく必要があります。そのため適切な連携を行うにあたって下記の事項をご了承いただきますようお願い申し上げます。

記

1） 在宅医療は、医師による継続的な診療が必要であるにもかかわらず、外来受診が困難であるときに行うことができます。

2） 在宅医療は、医療環境が整った病院等で検査及び治療等を集中的に受けることよりも、家族のサポートのもとで住み慣れた自宅で安心して療養を継続することを重視して行われるものです。そのため、患者が在宅での療養（医療）を希望されているのはもちろんのこと、患者をとりまく家族においても意思の統一が図られている必要があります。

3） 在宅医療は、病院診療に比べて十分ではない事項（例えば以下の事項）があります。
　① 訪問（往診）に時間を要すること
　② 検査内容及び診療内容が限られており、かつ検査結果が出るまでに時間を要すること
　③ 衛生面や医療設備等について万全ではない部分があること

4） 在宅医療の開始にあたっては、これまでの担当医からの同意を得ており、診療情報提供書（紹介状）を入手する必要があります。なお、診療情報提供書とは今までの診療経緯や薬の情報（使用禁忌の薬も含む。）等、患者の重要な情報が記載されているものです。

5） 在宅医療の継続にあたっては、患者及び家族と在宅主治医との間に確かな信頼関係を築くことが必要となります。

6） 容態の変化や療養環境の変化を把握するため原則として月二回以上の定期的な訪問診療を受ける必要があります。

7） 円滑な自宅での療養生活を継続していただくため、在宅療養（医療）をサポートする他の病院、診療所、助産所、薬局、訪問看護ステーション、介護事業者その他の関係者と連携を図る目的で、医療従事者や介護従事者その他の関係者が適切と認める通信手段（医療介護専用のコミュニケーションシステム「メディカルケアステーション」（MCS）*を含む）を用いて診療情報を含む個人情報を共有・提供させていただきます。

［注：MCS の説明を以下の通り追記しています。］

*メディカルケアステーション（MCS）は、株式会社日本エンブレースが提供する医療介護専用のコミュニケーションシステムで、以下のような特長があり、必要に応じて利用する場合があります。

・医療介護従事者の連携を円滑に図るために、医療介護専用に開発されたシステムです。
・医療介護ならではのセキュリティ、アクセス制御、管理体系が整った完全非公開型のシステムです。
・災害時等でも医療介護従事者間での連携が取りやすいように配慮されたシステムです。

8） 在宅医療期間中に患者から取得する個人情報の利用目的は、裏面に記載のとおりです。

以上

裏面

患者の個人情報の利用目的

1　当施設での利用
（1）　患者に提供する医療サービス
（2）　医療保険事務
（3）　入退院等の病棟管理（もし必要があれば）
（4）　会計・経理
（5）　医療事故等の報告
（6）　患者への医療サービスの向上
（7）　当施設での医療実習への協力
（8）　医療の質の向上を目的とした当施設での症例研究
（9）　その他患者に係る管理運営業務
2　当施設外への情報提供としての利用
（1）　他の病院、診療所、助産院、薬局、訪問看護ステーション、介護事業者等との連携
（2）　他の医療機関等からの照会への回答
（3）　患者の診療のため、外部の医師等の意見・助言を求める場合
（4）　検体検査業務等の業務委託及びその他の業務委託
（5）　家族等への病状説明
（6）　その他患者への医療提供に関する利用
（7）　保険事務の委託
（8）　審査支払機関へのレセプトの提供
（9）　審査支払機関または保険者からの照会への回答
(10)　その他医療・介護・労災保険・公費負担医療等に関する診療費請求のための利用及びその照会に対する回答
(11)　事業者等から委託を受けた健康診断に係る事業者等へのその結果通知
(12)　医師賠償責任保険等に係る医療に関する専門の団体及び保険会社等への相談又は届出等
(13)　その他患者への医療保険事務に関する利用
(14)　患者個人を識別あるいは特定できない状態にした上での症例研究、発表及び教育
3　その他の利用
（1）　医療・介護サービスや業務の維持・改善のための基礎資料
（2）　外部監査機関への情報提供

以上

（西暦）　　年　　月　　日

私は、上記事項について説明を受け、いずれも同意します。

＜患者＞

氏　　名	㊞
住　　所	

＜家族＞

氏　　名	㊞
住　　所	

［注：在宅をサポートする家族１名以上を記載することを想定しています。］

表面

業務情報保持に関する誓約書

山田クリニック
院長　山田一郎　殿

第１条（業務情報保持の誓約）

私は、貴施設の業務の従業者として、法令（法律、政令、省令、条例、規則、告示、通達、事務ガイドライン等を含みます。）及び貴施設内の諸規定（就業規則、マニュアル等を含みます。）を遵守するとともに、以下の情報（以下、「業務情報」といいます。）の一切を、貴施設の許可なく、開示、漏えい又は使用しないことを誓約します。

① 患者、患者の家族及び貴施設に関わる者並びにこれらの関係者の一切の個人情報（氏名、生年月日、住所、病歴、治療歴、提供するサービスの計画、提供したサービス内容等のほか、特定の個人を識別することができるものを含みます。）

② その他貴施設内で知り得た情報（患者、患者の家族及び貴施設に関わる者並びにこれらの関係者の一切の情報はもちろんのこと、それ以外の貴施設内における情報も含みます。）

③ その他業務に関連して知り得た情報（業務に関連して第三者から提供された情報を含みますがこれに限られません。）

第２条（情報の管理等）*［注：以下の通りＩＴ機器取扱いの注意点を追記しています。］*

１　私は、貴施設の業務に関連して取得する情報（紙媒体のものだけでなく、電子データも含みます。）を貴施設の許可なく複写したり、外部に持ち出したり、又は外部に送信したりしないものとします。

２　私は、貴施設から貸与を受けた機器（携帯電話、ノートパソコンを含みますがこれらに限られません。）以外の機器を業務で使用する場合には、必ず貴施設の書面による許可を得るものとし、許可を得た機器以外の機器に情報を保存しないものとします。また、許可を得た機器に保存されている情報については、業務上不要となった時点で速やかに消去するものとします。

３　私は、貴施設のシステムにアクセスする際に、与えられたアクセス権限を超えた操作を行ったり、不正な手段を用いてアクセスを行ったりしないものとします。

第３条（利用目的外での使用の禁止）

私は、当該情報を貴施設が定める目的以外で利用しないものとし、かつ患者その他の第三者のプライバシーその他の権利を侵害するような行為を一切しないものとします。

第４条（退職後の業務情報保持の誓約）

私は、貴施設を退職した後も、業務情報の一切を、貴施設の許可なく、開示、漏えい又は使用しないことを誓約します。

第５条（損害賠償）

私は、本誓約書の各条の規定に違反した場合、貴施設が被った一切の損害を賠償することを誓約します。

年　　月　　日

住所

氏名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿印

業務情報保持に関する誓約書

山田クリニック
院長　山田一郎　殿

第１条（業務情報保持の誓約）

私は、貴施設の業務の従業者として、法令（法律、政令、省令、条例、規則、告示、通達、事務ガイドライン等を含みます。）及び貴施設内の諸規定（就業規則、マニュアル等を含みます。）を遵守するとともに、以下の情報（以下、「業務情報」といいます。）の一切を、貴施設の許可なく、開示、漏えい又は使用しないことを誓約します。

① 患者、患者の家族及び貴施設に関わる者並びにこれらの関係者の一切の個人情報（氏名、生年月日、住所、病歴、治療歴、提供するサービスの計画、提供したサービス内容等のほか、特定の個人を識別することができるものを含みます。）
② その他貴施設内で知り得た情報（患者、患者の家族及び貴施設に関わる者並びにこれらの関係者の一切の情報はもちろんのこと、それ以外の貴施設内における情報も含みます。）
③ その他業務に関連して知り得た情報（業務に関連して第三者から提供された情報を含みますがこれに限られません。）

第２条（利用目的外での使用の禁止）

私は、当該情報を貴施設が定める目的以外で利用しないものとし、かつ患者その他の第三者のプライバシーその他の権利を侵害するような行為を一切しないものとします。

第３条（退職後の業務情報保持の誓約）

私は、貴施設を退職した後も、業務情報の一切を、貴施設の許可なく、開示、漏えい又は使用しないことを誓約します。

第４条（損害賠償）

私は、本誓約書の各条の規定に違反した場合、貴施設が被った一切の損害を賠償することを誓約します。

年　　月　　日

住所

氏名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿印