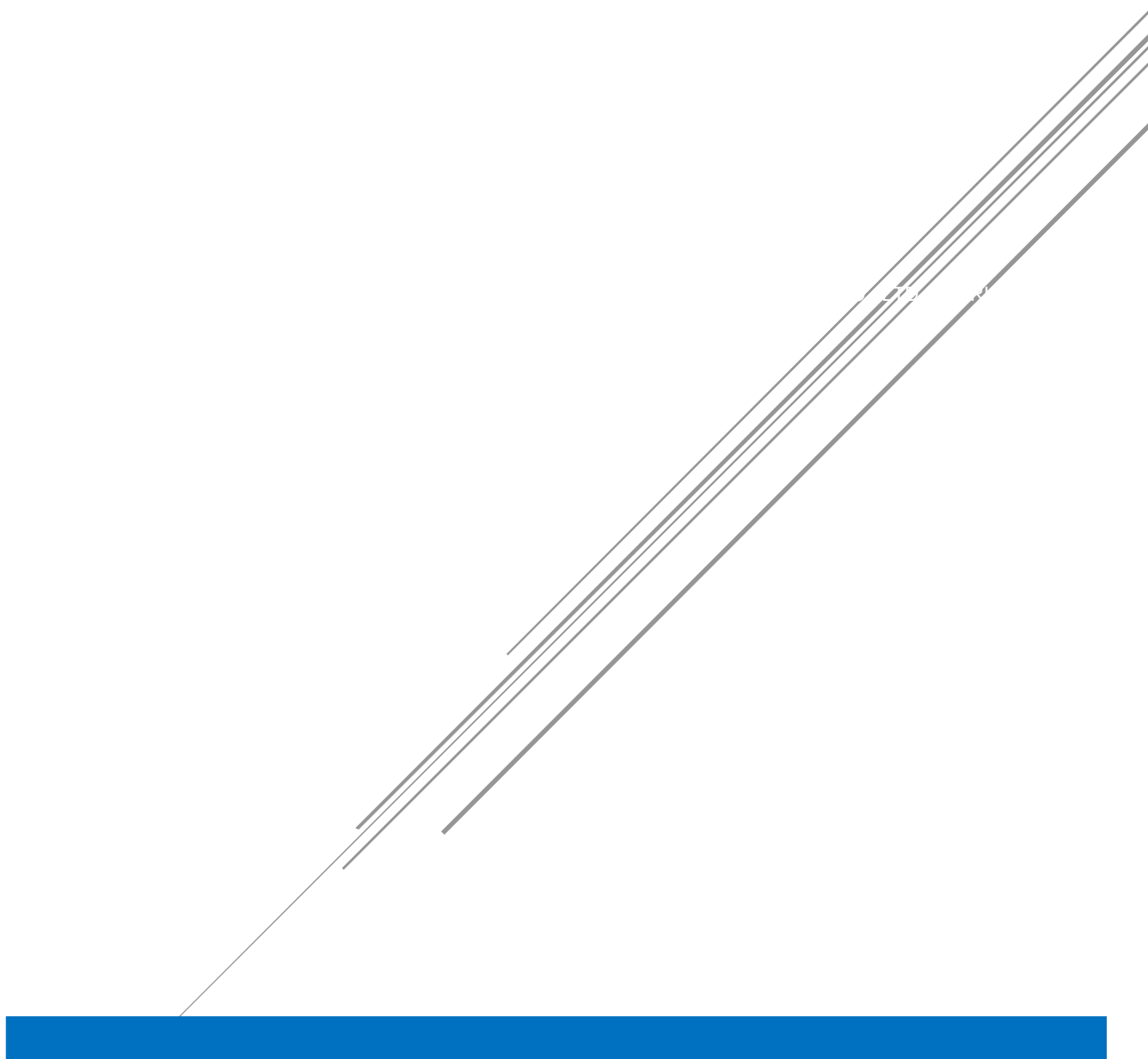


「MCS運用管理規程」

第1.3版(エンブレース株式会社 2024年9月11日改訂)



改訂履歴

版数	日付	内容
第1版	2021年5月	<ul style="list-style-type: none"> ・ 医療介護従事者向けに、MCSを利用する医療機関における医療情報の適切な安全管理および運用が実現されるため、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に基づき本運用管理規程を作成。
第1.1版	2023年4月	<ul style="list-style-type: none"> ・ 「5.患者同意」について、患者管理権限の移行に伴う患者情報保護・患者同意の取得しなおしに関する記述の追加。(5-3. 患者管理権限の移行に伴う同意の取得しなおしについて)
第1.2版	2024年4月	<ul style="list-style-type: none"> ・ 医療情報システムの安全管理に関するガイドライン第6.0版の記載内容を主として参照する形に変更。一部第6.0版には記載がないが安全にお使いいただくために有用と思われる内容について第5.2版の内容を参照しています。 ・ 医療情報連携加算の新設に伴い、患者同意書のひな型を統合し、内容を更新
第1.3版	2024年9月	<ul style="list-style-type: none"> ・ アプリ認証機能リリースに伴う、クライアント認証機能の新規提供停止に伴い、記述内容を更新

はじめに

厚生労働省「医療情報システムの安全管理に関するガイドライン 第6.0版」(※1)の経営管理編 第1章「安全管理に関する責任・責務」にある通り、医療情報の最終的な管理者としての責任は医療機関等(病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等、(以下、施設))にあります。

施設にて、「医師法」(昭和23年法律第201号)、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」(昭和35年法律第145号、以下、薬機法)、「個人情報の保護に関する法律」(平成15年法律第57号、以下、個人情報保護法)などの法令遵守はもちろん、「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ダンス」(平成29年4月14日付個情第534号・医政発0414第6号・薬生発0414第1号・老発0414第1号個人情報保護委員会事務局長・厚生労働省医政局長・医薬・生活衛生局長・老健局長通知、個人情報保護委員会と連名)や上述の「医療情報システムの安全管理に関するガイドライン」等に則って各種医療情報システムの適正な運用を行っていく必要があります。

その責任を完遂させるため医療情報システム等を提供する事業者は、医療情報の適切な利用と保護を目的に安全管理のためのリスクマネジメントを実施し、その結果をもとに医療機関等と適切な合意形成を図るべきであると「医療情報を取り扱う情報システム・サービス提供事業者における安全管理ガイドライン」(※2)において示されました。

当運用管理規程は、エンブレース株式会社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)を施設が運用するにあたり、上述の「医療情報システムの安全管理に関するガイドライン」に基づき、特に施設において対応を求める事項を整理したのになります。MCSを運用いただく場合、施設においてMCSの利用に関わるスタッフの方すべてに当運用管理規程の内容について周知し、理解及び遵守いただきますようお願いいたします。

また「医療情報システムの安全管理に関するガイドライン 第6.0版」の企画管理編第4章「医療情報システムの安全管理において必要な規程・文書類の整備」に記載されている通り、施設は医療情報システムの安全管理を適切に行うため、組織内において明文化されたルール等を定め周知、運用することが必要とされています。これらの運用管理規程や規則、マニュアルの整備の際、当運用管理規程の内容をご活用ください。

当運用管理規程についてはMCSを利用するすべての施設に対しその内容の理解及び遵守を求めるものですが、施設毎あるいはMCSを地域の情報連携ツールとして採用いただいた医師会等の団体毎に定められたセキュリティポリシー等によっては、当運用管理規程の内容以上のものを設ける場合があることを想定しています。そのためご施設あるいは地域独自の運用管理規程を作成いただく場合は当運用管理規程を「ひな型」としてその内容を含める、あるいは別途参照する形で作成・運用いただくようお願いいたします。

当資料は、法令や各省庁等の各種ガイドラインの改訂やMCSの機能変更などに伴って必要に応じて事前の告知なく改訂される場合があります。予めご了承ください。

目次

1. 基本的な考え方
2. 施設のMCS運用管理規程として定める必要がある事項・推奨事項
3. MCS管理者の設置とアクセス制御
4. スタッフ誓約書と教育
5. 患者同意
6. 参考情報

<用語>

<参考資料>

- ・患者同意書
- ・スタッフ誓約書

1. 基本的な考え方

MCSおよびMCSを提供するエンブレース株式会社(以下、エンブレース)は各種法令・制度上の要求事項を遵守し、各種ガイドラインに則ってMCSをご利用いただけるように各種システム上の設計や提供に係る体制を整備しています。しかしMCSをはじめとする各種医療情報システムの安全管理には、事業者と施設双方における適切な運用管理が必須となります。如何にMCSが堅牢なアクセス制御機能を有していたとしても、利用者がパスワードを利用端末に貼っていたり、アカウント情報を不特定多数で共有していれば、医療情報を守ることができません。

そのため適切な運用管理を実現するために、エンブレースがMCSを利用される場合に施設に求める対応を当運用管理規程に定めています。

1-1. 利用施設におけるリスクについて

「医療情報を取り扱う情報システム・サービス提供事業者における安全管理ガイドライン」では対象となる事業者に対し、提供する医療情報システム等特有のリスクに応じて適切な対応を行うためのリスクマネジメントのプロセスを定めています。エンブレースではこのリスクマネジメントを実践した結果特定したリスクについて、特にMCSを利用する施設と役割分担を明確化し、施設において対応をしなければならないものをここに整理します。なおここに記載されるリスクについてはすべてMCS利用者の端末や利用する場所(施設等の事業所や患家)におけるものであることを念頭に置いてください。

リスク (利用者の端末や利用場所 におけるリスク)	リスクの具体例
正当なもの以外による利用者個人情報/患者個人情報の不正な閲覧や作成、更新が行われる	<ul style="list-style-type: none">● アカウント情報を不正に取得した第三者によってMCSに不正にログイン・操作・閲覧等をされる● 紛失・盗難などで物理的に端末が第三者にわたり、端末内に保存されていたアカウント・パスワード情報が利用されMCSに不正にログイン・操作・閲覧等をされる
アプリケーション停止により、利用者個人情報/患者個人情報が見読不可になる	<ul style="list-style-type: none">● 地震等の災害により、物理的な断線や機器の破損が発生、または災害に起因する高負荷がMCSを提供するインフラに集中する等でネットワーク等に利用障害が発生しMCSを利用できなくなる

アプリケーションに混入した脆弱性の悪用により利用者個人情報/患者個人情報の漏洩・改竄・破壊が行われる	<ul style="list-style-type: none"> ● 悪意をもってMCS内のメッセージ等に添付された不正な働きをするファイルやフィッシングや攻撃を目的としたURL等を介して端末や利用ブラウザ等の情報が漏洩したり、端末の制御が奪われたり、端末に保管された情報が破壊される
利用者個人情報/患者個人情報の盗聴・なりすましが行われる	<ul style="list-style-type: none"> ● セキュリティ上欠陥のあるWi-FiからMCSを利用した際に、悪意ある第三者によって通信内容が盗み見られてしまう ● 自らの知り合いである医療・介護従事者を騙る悪意あるアカウントや不正な第三者に乗っ取られたアカウントとMCS上でつながり、情報を漏洩してしまう

1-2. リスクに対するエンブレースの対策について

1-1.において記されたリスクについて、エンブレースは各種法令やガイドラインに準拠、かつ利用者の利便性とセキュリティのバランスを踏まえて事業者として対策を講じており、MCS利用者に対して適用ないしは選択的な対策として提供しているものがあります。当運用管理規程においてはそれらの対策をエンブレースが事業者として行った上で施設に求める対応を定めたものになりますが、役割分担の明確化のためにその対策の内容についてここに整理します。

リスク (利用者の端末や利用場所におけるリスク)	事業者として講じている対策 ※利用者に対し選択的なものとして提供しているものについては (選択的)と記載
正当なもの以外による利用者個人情報/患者個人情報の不正な閲覧や作成、更新が行われる	<ul style="list-style-type: none"> ● MCSを利用するためには、利用者を一意に識別するID/パスワードによる認証を必要としている ● パスワードについては半角英数字を両方含む8文字以上でなければ設定ができないようにしている。また「医療情報システムの安全管理に関するガイドライン 5.2版」が定める「英数字、記号を混在させた13文字以上の設定」に対応している ● IDまたはパスワードを連続して3回以上間違えた場合、自動的に30分間アカウントロックされる ● 30分間操作が行われない場合、自動的にログアウトがなされる ● 事業者として定期的なデータバックアップの取得を実施している(オンラインで1日1回のバックアップし8世代分のバックアップを保存) ● (選択的)アプリ認証による2要素認証を提供している(※3)

<p>アプリケーション停止により、利用者個人情報/患者個人情報が見読不可になる</p>	<ul style="list-style-type: none"> ● MCSを提供するインフラにおける障害を検知し、即時対応できる仕組みを構築している ● MCSのインフラや開発環境等提供基盤については各種クラウドサービスを利用し、システムの冗長化を図り、BCP対策を行っている ● 事業者として定期的なデータバックアップの取得を実施している(オンラインで1日1回のバックアップし8世代分のバックアップを保存) ● WAF(Web Application Firewall)等を導入し、DDoS攻撃対策を実施している
<p>アプリケーションに混入した脆弱性の悪用により利用者個人情報/患者個人情報の漏洩・改竄・破壊が行われる</p>	<ul style="list-style-type: none"> ● アプリケーションの安全性・可用性について検証・評価するための各種テストを実施し評価結果に基づいた改善を行っている ● 各種セキュリティ対策(ウイルス対策、セキュリティパッチ等)についてはJPCERT/CCなどから最新のセキュリティ情報を収集し、脆弱性が発見されたものについては即時対応している ● WAF(Web Application Firewall)等クロスサイトスクリプティング(XSS)対策やSQLインジェクション対策を実施し、悪意のあるスクリプトの実行や埋め込みを実行できないようにしている ● 機密情報を保管しているデータベースを暗号化 ● ユーザーからアップロードされるファイルについてはウイルススキャンを実施し、悪意のあるソフトウェア等有害と検知されたファイルについてはアップロードされない処理を実施している
<p>利用者個人情報/患者個人情報の盗聴・なりすましが行われる</p>	<ul style="list-style-type: none"> ● クライアント端末とサーバーとの通信はSSL/TLS 1.2 の高セキュリティ型の設定により暗号化がなされています ● (選択的) 利用アカウントが医療介護従事者であることの本人認証(※4)サービスを提供しています ● (選択的) 患者の利用アカウントが患者本人によって操作されていることを確認しなりすましを防止するための患者本人確認機能を提供しています(※5)

2. 施設のMCS運用管理規程として定める必要がある事項・推奨事項

本項において1-1.において列挙されたリスクに対する対応として施設のMCS運用管理規程として定める必要がある事項・推奨事項を整理します。

特に施設のMCS運用管理規程として定める必要がある事項については、MCSを安全かつ適切にご利用いただくために必ず理解・遵守いただく必要のある項目ですが、推奨事項については施設の状況に応じてご利用いただける対応として挙げています。

対応については大きく下記の3つの観点でまとめています。

- 人的・組織的対策
- 物理的対策
- 技術的対策

また、MCSのサービスではない端末やネットワークの設定やソフトウェア・サービス等については(MCS外)と末尾に記載しています。

2-1. 人的・組織的対策

分類	対応事項
必要事項	<ul style="list-style-type: none">● アカウント情報(IDおよびパスワード)を紙や付箋など組織の内外を問わず他者がみる可能性がある場所などにメモしない● アカウント情報を組織の内外を問わず第三者と共有しない● 複数人で一つのアカウントの使いまわしをしない● 利用が終わったらログアウトする● 離席する等で利用端末から離れる場合ログアウトする● パスワードの設定は以下のいずれかを要件とすること<ul style="list-style-type: none">➢ 英数字、記号を混在させた13文字以上の推定困難な文字列➢ 英数字、記号を混在させた8文字以上の推定困難な文字列を定期的に変更する(最長2ヶ月以内)● 類推されやすいパスワードを使用しないこと● 類似のパスワードを繰り返し使用しないこと● 利用者が退職をする場合、アカウントの削除を行う● 端末を紛失してしまう、パスワードが流出した場合などで不正な利用が想定できる場合、パスワードの変更またはアカウントの停止申請を行う● MCS内にメッセージ等を投稿する際には投稿内容および投稿先をよく確

	<p>認の上行。またもし投稿内容や投稿先などに誤りがあったり、不適正な場合速やかにメッセージを削除する</p> <ul style="list-style-type: none"> ● MCS内の特定のグループ内の投稿情報等を口頭や画面のスクリーンショット等の手段でグループ参加者以外に共有しない ● MCS内のファイルをダウンロードする場合、信頼できない利用者のものはダウンロードしない ● MCS内に投稿されたURL(リンク)について信頼できない利用者のものや怪しいものについてはアクセスしない ● MCSの偽サイト(見た目がMCSそっくりな偽サイト)やMCSを偽るメール等に注意する ● MCSのアプリ版を利用する場合、正規の手段である「App Store」または「Google Play」で入手しインストールし、それ以外の手段で入手したものをインストールしない ● MCSを利用する端末についての管理方法を定めること ● MCSが利用できなくなった際のバックアッププランを予め定めておく
推奨事項	<ul style="list-style-type: none"> ● 登録後、利用者個人のプロフィール・顔写真を設定する ● 利用者が新規登録した際には本人認証(※4)を行う ● 患者のアカウントが登録された場合には患者本人確認(※5)を行う

(補足)

アカウントおよびパスワードに関する必要事項については「医療情報システムの安全管理に関するガイドライン 第5.2版」の「6.5.技術的安全管理対策」「C. 最低限のガイドライン」記載事項と共通しています。
アカウントの情報については原則として1利用者1アカウントの利用をお願いしています。

不正な第三者によるアカウント情報の取得、不正なアクセス、なりすまし等を防ぐためにも利用者が退職・異動、担当から外れるなどで利用の予定がなくなる場合はアカウントの削除(退会)をお願いしています。
アカウントの削除についてはアカウント保有者にのみ行っていただけますが、MCSサポートデスク(※6)へお問い合わせいただければ施設の管理者の方などに代表して停止・削除いただくことも可能です。

MCSでは個人プロフィール・顔写真を設定することができます。利用者毎にプロフィールを設定し、顔写真を設定することで、自他問わずMCSを通じて連携する施設の利用者から識別されやすくなります。本人認証やこのような設定を行うことで利用アカウントの信頼性を確保することを推奨しております。
また、機微情報を含むグループにアカウントを招待する・承認する際にはプロフィールや顔写真の設定状況を招待や承認の条件にする等運用管理規程の策定の参考にしてください。

MCSでは患者情報を交換するグループや地域の勉強会のグループ等様々なグループを多数作成して情報共有を行うことができます。グループ機能は、グループ毎に参加者を限定し、グループ非参加者にはグループ内の投稿情報を参照することができないようになっています。しかし投稿先を間違える・投稿内容に関係のない第三者の情報が含まれる

等、投稿先グループに共有すべきではない情報が含まれていると情報漏洩等につながってしまいます。投稿前には投稿先・投稿内容についてよく確認するようにしてください。

MCSの偽サイトや偽アプリ、MCSを偽るメールやSMSに注意するようにしてください。

MCSの正規URLは < https://www.medical-care.net/**/ >です。(**)には「login」や「home」などの文字列が入ります)リンクからMCSにアクセスする場合は正規のサイトURLであるかを確認してください。

MCSのシステムメール(※7)のアドレスは < no-reply@medical-care.net >、MCSサポートデスク(※6)のアドレスは < support@embrace.co.jp >です。エンブレース社の広報用メールアドレス< 例: press@medical-care.net、event@medical-care.net >やエンブレース社員のアドレスは@以降がembrace.co.jpとなっています。これらのアドレス以外からのメールでMCSやMCSの運営等と偽り名乗るメールについてはフィッシングやランサムウェア等のコンピュータウイルスへの感染等の攻撃を目的とした危険なメールである可能性があります。添付ファイルやリンクなどを開かないようにしてください。

スマートフォン・タブレットで利用できるMCSのアプリ版の正規の入手手段は、iOS端末をお使いの場合「App Store」、Androidアプリをお使いの場合「Google Play」からのインストールのみとなっています。ipaファイルやapkファイル、あるいはそれらを含むアーカイブファイルをインターネットや他者から入手する等の正規以外の手段で取得しインストールを行わないでください。

MCSを利用する端末については、端末自体の管理や施設内のどの端末で利用をするのか、モバイル端末などを施設外に持ち出す場合に管理者の事前の承認を得るようにするなど管理方法を定めるようにしてください。

万が一災害等でMCSを利用することができなくなった場合、直接口頭、電話やFax等別手段で連絡をとれるようにしておく等バックアッププランを施設として定め、施設内外の利用者に周知するようにしてください。

2-2. 技術的対策

分類	対応事項
必要事項	<ul style="list-style-type: none">● 利用端末について長時間操作を行わない場合、クリアスクリーン等の対策を実施すること(MCS外)● 利用端末について常時コンピュータウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとり、その有効性・安全性の確認・維持を行うこと(MCS外)● 無線LAN(Wi-Fi)に接続して利用する場合、WPA2-AES、WPA2-TKIP等通信が暗号されているものから接続し、暗号化されていない・管理者の正体不明等の信頼できない無線LANに接続して利用しないこと

<p>推奨事項</p>	<ul style="list-style-type: none"> ● 利用端末にPIN・パターン・パスワードなどによるデバイスロックの設定をする(MCS外) ● 利用端末のOSのバージョンを常に最新のものに更新する(MCS外) ● パスワード管理ツールなどの利用をする(MCS外) ● アプリ認証(※3)を行った端末での利用をする ● 端末をVirtual Private Network(VPN)接続をした状態で利用する(MCS外) ● 自施設外においてモバイル端末については自端末の携帯電話回線あるいはモバイルルータでインターネットに接続して利用する(MCS外) ● リモートワイプサービス・モバイルデバイス管理サービス(MDM)の利用(MCS外)
-------------	---

(補足)

必要事項については「医療情報システムの安全管理に関するガイドライン 第6.0版」の第12章「物理的安全管理措置」や第13章「ネットワークに関する安全管理措置」等で定められた遵守事項と共通しています。

MCSの利用についてはインターネットの接続が必須ですが、特に無線LANを利用する場合、事業所などの無線LANの設定が安全であるか、公衆無線LANへの自動接続設定を見直すなど盗聴対策を十分に行っていただくことを推奨します。

端末内にデータやアカウント情報を一切残さないことが理想ですが、端末を紛失する等万が一の際に端末に残るデータをリモートで削除するリモートワイプサービスやデバイスをロックしたり、位置情報によってデバイスの位置を把握したりすることができるMDMの利用なども状況に応じてご検討ください。

2-3. 物理的対策

分類	対応事項
必要事項	<ul style="list-style-type: none">● モバイルの利用端末を保管する場合保管場所に鍵をかけるなど利用していないときに不特定個人が利用できる状態にしない
推奨事項	<ul style="list-style-type: none">● モバイルの利用端末には覗き見対策の実施を行う

(補足)

利用端末の紛失や盗難を避けるためにも利用端末の保管場所に鍵を掛ける、コンピュータに物理的なセキュリティロックを施す等の物理的な対策を実施してください。

3. MCS管理者の設置とアクセス制御

医療情報システムの安全管理に関するガイドライン 第6.0版(※1) 第3章の「医療情報システムにおける統制上の留意点」において遵守事項として「医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること」としています。

規模や必要に応じて、上記ほか情報システム運用担当者、企画管理者や運用担当者とは独立した監査を実施する組織、医療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、医療情報システム安全管理責任者の方または企画管理者の方が、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。

「2. 施設として運用管理規程に定める必要がある事項・推奨事項」の内容を熟知した上で施設のMCS運用管理規程を設定し、それが施設の全利用者によって遵守の上運用されるよう努めてください。

3-1. 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りますので、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管理者ユーザーの権限を保有し、MCSの利用環境・MCS内の情報管理等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管理者ユーザーのみが利用できるMCSの管理機能です。

3-2. 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管理者ユーザー(管理者権限を持つ医療介護従事者)

- ・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が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 の管理者ユーザーは、施設として担当しなくなった患者について、「保管機能」を使って速やかに保管庫に移す。
- ・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管理者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書き込んだ内容の削除を行う。
- ・MCSの管理者ユーザーも、以下に示すMCSユーザーの利用方法を遵守する。

(2) MCS ユーザー(管理者権限を持たない医療介護従事者)

- ・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
- ・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、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、アカウントの削除など、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、医療情報システムの安全管理に関するガイドライン 第5.2版(※1)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。

- ・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。
- ・参照した情報を、目的外に利用しないこと。
- ・患者のプライバシーを侵害しないこと。
- ・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。
- ・不正操作・アクセスを発見した場合、速やかに管理者に連絡し、その指示に従うこと。

4. スタッフ誓約書と教育

医療情報システムの安全管理に関するガイドライン 第6.0版(※1) 企画管理編 第7章「安全管理のための人的管理」の遵守事項として、「医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。」「個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。」としています。

4-1. 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程を遵守し、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。

4-2. スタッフ教育

施設ごとに作成したMCS運用管理規程を徹底するために、施設責任者によって、MCS管理者および利用者に対して、定期的に教育を行っていきましょう。また、MCSの位置づけを利用者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。

5. 患者同意

MCSを用いて患者情報を取り扱う場合、MCSへ当該患者情報を登録した施設が患者情報の管理権限を有する施設として患者情報保護に主たる責任を負うこととなります。また、他施設とつながる多職種連携は患者・介護利用者の個人情報・個人データを法人を跨いで第三者提供することになるため、患者本人の同意が必要です。

個人情報の適切な取り扱いのためにも、MCSを用いて患者情報を自施設外と共有する場合や、治療や介護などの目的外で情報を利用する場合などには同意を取得した上でMCSをご利用ください。

5-1. 多職種連携のための患者同意取得の方法

患者本人からの同意取得については実務上「オプトイン方式」または「黙示の同意」の2つの方法が用いられていますが、MCSの利用に伴う多職種連携には、黙示の同意に頼ることなく、オプトイン方式を推奨しています。

オプトイン方式は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。例えば、患者ごとに患者同意書を交わす方法が該当します。

5-2. 患者同意書について

オプトイン方法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、最適なもので同意を取るようになしてください。また、患者の希望により同意できない部分がある場合、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。

5-3. 患者管理権限の移行に伴う同意の取得しなおしについて

主治医の変更などの事由により、自施設において同意を取得し、MCSに登録した患者情報の管理権限を他施設へ移行する場合、移行先の施設で患者情報の適切な取り扱いを行い、個人情報保護に責任を負う旨の承諾を得た上、移行を行ってください。また、他施設において同意を取得しMCSに登録された患者情報の管理権限を自施設に移行する場合、当該患者情報の主たる管理責任を負うこととなります。事前に自施設において患者本人の同意を改めて取得しなおしてください。

6. 参考情報

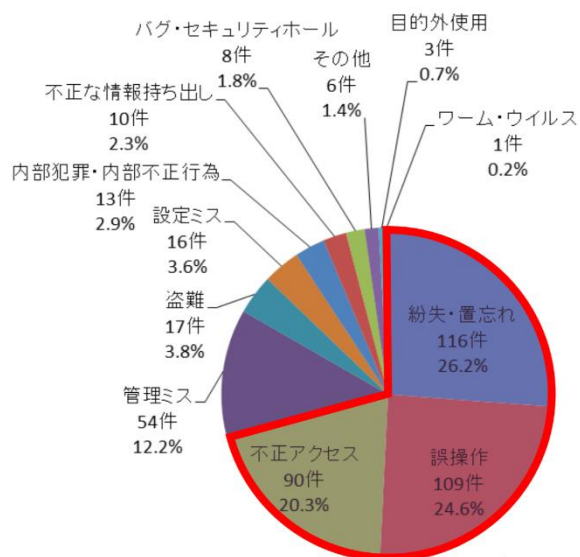
6-1. 個人情報漏えいの現状について

・個人情報漏えいの原因について

以下は、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による、2018年の個人情報漏えいの原因別調査結果です。この調査結果では、紛失・置き忘れ(26.2%)、不正アクセス(20.3%)の2つで50%弱を占めています。MCSを利用する端末の紛失・盗難時や不正アクセス防止の情報漏えいリスクを回避するためにもアカウント情報や利用端末の管理の徹底が重要になります。

また、紛失・置き忘れ(26.2%)、誤操作(24.6%)、管理ミス(12.2%)、設定ミス(3.6%)など情報漏えいの約2/3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。

原因別 漏えい件数

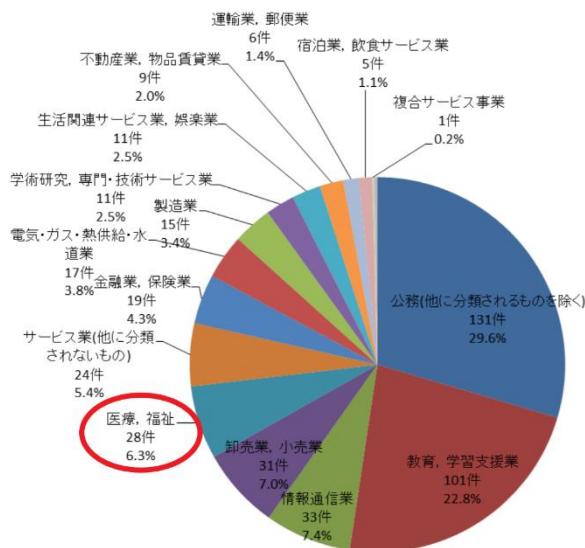


出典：NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ報告の「2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～(速報版)」

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6.3%です。漏えいしている事実を目を向けて、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「2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～(速報版)」

6-2. 運用管理規程の作成のために参考となる資料(ガイドラインを除く)


運用管理規程を作成・運用するにあたってガイドラインや当運用管理規程以外に参考となる資料をこちらで紹介します。


- 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)発行「情報漏えい発生時の対応ポイント集」
 - 情報漏えいが発生した際の手順や調査の方法について詳しく知ることができます。
- 内閣サイバーセキュリティセンター発行「インターネットの安全・安心ハンドブック」
 - サイバー攻撃やインターネットに関する技術のセキュリティについて図解で詳しく解説があり、対策についてもまとめられています。

用語

注釈番号	用語名	内容
1	医療情報システムの安全管理に関するガイドライン	<p>医療情報システムの安全管理に関するガイドラインとして技術的及び運用管理上の観点から医療機関等に求められる所要の対策を示したもの。</p> <p>平成17年3月31日「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」(医政発第0331009号・薬食発第0331020号・保発第0331005号厚生労働省医政局長・厚生労働省医薬食品局長・厚生労働省保険局長連名通知)の別添として、個人情報保護に資する情報システムの運用管理、個人情報保護法への適切な対応等について示されました。</p> <p>その後平成29年5月にガイドライン第5版が策定されましたが、近年のサイバー攻撃の手法の多様化・巧妙化、情報セキュリティに関するガイドラインの整備、地域医療連携や医療介護連携等の推進、クラウドサービス等の普及等に伴い、医療機関等を対象とするセキュリティリスクが顕在化していることへの対応として、情報セキュリティの観点から医療機関等が遵守すべき事項等の規定を設けるなど所要の改定が行われ、令和3年1月「医療情報システムの安全管理に関するガイドライン 第5.1版」が策定されました。</p> <p>全体構成の見直しや新技術・制度・規格への対応内容が盛り込まれた令和5年5月「医療情報システムの安全管理に関するガイドライン 第6.0版」が策定されました。</p>

2	医療情報を取り扱う情報システム・サービス提供事業者における安全管理ガイドライン	<p>医療機関等との契約等に基づいて医療情報システムやサービス(以下、医療情報システム)を提供する事業者を対象に、提供する医療情報システム等について、医療機関等と義務や責任についての合意形成を図ることが求められている。</p> <p>両者間における適切な合意形成のために、必要な安全管理のための情報の共有、役割分担の明確化、医療情報システム等の安全管理に係る評価の共有等がなされる必要があり、その手段等(情報提供項目やリスクマネジメント手法)について事業者に求められる責任を示したものの。</p> <p>令和2年8月に総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」、および経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」が定める要件を整理・統合したガイドラインである。</p> <p>令和5年7月「医療情報システムの安全管理に関するガイドライン」への対応のため改定(第1.1版)</p>
3	アプリ認証	<p>アプリ認証とは、MCSへのログイン時にモバイル端末にインストールした認証アプリで認証コードを取得し、認証する、いわゆる「二段階認証機能」に該当する機能となります。</p> <p>本機能を有効にすることによってMCSへのログイン時にパスワード以外にもモバイル端末で受け取る認証コードが必要となるため、第三者による不正使用のリスクを軽減することができます。</p> <p>利用者の求めるセキュリティポリシーに応じてお使いいただけるよう選択的に機能提供しています。</p>

		<p>下記リンクより詳細をご確認ください。</p> <p>https://support.medical-care.net/hc/ja/articles/36906789136409-%E3%82%A2%E3%83%97%E3%83%AA%E8%AA%8D%E8%A8%BC%E3%82%92%E8%A8%AD%E5%AE%9A-%E8%A7%A3%E9%99%A4%E3%81%99%E3%82%8B</p>
4	本人認証	<p>MCSにおける本人認証は当該アカウントの持ち主が本人であり、かつ医療介護従事者であることをメディカルケアステーション事務局が認証する本人認証サービスを選択的に提供しています。本人認証が完了したアカウントについてはアカウントのアイコンの右下にチェックマークが付くようになり、本人認証が完了している</p>  <p>ことが他の利用者からわかるようになります。</p> <p>MCSに登録後各職種の登録証や認定証などをMCSの設定 > 本人確認 > 医療介護関係者の認証をする より本人認証を行います。</p>
5	患者本人確認	<p>患者のアカウントについて、そのアカウントが患者本人であることを確認し、信頼性を担保し、なりすましを防止するための機能で選択的に利用することができます。</p> <p>本人確認が完了した患者アカウントについては本人確認マークがアイコンの右上に表示されるようになり、他の利用者からわかるようになります。</p>

		 <p>この機能の利用の方法については下記リンクより「MCS 医療介護関係者による患者本人確認と患者情報修正方法」の操作資料をご覧ください。</p> <p>https://www.medical-care.net/html/usersguide/download/pdf/mcs_patient_edit.pdf</p>
6	MCSサポートデスク	<p>MCSの導入方法・サービス内容についてのお問い合わせ窓口です。</p> <p>受付時間: 平日9:00～18:00</p> <p>下記リンクのお問い合わせフォームよりお問い合わせいただけます。</p> <p>https://about.medical-care.net/html/contact/</p>
7	MCSシステムメール	<p>MCSにアカウントを作成した際にアカウントのIDとしてご登録いただいたメールアドレスへ、MCSから送られる各種通知のメールを指します。</p> <p>他の利用者から新たに招待されたり、承認依頼や参加グループやつながりへのメッセージ受信などがあつた際に送信されるものです。(メールによる通知についてはオンオフの設定ができます)</p>

<参考資料>

・患者同意書

ひな型: 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、MCSの説明を追記したものです。個人情報の利用目的の明細が記述されています。

在宅医療情報連携加算等の算定要件として記載されている、下記のポイントについてMCSを用いて行う旨を記載しています。

- ・ 「当該保険医療機関の医師が、医療関係職種等によりICTを用いて記録された患者の医療・ケアに関わる情報を取得及び活用した上で、計画的な医学管理を行うこと。」
- ・ 「医師が診療を行った際の診療情報等についてICTを用いて記録し、医療関係職種等に共有すること。」
- ・ 「当該保険医療機関の患者の医療・ケアに関わる者が、患者の人生の最終段階における医療・ケア及び病状の急変時の治療方針等についての希望を患者又はその家族等から取得した場合に、患者又はその家族等の同意を得た上でICTを用いて医療関係職種等に共有できるように記録すること」

・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。

在宅医療の開始及び個人情報の取得・利用に関する同意説明書

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、ご同意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) 医師が計画的な医学管理を行い、患者が円滑な在宅での療養生活を継続していただくことを目的に、在宅療養(医療、介護)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、介護事業者等の医療関係職種と連携し、ICTツール(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)*)を用いて下記の情報を相互に共有させていただきます。
 - ・ 医師が患者の診療を行った際の診療情報
 - ・ 医療関係職種が記録した患者の医療・ケアに関わる情報
 - ・ 医師及び医療関係職種が患者の人生の最終段階における医療・ケア及び病状の急変時の治療方針等についての希望を患者・家族から取得した情報
- *メディカルケアステーション(MCS)は、エンブレース株式会社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、医療介護専用開発されたシステムです。
 - ・ 医療情報等を安全に取り扱うためのセキュリティ、アクセス制御、管理体系が整った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。

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

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

在宅医療の開始及び個人情報の取得・利用に関する同意書

山田クリニック
院長 山田一郎 殿

私は、在宅医療の開始およびそれに伴う個人情報の取得と利用について、説明担当者より説明を受け、その趣旨・内容について理解し、同意します。

以上の同意を証するため、以下の欄に記入し、署名をします。なお、この同意書(以下「本同意書」といいます。)の写しを受け取りました。

(西暦) _____ 年 _____ 月 _____ 日

<患者>

氏 名	_____ (印)
住 所	_____

<家族>

氏 名	_____ (印)
住 所	_____

[注1: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。]

[注2:同意書の写しを作成しお渡しすることを想定しています。]

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