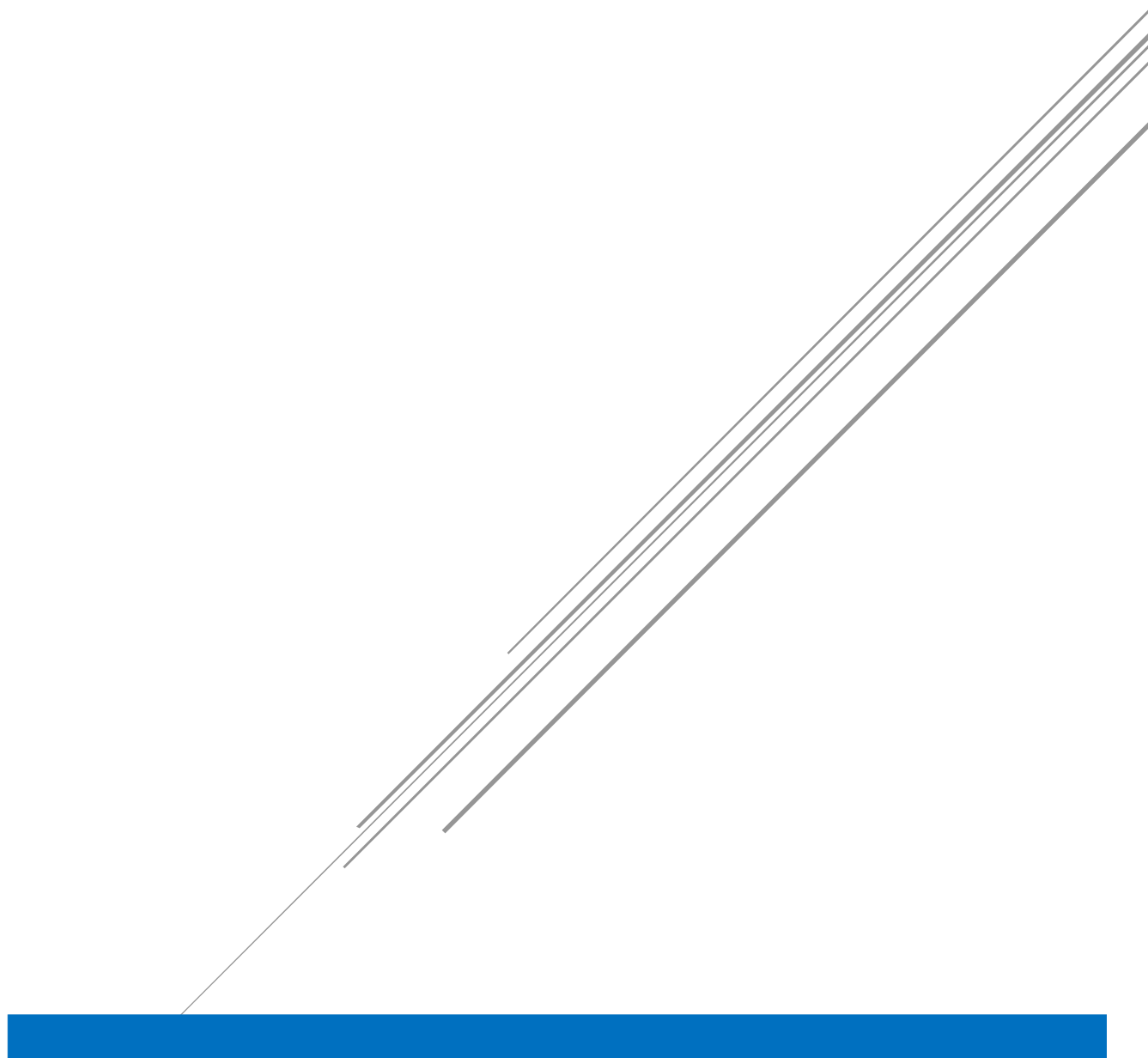


「エンブレースの安全管理に関する情報提供」

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	<p>医療介護従事者向けに、エンブレース株式会社におけるMCSの安全管理に関する情報提供を目的として作成。</p> <p>医療機関等が「医療情報システムの安全管理に関するガイドライン」(※1)に基づき、医療情報を取り扱う情報システム・サービスの事業者選定にあたり必要な情報共有を得られるよう「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ガイドライン(※2)」の内容に準拠。</p>
第1.1版	2022年4月	<p>エンブレース株式会社の役員変更に伴い、1-2. 医療情報等の安全管理に係る実施体制の整備状況の内容変更。</p> <p>2-2. MCSシステムの全体構成図へシステムを構成するインフラ・運用に必要な業務が国内で完結している旨追記。</p>
第1.2版	2024年4月	<p>エンブレース株式会社の役員変更に伴い、1-2. 医療情報等の安全管理に係る実施体制の整備状況の内容変更。</p> <p>医療情報システムの安全管理に関するガイドラインの第6.0版の内容を参照する形で各記述の変更。</p> <p>MCSシステムの構成更新に伴い、全体構成図を更新。</p>
第1.3版	2024年9月	<p>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</p>

はじめに

MedicalCareStation(以下、MCS)を運営するエンブレース株式会社(以下、エンブレース)から、MCSの利用を検討する、または利用をしている医療機関等(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))に対してMCSの安全管理に関する情報提供を目的として当資料を用意しています。

MCSの利用に際しては大前提として法令遵守はもちろん適用ガイドラインに準拠いただいた上、当資料およびMCSを利用される際に運用管理規程として施設に定めていただきたい内容をまとめた「MCS運用管理規程」、そしてMCSの各種利用規約等の内容についても十分理解・合意の上ご利用ください。

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. MCSの安全管理に関する運用体制・基本方針等
2. 施設との共通理解を形成するための情報提供等

<用語>

1. MCSの安全管理に関する運用体制・基本方針等

1-1. 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況

エンブレースが医療情報を取り扱う情報システム・サービス提供事業者として安全管理義務を果たし、適切にMCSを提供するために定めている方針・規程等をこちらにまとめています。

項目	開示先・作成状況等
情報セキュリティポリシー	<ul style="list-style-type: none">● 下記URL上、MCSプロモーションサイト上に開示● https://www.medical-care.net/html/informationsecurity/
個人情報保護方針(プライバシーポリシー)	<ul style="list-style-type: none">● 下記URL上、MCSプロモーションサイト上に開示● https://www.medical-care.net/html/privacypolicy/
機密情報管理規程	<ul style="list-style-type: none">● 社内公布(2019年9月18日制定、2020年6月1日改訂)● 役職員が職務上知り得た機密情報(MCS及び関連アプリ等によって知り得たすべて施設情報、医療介護従事者、福祉、行政従事者、患者・家族等のすべての個人情報含む)を故意・過失問わず第三者への漏洩を禁じ、退職後も機密保持義務の遵守を定めたもの。
個人情報管理規程	<ul style="list-style-type: none">● 社内公布(2020年6月1日制定)● 役職員の個人情報の取り扱いについて個人情報保護法やその他最新の関連法令の遵守、個人情報保護体制の実施及び運用について定めたもの。
特定個人情報管理規程	<ul style="list-style-type: none">● 社内公布(2020年6月1日制定)● 「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「特定個人情報の適正な取り扱いに関するガイドライン(事業者編)」に基づき、会社の取り扱う特定個人情報の適正な取り扱いを確保するために定める事項を定めたもの。

1-2. 医療情報等の安全管理に係る実施体制の整備状況

情報セキュリティに関する役職	役職及び氏名	役割
管理責任者	<ul style="list-style-type: none"> ● 荒木 真哉 ● 代表取締役社長 	<ul style="list-style-type: none"> ● 最終的な管理責任者として医療情報の安全管理に係る実施体制の構築および実施に責任を持つ
システム管理者	<ul style="list-style-type: none"> ● 濱口 和喜 ● 執行役員 / デベロップメント・カスタマーサクセス ディビジョンディレクター 	<ul style="list-style-type: none"> ● 十分な技術的能力及び経験を有し、MCSのシステムの運用状況管理、リスク管理等を行う ● システムにおける個人情報に関するリスク(不正アクセス、紛失、盗難、滅失、破壊、改ざん、漏洩等)に対し、必要且つ適切な安全管理対策を講じる
運用管理責任者	<ul style="list-style-type: none"> ● 吉田 功一郎 ● 常勤取締役 	<ul style="list-style-type: none"> ● MCSの運用に関する事務を統括
個人情報保護責任者	<ul style="list-style-type: none"> ● 荒木 真哉 ● 代表取締役社長 	<ul style="list-style-type: none"> ● 個人情報保護体制の実施及び運用に関する権限と責任を有し、社内における個人情報の統括管理を行う

1-3. 実績等に基づく個人データ安全管理に関する信用度

実績	内容
個人情報流出事故がない	<ul style="list-style-type: none"> ● 2013年7月16日のサービス開始以降、MCSにご登録いただいた個人情報システムまたは運営元であるエンブレースより漏洩したという事故は発生していません
受託情報の目的外利用、不当利用等を行っていないこと	<ul style="list-style-type: none"> ● MCSにご登録いただいた個人情報について事前の同意なくサービスの提供に必要な目的を超えての利用を行っていません
情報セキュリティに係る公的な第三者認証	<ul style="list-style-type: none"> ● プライバシーマーク認定（登録番号 17001617） ● ISMS認証(ISO/IEC 27001:2013 (JIS Q 27001:2014)) (2020年取得) ● ISMSクラウドセキュリティ(ISO/IEC 27017:2015)(2023年取得)

1-4. 財務諸表等に基づく経営の健全性

項目	開示先・内容
財務諸表等	<ul style="list-style-type: none"> ● エンブレース株式会社は、2021年4月をもって株式会社スズケン（東証一部上場：証券コード9987）の連結子会社になっております ● 株式会社スズケンの連結財務諸表等は、以下URLで公表しております。IRライブラリ https://www.suzuken.co.jp/ir/library/

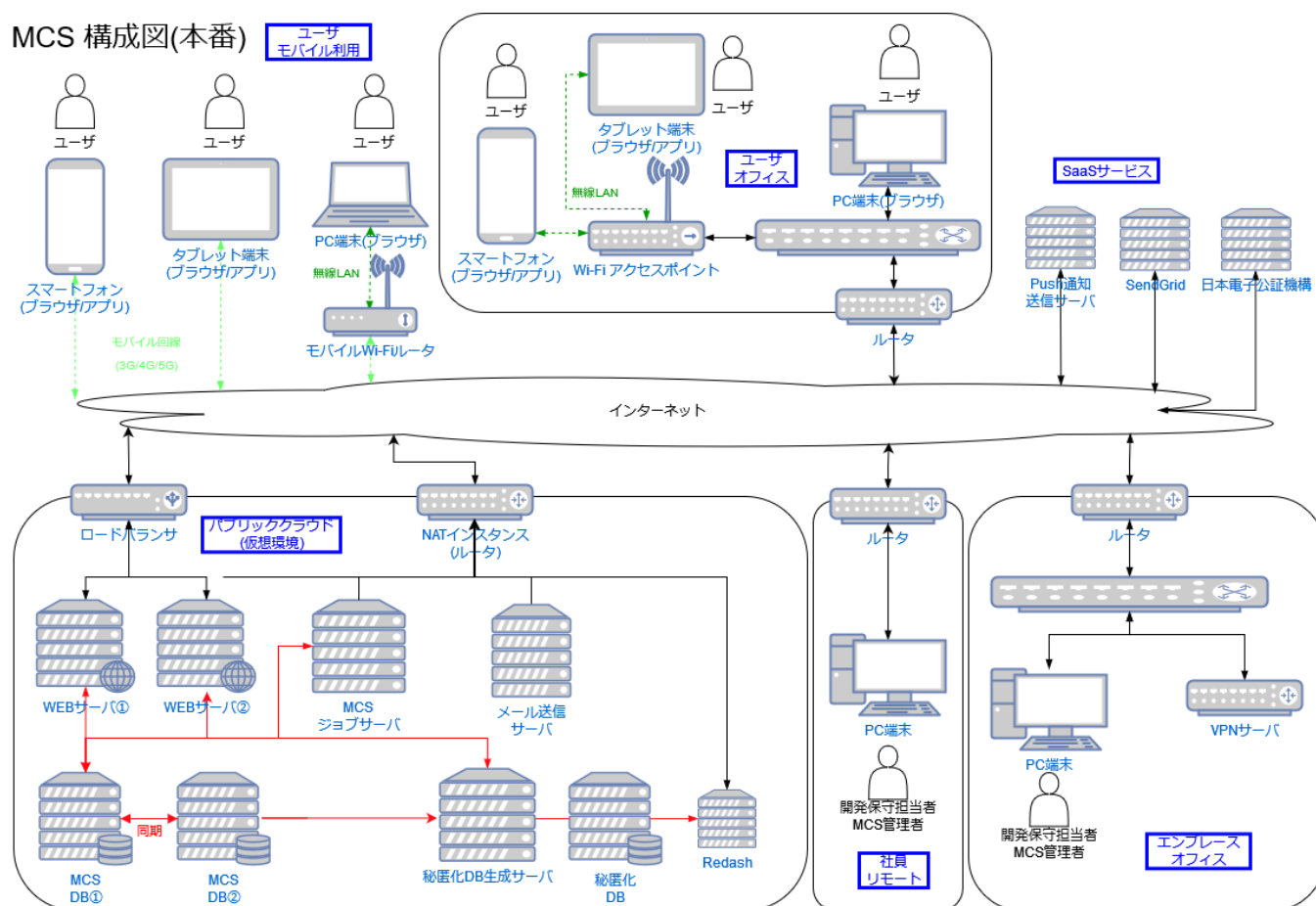
2. 施設との共通理解を形成するための情報提供等

2-1. 施設等の運用管理規程に定める必要がある事項

別途「MCS運用管理規程」の形でまとめて提供しています。
内容については下記リンク先ページより最新版をダウンロードいただけます。

情報開示先: https://about.medical-care.net/html/service/guideline_docs.html

2-2. MCSのシステムの全体構成図



MCSの運用に必要なインフラ(サーバ等)はすべて日本国内のものを運用しています。MCS上に保存・記録される情報についてはすべて国内法の適用範囲内となります。またMCSのシステム運用について国外への業務委託は行っており、国外にある事業者がMCSの運用システムやデータ等にアクセスしたり、国外サーバへデータが移管・保管されることはありません。また、エンブレースも国外向けにはサービス展開しておりません。

2-3. リスク対応

リスクマネジメントについては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の5章安全管理のためのリスクマネジメントプロセスに則り実施をしています。

特に利用者側におけるリスクに対する事業者としての対応の内容については、2-1. の「MCS運用管理規程」内「1-2. リスクに対するエンブレースの対策について」に記載をしております。

2-4. MCSの安全管理に係る基本方針

MCSの安全管理に関する基本方針として、以下の事項を遵守・準拠しております。

- 「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」及び「医療情報システムの安全管理に関するガイドライン」
- 個人情報保護法やその他最新の関連法令等の遵守
- 個人情報の保護に関する法律についてのガイドライン(通則編、外国にある第三者への提供編、第三者提供地の確認・記録義務編)
- 個人情報保護委員会及び厚生労働省が定める「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)」に基づき、患者等が死亡した後においても、当該患者等の情報を保存している場合には、死者に係る情報であっても、個人情報と同等の安全管理措置の実施
- 個人情報保護方針(プライバシーポリシー)策定およびその遵守を担保する組織体制の構築

2-5. MCSの提供に係る体制

(a)サービス提供体制

部門	役割
ディベロップメントディビジョン	● MCSの情報システムに関する運用管理・監視・開発等を行うシステムの統括部門
カスタマーサクセスディビジョン	● MCSの利用者・利用検討者との問い合わせ対応を行う部門

(b)サービス提供に係る再委託の状況

再委託事業者の有無	再委託事業者がある場合、再委託業務の内容
無	無

2-6. 契約書・マニュアル等の文書の管理方法

原則としてMCSの利用施設とは契約書の取り交わしを行っておりません。例外的に契約書を取り交わすケースや群市区医師会・法人等と契約書を締結する場合、社内のコーポレート部門のみがアクセス可能な施錠された金庫内に原本を保管し、写しをクラウド上のデータベースにて厳密なアクセス制限を施した上保存しております。

社内規程や運用管理規程等についてもクラウド上のデータベースに保存し、運用に係る担当者が随時閲覧できるようにしております。

2-7. 事故発生時の対応方法及び施設等への報告方法

- 受託する医療情報が漏洩した場合には、原因の究明、被害拡大の防止、所管官庁への報告及び指示への対応、その他利用者・患者の情報の安全性の確保に必要な対応を行います。
- 受託する医療情報が漏洩した場合、漏洩状況についてMCSプロモーションサイト(<https://www.medical-care.net/html/>)およびMCS内の事務局お知らせよりご連絡いたします。
- 受託する医療情報が漏洩した場合、その被害にあわれた方が特定可能な場合、登録いただいたメールアドレスもしくは電話番号の連絡先へ別途連絡し状況について報告いたします。
- 受託する医療情報が漏洩した場合には、その原因が明確になり、対策が万全となるまで、サービスの一部または全部の提供を停止することがあります。

2-8. 医療情報を格納する記憶媒体の管理方法

MCSにご登録いただいた情報についてはすべてAmazon.com, Incにより提供されている「Amazon Web Service」のクラウドストレージに暗号化の上格納されています。その管理・アクセスについてはエンブレースのMCSのシステム運用担当者に限定されています。

2-9. 医療情報の外部保存に係る患者等への説明方法

MCSの利用に係る患者等への説明については、第一次的には利用者において対応いただき、エンブレースにおいては必要な資料等の提供等の範囲で対応いたします。

2-10. 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況

日次の8世代バックアップに加え、特定時点でのデータベースインスタンスへの復元もできるようにしています。そのため攻撃前の状態に復元することで安全な状態への回復が可能になります。

また、バックアップデータ自体も暗号化され、なおかつイミュータブル(不変)に保管されており、ランサムウェア等による改ざんや削除を防止しています。

WAF等のセキュリティ対策を施し、モニタリングツールを使用しての異常検知(不審なアクティビティや予期せぬシステムの変更が検出された場合のアラート)も用いて防御し、なおかつ攻撃を受けても受ける前の状態に復元することを可能にしています。

2-11. 医療情報システム等の安全管理に係る評価の結果

ISMSの国際規格であるISO/IEC27001及びISO/IEC27017の認証に伴い、第三者機関による定期的な審査を受けています。直近の実施としては2024年3月にBSIジャパン株式会社によって行われ、上記認証範囲が適切である旨を確認されています。

2-12. 施設等の管理者からの問い合わせ窓口

問い合わせ窓口名称	MCSサポートデスク
問い合わせ対応メールアドレス	<ul style="list-style-type: none">● support@embrace.co.jp
問い合わせフォーム	<ul style="list-style-type: none">● https://about.medical-care.net/html/contact/
受付対応時間	<ul style="list-style-type: none">● 受付時間 月曜日～金曜日 祝祭日を除く 9時～18時

一次問い合わせとしては問い合わせフォームまでご連絡ください。

2-13. 制度上の要求事項への対応状況

医療分野の制度が求める安全管理の要求事項については 2-4. MCS の安全管理に係る基本方針記述の通り MCS のサービス提供に際して個人情報保護法及び同施行令、施行規則を遵守し、各種ガイドラインに対応しております。

(1)電子保存の要求事項

a. 真正性の確保

事項	説明
入力者及び確定者の識別・認証	<ul style="list-style-type: none"> ● MCSへの入力・記録には個別のアカウントを作成して、アカウントのIDおよびパスワードをもって認証(多要素認証を採用している場合はその認証を含む)されることが必須となっています。 ● 誰(どのアカウント)によって入力・記録された情報であるかはMCS上で識別が可能になっています。 ● MCSにおける情報の入力・閲覧についてはグループへの招待・承認機能、管理者権限機能を用いることでアクセスコントロールを任意の形で実施することができるようになっています。 ● 一度入力・記録された情報については自ら・第三者を含めて完全に消去しないしは入力・記録内容の変更を行うことができないようになっています。
記録の確定手順と、識別情報の記録	<ul style="list-style-type: none"> ● MCS上に作成された記録・情報については「どのアカウントによって」「いつ」記録されたものなのかの情報が保管されています。 ● 特にタイムラインの投稿には投稿者・作成時間の情報が第三者からもわかるように自動的に記録されます。
更新履歴の保存	<ul style="list-style-type: none"> ● MCS上のタイムラインの入力・記録については一旦入力・記録されたものについては内容の変更・更新ができないようになっており、新規投稿による追記等を行わなければならない、またその投稿については時系列の順に記録され入力・記録の順序性がわかるようになっています。 ● MCS上の患者基礎情報画面については記録内容の更新が可能となっていますが、記録の都度更新履歴が保存されるようになっています。
ネットワークを通じて医療機関等の外部に保存する場合	<ul style="list-style-type: none"> ● MCSの利用には個別のアカウントを作成して、アカウントのIDおよびパスワードをもって認証(二要素認証を採用している場合はその認証を含む)されることが必須となっています。(通信の相手先が正当であることを認識するための相互認証) ● MCSの通信についてはインターネットを介して行われますがTLS1. 2 + 「TLS暗号設定ガイドライン3.0.1版」に規定される最も安全性水準の高い「高セキュリティ型」の設定に準じて暗号化および改竄や盗聴等を防いでおります。(ネットワーク上で「改ざん」されていないことを保証すること) ● アプリ認証機能(二要素認証)を設定することで自管理端末以外からのログインを防ぐことができるようになっています。(リモートログイン機能の制限)

b. 見読性の確保

事項	説明
情報の所在管理	<ul style="list-style-type: none"> ● MCS上では患者ごとにグループを作成して情報を記録できるようになっているため、日常的にどの患者の情報がどこにあるかを管理しやすくなっています。
見読化手段の管理 見読目的に応じた応答時間	<ul style="list-style-type: none"> ● MCSはパソコン・スマートフォン・タブレット等のインターネットに接続可能な機器のウェブブラウザで利用することができます。またスマートフォン・タブレットについてはアプリ版のMCSがあり、見読目的に応じて使い分けられるようになっています。
システム障害対策としての冗長性の確保	<ul style="list-style-type: none"> ● アプリケーションおよびデータベースをいずれもクラウド構成にし、冗長化し、障害や災害に強い高い可用性を実現しています。 ● 運用については予定されたシステムメンテナンス時間を除き24時間365日をスケジュールしています。 ● 2023年の稼働率は99.9998%(利用不可時間: 月あたり約10秒)。

c. 保存性の確保

事項	説明
各種法令への準拠 (法令上作成保存が求められている書類に係る法令等)	<ul style="list-style-type: none"> ● MCSに入力・記録される情報についてはすべて診療諸記録等と同様のものと捉え、5年を超えてその記録をデータベース上に保管することとしております。
情報の滅失・破壊の防止	<ul style="list-style-type: none"> ● MCS上の記録についてはオンラインで1日1回のバックアップを実施しており、8世代分のバックアップを保存しています。
記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	<ul style="list-style-type: none"> ● MCSを構成するアプリケーションおよびデータベースについてはいずれもクラウド構成となっており特定の機器・設備に依存していないため、記録媒体や設備の劣化・不整合による情報の毀損・復元不能等が起こらないようになっています。 ● またMCSのWebアプリケーションおよびiOS/Androidアプリケーションを構成するソフトウェアやプログラミング言語についても定期的なバージョンアップを実施し、OSや言語等による陳腐化による情報の復元不能の防止をしています。
データ形式及び転送プロトコルのバージョン管理と継続性	<ul style="list-style-type: none"> ● MCS上に保管されるデータ形式および転送プロトコルについては特定の形式やプロトコルに依らず、バージョンアップや変更等によって閲覧等ができなくなるといったことはありません。

(2)法令で定められた記名・押印を電子署名で行うことについて

MCSでは現段階において電子署名を採用しておりませんが、HPKI等の電子署名された文書の交換を行っていただきます。

(3)その他取扱いに注意を要する文書等の取扱い

下記、文書・記録等についてもMCSのその他の文書・記録同様医療情報安全管理ガイドラインに従って取り扱われます。

- 施行通知には含まれていないものの、e-文書法の対象範囲で、かつ患者の個人情報が含まれている文書等（麻薬帳簿等）
- 法定保存年限を経過した文書等
- 診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像
- 診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等

(4)外部保存の要求事項

MCSに記録される情報についてはすべて診療諸記録と同等の扱いとして保管し、「「診療録等の保存を行う場所について」の一部改正について」（平成25年3月25日付け医政発0325第15号・薬食発0325第9号・保発0325第5号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下、「外部保存改正通知」。）の「第2 1 電子媒体により外部保存を行う場合」の要求事項をみたしています。

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>
--	--	--