サービス事業者による医療情報セキュリティ開示書（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版対応）

作 成 日	2023年10月31日
サービス事業者	日本医師会ORCA管理機構株式会社
サービス名称	WebQKANクラウド版
バージョン	Ver2.0.0

※本書式を作成したJAHIS/JIRAは、製品設計・設置・保守等の認証・試験・検査等は行っていません。また、特定の医療機関等における特定の目的・ニーズを満たすこと、あるいは個々の製品またはサービスの性能を保証するものではありません。この書式への記入内容は、記入した製造業者/サービス事業者が全責任を負います。

診療録及び診療諸記録を外部に保存する際の基準(8.)					
1　診療録及び診療諸記録の外部保存を受託するか？(8.3)	**該当**	非該当		備考	1
1．1　保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(8.3.C1(1)～(5))	はい	いいえ	**対象外**	備考	-
1．2　保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(8.3.C2(1)～(9))	**はい**	いいえ	対象外	備考	2
医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践(6.2)					
2　扱う情報のリストを医療機関等に提示できるか？(6.2.C1)	**はい**	いいえ	対象外	備考	3
組織的安全管理対策（体制、運用管理規程）(6.3)					
3　医療情報システムを運用する際に、医療情報システム安全管理責任者を設置しているか？(6.3.C1)	**はい**	いいえ	対象外	備考	4
4　医療情報システムを運用する際に、運用担当者を限定しているか？(6.3.C1)	**はい**	いいえ	対象外	備考	5
5　個人情報が参照可能な場所に対しては、入退管理のルールを定めているか？(6.3.C2)	**はい**	いいえ	対象外	備考	6
6　情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？(6.3.C3)	**はい**	いいえ	対象外	備考	7
7　医療機関等との契約に安全管理に関する条項を含めているか？(6.3.C4)	**はい**	いいえ	対象外	備考	8
8　個人情報を含む医療情報システムの業務をサービス事業者が外部委託する場合、その外部委託先との契約に再委託先を含めた安全管理に関する条項を含めているか？(6.3.C4)	**はい**	いいえ	対象外	備考	9
9　運用管理規程等において組織的安全管理対策に関する事項等を定めているか？(6.3.C5)	**はい**	いいえ	対象外	備考	10
物理的安全対策(6.4)					
10　個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠しているか？(6.4.C1)	**はい**	いいえ	対象外	備考	11
11　個人情報を入力・参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されているか？(6.4.C2)	**はい**	いいえ	対象外	備考	12
12　個人情報が保存されている機器が設置されている区画への入退管理を実施しているか？(6.4.C3)	**はい**	いいえ	対象外	備考	13
12．1　入退出の事実を記録しているか？(6.4.C3)	**はい**	いいえ	対象外	備考	14
12．2　入退者の記録を定期的にチェックし、妥当性を確認しているか？(6.4.C3)	**はい**	いいえ	対象外	備考	15
13　個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置しているか？(6.4.C4)	**はい**	いいえ	対象外	備考	16
14　個人情報が入力・参照できる端末に覗き見防止の機能があるか？(6.4.C5)	**はい**	いいえ	対象外	備考	17
15　サービス事業者の管理端末に覗き見防止対策が取られているか？(6.4.C5)	**はい**	いいえ	対象外	備考	17
技術的安全対策(6.5)					
16　権限を持たない者による不正入力を防止する対策が行われているか？(6.5.C1、6.5.C4)	**はい**	いいえ	対象外	備考	18
17　アクセス管理の機能があるか？(6.5.C1)	**はい**	いいえ	対象外	備考	
17．1　利用者の認証方式は？(6.5.C1)(6.5.C13)					
・記憶（ID・パスワード等）	**はい**	いいえ	対象外	備考	19
・生体認証（指紋等）	はい	**いいえ**	対象外	備考	-
・物理媒体（ICカード等）	**はい**	いいえ	対象外	備考	20
・上記のうちの2要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	**はい**	いいえ	対象外	備考	21
・その他（具体的な方法を備考に記入してください）	**はい**	いいえ	対象外	備考	22
17．1．1　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C14 (1)～(5))	**はい**	いいえ	対象外	備考	-
17．1．1．1　他の手段と併用した際のパスワードの運用方法を運用管理規程に定めているか？(6.5.C14(1))	**はい**	いいえ	対象外	備考	23
17．1．1．2　本人確認の実施の際、本人確認方法を台帳に記載しているか？(6.5.C14(2))	はい	**いいえ**	対象外	備考	-
17．1．1．3　パスワードの有効期限が管理できるか？(6.5.C14(4))	**はい**	いいえ	対象外	備考	24
17．1．1．4　文字列制限をチェックすることができるか？(6.5.C14(4))	**はい**	いいえ	対象外	備考	25

１７．１．１．５　類推しやすいパスワードをチェックすることができるか？(6.5.C14(5))	はい	**いいえ**	対象外	備考	-
１７．１．１．６　パスワード変更の際に類似性のチェックをすることができるか？(6.5.C14(5))	**はい**	いいえ	対象外	備考	26
１７．１．１．７　IDとパスワードの組み合わせが本人しか知りえないよう保たれているか？(6.5C2)	**はい**	いいえ	対象外	備考	27
１７．１．２　運用管理規程にセキュリティ・デバイスの代替手段が規定されているか？(6.5C3)	はい	**いいえ**	対象外	備考	28
１７．２　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	**はい**	いいえ	対象外	備考	29
１７．３　アクセス記録（アクセスログ）機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	30
１７．３．１　アクセスログを利用者が確認する機能があるか？(6.5.C7)	はい	**いいえ**	対象外	備考	31
１７．３．２　アクセスログへのアクセス制限ができるか？(6.5.C8)	**はい**	いいえ	対象外	備考	32
１７．３．３　アクセスログへのアクセス制限機能がない場合、不当な削除/改ざん/追加等を防止する運用的対策を講じているか？(6.5.C8)	はい	いいえ	**対象外**	備考	-
１７．４　アクセス記録（アクセスログ）機能が無い場合、利用者が監査できる形でサービス事業者が業務日誌等に操作の記録を行っているか？(6.5.C7)	はい	いいえ	**対象外**	備考	-
１８　時刻情報の正確性を担保する仕組みがあるか？(6.5.C9)	**はい**	いいえ	対象外	備考	33
１９　不正なソフトウェアが混入していないか確認しているか？(6.5.C10、6.5.C11)	**はい**	いいえ	対象外	備考	34
２０　システムにメールの送受信機能がある場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(6.5.C12)	はい	いいえ	**対象外**	備考	35
２１　システムでファイル交換機能を使用する場合、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理等が行われているか？(6.5.C12)	はい	いいえ	**対象外**	備考	36
２２　無線LANを利用する場合のセキュリティ対策機能はあるか？(6.5.C15)	**はい**	いいえ	対象外	備考	37
２３　IoT機器を使用する場合、IoT機器により患者情報を取り扱うことに関する運用管理規程を定めた上で、医療機関等に開示できるか？(6.5.C16(1))	はい	いいえ	**対象外**	備考	38
２３．１　ウェアラブル端末や在宅設置のIoT機器を利用する場合、患者のリスク等に関する説明資料を提供できるか？（6.5.C16(2))	はい	いいえ	対象外	備考	-
２３．２　IoT機器のセキュリティアップデートを必要なタイミングで適切に実施できるか？(6.5.C16(3))	はい	いいえ	対象外	備考	-
２３．３　使用が終了または停止したIoT機器の接続を遮断できるか？（6.5.C16(4))	はい	いいえ	対象外	備考	-
人的安全対策(6.6)					
２４　従業者との間で、雇用時または契約時に守秘義務契約を結んでいるか？（6.6C1(1))	**はい**	いいえ	対象外	備考	39
２５　従業者に対し、定期的に個人情報管理に関する教育訓練を行っているか？（6.6C1(2))	**はい**	いいえ	対象外	備考	40
２６　従業者の退職後または契約終了後における個人情報保護に関する規程が従業者との契約に含まれているか？（6.6C1(3))	**はい**	いいえ	対象外	備考	41
２７　就業規則等には守秘義務違反に対する包括的な罰則規定が含まれているか？（6.6C2(1)a)	**はい**	いいえ	対象外	備考	42
２８　保守作業等で医療情報システムに直接アクセスする作業を行う際には、作業者・作業内容・作業結果を医療機関等に報告できるようになっているか？（6.6C2(1)b)	**はい**	いいえ	対象外	備考	43
２９　清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行っているか？(6.6C2(1)c)	はい	**いいえ**	対象外	備考	44
３０　業務の一部を外部委託する場合に、外部委託先に対し、自らに課しているのと同等の個人情報保護に関する対策を施す義務を、契約によって担保しているか？（6.6C2(1)d)	**はい**	いいえ	対象外	備考	45
３１　やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行っているか？(6.6C2(2))	**はい**	いいえ	対象外	備考	46
情報の破棄(6.7)					
３２　ユーザに提示できる情報種別ごとの破棄の手順があるか？(6.7.C1)	**はい**	いいえ	対象外	備考	47
３２．１　手順には破棄を行う条件を含めているか？(6.7.C1)	**はい**	いいえ	対象外	備考	47
３２．２　手順には破棄を行うことができる従業者の特定を含めているか？(6.7.C1)	**はい**	いいえ	対象外	備考	47
３２．３　手順には破棄の具体的な方法を含めているか？(6.7.C1)	**はい**	いいえ	対象外	備考	47
３３　情報処理機器自体を破棄する場合、必ず専門的な知識を有する者が行うこととし、残存し、読み出し可能な情報がないことを報告できるか？(6.7.C2)	**はい**	いいえ	対象外	備考	48
３４　破棄を外部委託した場合、外部委託業者の監督及び守秘義務契約に準じた監督責任の下、情報の破棄を確認しているか？(6.7.C3)	**はい**	いいえ	対象外	備考	49
３５　不要になった個人情報を含む媒体の破棄を、運用管理規程に定めているか？(6.7.C4)	**はい**	いいえ	対象外	備考	48
医療情報システムの改造と保守(6.8)					
３６　改造や保守に関する動作確認で個人情報を含むデータを使用する場合、作業員と守秘義務契約を交わしているか？(6.8.C1)	はい	いいえ	**対象外**	備考	50
３７　作業員はサービス事業者自身が定めた運用管理規程に従い、改造や保守に関する業務を行っているか？(6.8.C1)	**はい**	いいえ	対象外	備考	51
３８　運用管理規程には作業終了後に動作確認で使用した個人情報を含むデータを消去する規定が含まれているか？(6.8.C1)	はい	いいえ	**対象外**	備考	52

３９　改造や保守に用いるアカウントは、作業員個人の専用アカウントを使用しているか？(6.8.C2)	**はい**	いいえ	対象外	備考	53
４０　改造や保守に関する作業の記録として、個人情報へのアクセス有無、及びアクセスした対象を特定できる情報を医療機関等に提供できるか？(6.8.C2)	はい	いいえ	**対象外**	備考	52
４１　アカウント情報の外部流出等による不正使用の防止に努めているか？(6.8.C3)	**はい**	いいえ	対象外	備考	54
４２　作業員の離職や担当替え等に対して速やかに保守用アカウントを削除しているか？(6.8.C4)	**はい**	いいえ	対象外	備考	55
４３　改造や保守を外部委託している場合、保守要員の離職や担当替え等の際に報告を義務付けているか？(6.8.C4)	**はい**	いいえ	対象外	備考	56
４３．１　報告に応じてアカウントを削除する管理体制ができているか？(6.8.C4)	**はい**	いいえ	対象外	備考	57
４４　メンテナンスを実施する場合は、事前に医療機関等に作業申請を提出できるか？(6.8.C5)	**はい**	いいえ	対象外	備考	58
４５　メンテナンス終了時に、速やかに医療機関等に作業報告書を提出できるか？(6.8.C5)	**はい**	いいえ	対象外	備考	59
４６　保守を外部委託する場合、保守事業者 と守秘義務契約を締結しているか？(6.8.C6)	**はい**	いいえ	対象外	備考	60
４７　個人情報を含むデータを組織外に持ち出す際に、医療機関等の責任者の承認を得ることが運用管理規程に定められているか？(6.8.C7)	はい	いいえ	**対象外**	備考	61
４８　リモートメンテナンスによる改造・保守を行う場合は、アクセスログを収集するか？(6.8.C8)	**はい**	いいえ	対象外	備考	62
４９　リモートメンテナンスにおいて、医療機関等へ送付等を行うファイルは、送信側で無害化処理が行われているか？(6.8.C9)	はい	いいえ	**対象外**	備考	
５０　保守業務を外部委託している場合、外部委託事業者にも自らと同等な義務を求め、契約しているか？(6.8.C10)	**はい**	いいえ	対象外	備考	64
情報 及び 情報機器の持ち出し 並びに 外部利用 について(6.9)					
５１　持出機器を提供しているか？(6.9)	該当	**非該当**		備考	65
５１．１　持出機器においてソフトウェアのインストールを制限する機能があるか？(6.9)	はい	いいえ	対象外	備考	-
５１．２　持出機器において外部入出力装置の機能を無効にすることができるか？(6.9)	はい	いいえ	対象外	備考	-
５１．３　外へ持ち出す際、情報に対して暗号化等の対策を行うことができるか？(6.9.C7)	はい	いいえ	対象外	備考	-
５１．４　持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)	はい	いいえ	対象外	備考	-
５２　提供するサービスに係わる情報及び情報機器の持ち出しについて、リスク分析を実施しているか？(6.9.C1)	**はい**	いいえ	対象外	備考	66
５３　サービス事業者が情報及び情報機器を持出する場合があるか？(6.9.C1)	**該当**	非該当		備考	
５３．１　リスク分析の結果を受けて、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に定めているか？(6.9.C1)	**はい**	いいえ	対象外	備考	67
５３．２　持ち出した情報及び情報機器の管理方法を定めているか？(6.9.C2)	**はい**	いいえ	対象外	備考	68
５３．３　情報を格納した媒体及び情報機器の盗難、紛失時の適切な対応を自社方針・規則等に定めているか？(6.9.C3)	**はい**	いいえ	対象外	備考	69
５３．４　自社方針・規則等で定めた盗難、紛失時の対応を従業員等に対して周知徹底し、教育を行っているか？(6.9.C4)	**はい**	いいえ	対象外	備考	70
５３．５　情報機器について、起動パスワード等を設定しているか？(6.9.C6)	**はい**	いいえ	対象外	備考	71
５３．６　パスワード設定においては、適切なパスワード管理措置を行っているか？(6.9.C6)	**はい**	いいえ	対象外	備考	72
５３．７　サービス事業者が外へ持ち出す際、情報に対して暗号化等の対策を行っているか？(6.9.C7)	**はい**	いいえ	対象外	備考	73
５３．８　医療機関等または医療機関等に委託されたサービス事業者が、持ち出した情報機器を外部のネットワークや他の外部媒体に接続する場合、情報漏えいや改ざんの対策を実施しているか？(6.9.C8)	**はい**	いいえ	対象外	備考	74
５４　情報の管理者は情報機器・媒体の所在について台帳を用いる等して管理しているか？(6.9.C5)	**はい**	いいえ	対象外	備考	75
５５　個人保有の情報機器の利用を禁止しているか？(6.9.C10)	**はい**	いいえ	対象外	備考	76
災害、サイバー攻撃等の非常時の対応(6.10)					
５６　医療機関等に提供可能なサービス事業者のBCP手順書が用意されているか？(6.10.C1、6.10.C2)	**はい**	いいえ	対象外	備考	77
５７　非常時アカウント又は、非常時にも医療サービスを継続して提供できる機能を持っているか？　(6.10.C4)	はい	**いいえ**	対象外	備考	78
５７．１　「非常時のユーザアカウントや非常時用機能」の管理手順を提供できるか？ (6.10.C4(1))	はい	いいえ	対象外	備考	-
５７．２　非常時機能を有している場合、非常時機能が定常時に不適切に利用されることがないよう適切に管理及び監査できる情報を提供できるか？(6.10.C4(2))	はい	いいえ	対象外	備考	-
５７．３　非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更できるか？(6.10.C4(3))	はい	いいえ	対象外	備考	-
５７．４　標的型メール攻撃等により医療情報システムに不正ソフトウェアが混入した場合、関係先への連絡手段を準備しているか？(6.10.C4(4))	はい	いいえ	対象外	備考	-
５８　重要なファイルをバックアップしているか？(6.10.C4(5))	**はい**	いいえ	対象外	備考	79
５８．１　バックアップは数世代、複数の方式で実施しているか？(6.10.C4(5))	**はい**	いいえ	対象外	備考	80
５８．２　数世代、複数方式のバックアップの一部は不正ソフトウェアの混入による影響が波及しないように管理されているか？(6.10.C4(5))	**はい**	いいえ	対象外	備考	81
５８．３　バックアップからの復元手段が整備されているか？(6.10.C4(5))	**はい**	いいえ	対象外	備考	82

外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理(6.11)

５９～６３の質問は、提供するサービスで利用している通信方式について確認するものです。通信方式によって対策すべき項目が異なりますので、対応している通信方式それぞれに対して確認が必要です。対応する通信方式に「該当」とし、対応していない通信方式を「非該当」としてください。

５９ 通信方式として専用線に対応しているか？(6.11)	該当	**非該当**		備考	-		
５９．１ 提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考	-		
５９．２ 採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-		
６０ 通信方式として公衆網に対応しているか？(6.11)	該当	**非該当**		備考	-		
６０．１ 提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考	-		
６０．２ 採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-		
６１ 通信方式としてIP-VPNに対応しているか？(6.11)	該当	**非該当**		備考	-		
６１．１ 提供事業者に閉域性の範囲を確認しているか？(6.11.C1)	はい	いいえ	対象外	備考	-		
６１．２ 採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-		
６２ 通信方式としてIPsec-VPN ＋IKEに対応しているか？(6.11)	該当	**非該当**		備考	-		
６２．１ セッション間の回り込み等の攻撃への適切な対策をしているか？(6.11.C11)	はい	いいえ	対象外	備考	-		
６２．２ 採用する認証手段が定められているか？(6.11.C2)	はい	いいえ	対象外	備考	-		
６３ チャネル・セキュリティとしてTLS1.2以上のクライアント認証に対応しているか？(6.11)	**該当**	非該当		備考	-		
６３．１ サーバ/クライアントともに「TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行っているか？(6.11.C11)	**はい**	いいえ	対象外	備考	83		
６３．２ セッション間の回り込み等による攻撃への適切な対策を実施しているか？(6.11.C11)	はい	いいえ	**対象外**	備考	84		
６４ ネットワーク上において、改ざんを防止する対策を行っているか？(6.11.C1)	**はい**	いいえ	対象外	備考	85		
６５ ネットワーク上において、盗聴を防止する対策を行っているか？(6.11.C1)	**はい**	いいえ	対象外	備考	85		
６６ ネットワーク上において、なりすましへの対策を行っているか？(6.11.C1)	**はい**	いいえ	対象外	備考	85		
６７ データ送信元と送信先において、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行っているか？(6.11.C2)	**はい**	いいえ	対象外	備考	86		
６８ ネットワークの経路制御・プロトコル制御を行える機器または機能を有するか？(6.11.C4)	**はい**	いいえ	対象外	備考	87		
６９ ネットワークの経路制御・プロトコル制御に関わる機器または機能は、安全性を確認できるようなセキュリティ対策が規定された文書を示すことができるか？(6.11.C4)	**はい**	いいえ	対象外	備考	88		
７０ 医療機関等との通信経路について回り込みが行われないように経路設定を行っているか？(6.11.C4)	**はい**	いいえ	対象外	備考	89		
７１ 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しているか？(6.11.C5)	**はい**	いいえ	対象外	備考	90		
７２ 暗号化を利用する場合、暗号化の鍵について電子政府推奨暗号のものを使用しているか？(6.11.C5)	**はい**	いいえ	対象外	備考	91		
７３ 脅威に対する管理責任の範囲について、医療機関等に明確に示し、その事項を示す文書等が提示できるか？(6.11.C6、6.11.C9)	**はい**	いいえ	対象外	備考	92		
７４ 医療機関等から委託をされた範囲において、脅威に対する管理責任の範囲を医療機関等に明確に示し、その事項を示す文書等を提示できるか？(6.11.C6)	**はい**	いいえ	対象外	備考	93		
７５ リモートメンテナンスサービスを有しているか？(6.11.C8)	**該当**	非該当		備考	-		
７５．１ リモートメンテナンスサービスに関し、不必要なリモートログインを制限する仕組みを有しているか？(6.11.C8)	**はい**	いいえ	対象外	備考	94		
７６ 回線の可用性等の品質に関して問題がないことを確認し、明確に文書等の証跡を残し、医療機関等に提示できるか？(6.11.C9)	はい	いいえ	**対象外**	備考	95		
７７ 患者に情報を閲覧させる機能があるか？(6.11.C10)	該当	**非該当**		備考	96		
７７．１ 情報の閲覧のために公開しているサービスにおいて、医療機関等の内部システムに不正な侵入等が起こらないように対策を実施しているか？(6.11.C10)	はい	いいえ	対象外	備考	-		
７７．２ 医療機関等が患者等へ危険性や情報提供の目的について説明を行うために必要となる情報を資料として提示できるか？(6.11.C10)	はい	いいえ	対象外	備考	-		
７７．３ 説明資料では、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にしているか？(6.11.C10)	はい	いいえ	対象外	備考	-		

保存が義務付けられている文書を扱っている場合のみ下記対象

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(6.12)

７８ 記名・押印が義務付けられた文書を扱っているか？(6.12.C1)	該当	**非該当**		備考	97		
７８．１ HPKI対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の署名機能があるか？(6.12.C1)	はい	いいえ	対象外	備考	-		
７８．２ HPKI対応、又は認定認証局もしくは公的個人認証サービスが発行する証明書対応の検証機能があるか？(6.12.C1)	はい	いいえ	対象外	備考	-		
７８．２．１ 特定の国家資格の確認を行う必要がある場合に、電子的に検証できる機能があるか？(6.12.C1)	はい	いいえ	対象外	備考	-		

７８．３　総務省の「時刻認証業務の認定に関する規程」に基づき認定された事業者が提供する認定のタイムスタンプが付与可能か？(6.12.C2)	はい	いいえ	対象外	備考	-
７８．４　総務省の「時刻認証業務の認定に関する規程」に基づき認定された事業者が提供するタイムスタンプが検証可能か？(6.12.C2)	はい	いいえ	対象外	備考	-
７８．５　保存期間中の文書の真正性を担保する仕組みがあるか？(6.12.C2)	はい	いいえ	対象外	備考	-
７９　上記タイムスタンプを付与する時点で有効な電子証明書を用いているか？(6.12.C2(4))	はい	いいえ	**対象外**	備考	-
真正性の確保について(7.1)					
８０　入力者及び確定者を正しく識別し、認証を行う機能があるか？(7.1.C1(1)a)	はい	いいえ	**対象外**	備考	-
８０．１　区分管理を行っている対象情報ごとに、権限管理（アクセスコントロール）の機能があるか？(7.1.C1(1)b)	はい	いいえ	対象外	備考	-
８０．２　権限のある利用者以外による作成、追記、変更を防止する機能があるか？(7.1.C1(1)b)	はい	いいえ	対象外	備考	-
８０．３　サービス事業者内の利用者の権限管理の機能があるか？(7.1.C1(1)b)	はい	いいえ	対象外	備考	-
８０．４　サービス事業者内の利用者が作成、追記、変更を防止する機能があるか？(7.1.C1(1)b)	はい	いいえ	対象外	備考	-
８０．５　システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(7.1.C1(1)c)	はい	いいえ	対象外	備考	-
８０．６　システムがサービス事業者の保守等端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(7.1.C1(1)c)	はい	いいえ	対象外	備考	-
８１　システムは記録を確定する機能があるか？(7.1.C2(1)a)	はい	いいえ	**対象外**	備考	-
８１．１　確定情報には、入力者及び確定者の識別情報、信頼できる時刻源を用いた作成日時が含まれているか？(7.1.C2(1)a)	はい	いいえ	対象外	備考	-
８１．２　「記録の確定」を行うにあたり、内容の確認をする機能があるか？(7.1.C2(1)b)	はい	いいえ	対象外	備考	-
８１．３　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止する機能があるか？(7.1.C2(1)d)	はい	いいえ	対象外	備考	-
８２　装置が確定機能を持っていない場合、記録が作成される際に、当該装置の管理責任者や操作者の識別情報、作成日時を含めて記録する機能があるか？ (7.1.C2(2)a)	はい	いいえ	**対象外**	備考	-
８３　確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能があるか？(7.1.C3(1))	はい	いいえ	**対象外**	備考	-
８３．１　同じ診療録等に対して複数回更新が行われた場合、更新の順序性を識別できる機能があるか？(7.1.C3(2))	はい	いいえ	対象外	備考	-
８４　代行入力の承認機能があるか？(7.1.C4)	はい	いいえ	**対象外**	備考	-
８４．１　代行入力が行われた場合、誰の代行がいつ誰によって行われたかの管理情報を、その代行入力の都度、記録する機能があるか？(7.1.C4(2))	はい	いいえ	対象外	備考	-
８４．２　代行入力により記録された診療録等に対し、確定者による「確定操作（承認）」を行う機能があるか？(7.1.C4(3))	はい	いいえ	対象外	備考	-
８５　システムがどのような機器・ソフトウェアで構成され、どのような場面、用途で利用されるのか明確にしているか？(7.1.C5(1))	はい	いいえ	**対象外**	備考	-
８６　機器・ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されているか？(7.1.C5(2))	はい	いいえ	**対象外**	備考	-
８７　機器・ソフトウェアの品質管理に関する作業内容をルールに定めて、策定したルールに基づいて従業者等への教育を実施しているか？(7.1.C5(3))	はい	いいえ	**対象外**	備考	-
８８　システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施しているか？(7.1.C5(4))	はい	いいえ	**対象外**	備考	-
８９　通信の相手先が正当であることを確認するための相互認証を実施しているか？ (7.1.C6)	はい	いいえ	**対象外**	備考	-
９０　ネットワークの転送中に改ざんされていないことを保証する機能を有しているか？(7.1.C7)	はい	いいえ	**対象外**	備考	-
９１　サービス事業者の機器・システムはリモートログインの機能を制限しているか？ (7.1.C8)	はい	いいえ	**対象外**	備考	-
見読性の確保について(7.2)					
９２　患者ごとの全ての情報の所在が日常的に管理されているか？(7.2.C1)	はい	いいえ	**対象外**	備考	-
９３　電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理し、また、見読化手段である機器・ソフトウェア・関連情報等は常に整備されているか？(7.2.C2)	はい	いいえ	**対象外**	備考	-
９４　目的に応じて速やかに検索結果を出力する機能又はサービスがあるか？(7.2.C3)	はい	いいえ	**対象外**	備考	-
９５　システム障害に備えた冗長化手段や代替的な見読化手段はあるか？(7.2.C4)	はい	いいえ	**対象外**	備考	-
９５．１　冗長化手段があるか？(7.2.C4)	はい	いいえ	対象外	備考	-
９５．２　システム障害に備えた代替的な見読化手段があるか？(7.2.C4)	はい	いいえ	対象外	備考	-
保存性の確保について(7.3)					
９６　不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行っているか？(7.3.C1(1))	はい	いいえ	**対象外**	備考	-
９７　記録媒体及び記録機器の院内での保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？また、クラウドサービスを提供する場合において、サービス事業者による記録媒体及び記録機器の保管及び取扱いについてSLA等の文書に含めて医療機関等に提供されているか？(7.3.C2(1))	はい	いいえ	**対象外**	備考	-
９８　情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？ (7.3.C2(2))	はい	いいえ	**対象外**	備考	-

９９　システムが保存する情報へのアクセスについて、履歴を残しているか？ (7.3.C2(4))	はい	いいえ	**対象外**	備考	-
９９．１　システムが保存する情報へのアクセスについてその履歴を管理しているか？(7.3.C2(4))	はい	いいえ	対象外	備考	-
１００　システムが保存する情報がき損した時に、バックアップされたデータ等を用いて、き損前の状態に戻せるか、又はもし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしているか？(7.3.C2(5))	はい	いいえ	**対象外**	備考	-
１０１　システムの移行の際に診療録等のデータを、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式にて出力及び入力できる機能があるか？(7.3.C4(1))	はい	いいえ	**対象外**	備考	-
１０２　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能またはサービスを備えているか？(7.3.C4(2))	はい	いいえ	**対象外**	備考	-
１０３　外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持できるか？(7.3.C5)	はい	いいえ	**対象外**	備考	-
１０４　SLA等に医療機関等に対して設備の条件を提示して、回線や設備が劣化した場合はSLA等の要件を満たすように更新できるか？(7.3.C6)	はい	いいえ	**対象外**	備考	-
診療録等をスキャナ等により電子化して保存する場合について(9.)					
１０５　診療録などをスキャナなどにより電子化して原本として保存する機能があるか？(9.1.C1、9.4)	該当	**非該当**		備考	-
１０５．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(9.1.C1)	はい	いいえ	対象外	備考	-
１０５．２　電子署名等を付与する機能があるか？(9.1.C2、9.4.C2)	はい	いいえ	対象外	備考	-
１０６　診療録などをスキャナなどにより電子化して参照情報として保存する機能があるか？(9.5)	該当	**非該当**		備考	-
１０６．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？(9.5.C1)	はい	いいえ	対象外	備考	-

備考記載欄	
1	レセプト請求に必要な個人情報を保存している
2	AWSを利用しておりリファレンスが開示されている
3	扱う情報はデータベース構造ととも掲載している
4	ISMS（ISO27001）にて安全管理責任者を任命している
5	医療情報システムの運用者を証明書で制限をしている
6	ISMS（ISO27001）セキュリティエリアを定め、外部の入退室を制限している
7	ISMS（ISO27001）で定めている
8	ORCAMOクラウド セキュリティ利用規約に記載している
9	契約書では機密情報の保持、管理体制、目的外使用の禁止等を定めている
10	ISMS（ISO27001）で定めている
11	個人情報はAWSに保存されており、リファレンスのとおり入退室の管理がされている
12	個人情報はAWS内では閲覧はできない
13	個人情報が記録されているAWS上のクラウドサーバは持ち出しが禁止されている
14	個人情報はAWSに保存されており、リファレンスのとおり入退室の管理がされている
15	個人情報はAWSに保存されており、リファレンスのとおり入退室の管理がされている
16	個人情報が記録されているAWS上のクラウドサーバは持ち出しが禁止されている
17	AWS内では個人情報は閲覧できない。AWSサーバの保守用PCは社内ではセキュリティエリアのみでの利用となっている。移動可能なノートPCにはのぞき見防止フィルターを付けている。
18	社内のPCにはISMS（ISO27001）でクリアスクリーン等の実施を定めている
19	社内のPCにはIDとパスワードが設定できる
20	サーバにログインする際にはワンタイムパスワードが必要になっている。
21	サーバにはワンタイムパスワードとIDとパスワードが必要になっている。
22	サーバにログインするには入退室による作業員の制限とワンタイムパスワード、ID、パスワードの組み合わせが必要になっている
23	ISMS（ISO27001）でパスワードの運用方法が定められている
24	ワンタイムパスワードとの併用でありパスワードに期限は定めていないが設定すれば利用できる
25	サーバのアカウントパスワードは8文字以上、3種類の文字を組み合わせることになっている
26	サーバのアカウントは同じパスワードは設定できない
27	サーバのパスワードは暗号化されて保存されている
28	サーバへのアクセスはシステム管理者にて新たなアカウント発行などの権限はあるが代替手段として運用管理規程には定めていない
29	サーバへのアクセスはアカウント毎にアクセス管理が設定できる
30	サーバへのアクセス記録は保存されている

31	サーバへのアクセスログは管理者のみが閲覧可能となっている
32	サーバへのアクセスログは管理者のみが閲覧可能となっている
33	AWSのリファレンスで時刻同期が定められている
34	サーバにプログラムやデータをアップロードするPCは不正なソフトウェアが混入しないようにウィルス対策ソフトを組み込んでいる
35	サーバではメールは利用できない
36	サーバではファイル交換サービスは利用できない
37	AWSでは無線LANは利用されていない。社内での無線LANはIDとパスワードを秘匿化しているので検出されない設定となっている
38	業務でのIOTの利用はISMS（ISO27001）で禁止しており、利用する場合は許可制となっている
39	就業規則に記されている
40	ISMS（ISO27001）において定期的な訓練を行っている
41	就業規則に記されている
42	就業規則に記されている
43	作業前にメンテナンスのお知らせに掲載するほか、メーリングリストで案内、報告をしている
44	AWS内の清掃などの簡易な作業については報告をしてはいない
45	委託契約書に記載している
46	委託契約書に記載している
47	社内はISMS（ISO27001）において情報資産の台帳管理と破棄の方法、破棄の責任者を定めている。データセンター内はリファレンスに運用が記されている。
48	社内はISMS（ISO27001）において破棄手順が定められている。データセンター内はリファレンスに運用が記されている。
49	委託先のデータセンターではリファレンスに運用が記されている
50	動作確認にはテストデータを利用しており個人情報は利用していない
51	ISMS（ISO27001）で実データの利用は禁止している
52	動作確認にはテストデータを利用しており個人情報は利用していない
53	作業者毎に異なるアカウントを設けている
54	ISMS（ISO27001）でアカウントの管理を定めている
55	ISMS（ISO27001）の入社退職時チェックリストに基づきアカウントの削除等を行っている
56	体制表の提出をさせている
57	体制表に応じてアカウントを管理している
58	サーバのメンテナンス時はお知らせやメーリングリストで報告をしている
59	サーバのメンテナンス時はお知らせやメーリングリストで報告をしている
60	委託契約書に記載している
61	個人情報を含む実データは取り扱っていない
62	サーバのリモートメンテナンスではログを記録している
63	リモートメンテナンスで医療機関に情報を送受信することはない
64	委託契約書に記載している
65	利用者に機器は提供していない
66	ISMS（ISO27001）でリスク分析を行っている
67	ISMS（ISO27001）で規定している
68	社内業務で利用する持出機器はISMS（ISO27001）で申請による許可制としている
69	ISMS（ISO27001）にて規定されている
70	ISMS（ISO27001）にて定期的に教育をしている
71	起動時のパスワードは設定している
72	パスワードの文字数制限等を行い、パスワードの運用管理についてはISMS（ISO27001）にて規定している
73	持出の情報機器はディスクの暗号化を実施している
74	防止策としてウィルス対策ソフトを導入している
75	持出の情報機器は台帳管理している
76	ISMS（ISO27001）にて禁止し、必要な場合は許可制としている
77	ISMS（ISO27001）でBCP対策が規定されている
78	非常時アカウントは存在せず、アカウントの再発行となる
79	サーバは冗長化してあり、それとは別に複数世代のバックアップを保存している
80	複数世代のデータをバックアップしている

81	バックアップデータは隔離しているのでウィルスの影響は受けない
82	バックアップデータからの復元手順は整備してある
83	TLS1.2の高セキュリティ設定かTLS1.3の利用に限定している
84	サーバ側ではクローズドネットワークへの接続は無い
85	WAFで防御している
86	利用者固有の管理番号で医療機関を、クライアント証明書で端末機器を、ID、パスワードで利用者を識別できる
87	WAFを導入している
88	ホームページ（https://www.barracuda.com/company/legal/security-compliance#paranav-navbar）にて掲載している
89	WAFで防御している
90	ネットワーク通信ではTLS1.2またはTLS1.3を採用している
91	AES256－GCM他を採用している
92	責任分界点を提示している
93	責任分界点を提示している
94	リモートメンテナンスができる場所、人員、アクセス範囲を制限している
95	通信回線は通信事業者によるものと考えており当社から品質を保証するものではない
96	患者閲覧させる機能は無い
97	医療訪問看護計画書、医療訪問看護報告書は電子的に保存ではなく、印刷して保存することとしているため3原則の対象外としている
98	
99	
100	
101	
102	
103	
104	
105	
106	
107	
108	
109	
110	
111	
112	
113	
114	
115	
116	
117	
118	
119	
120	
121	
122	
123	
124	
125	
126	
127	
128	
129	
130	

131	
132	
133	
134	
135	
136	
137	
138	
139	
140	
141	
142	
143	
144	
145	
146	
147	
148	
149	
150	
151	
152	
153	
154	
155	
156	
157	
158	
159	
160	
161	
162	
163	
164	
165	
166	
167	
168	
169	
170	
171	
172	
173	
174	
175	
176	
177	
178	
179	
180	
181	
182	
183	
184	
185	

186	
187	
188	
189	
190	
191	
192	
193	
194	
195	
196	
197	
198	
199	
200	