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	2024年9月1日 日曜日
サービス事業者	メドピア株式会社
サービス名称	やくばと医療機関システム
バージョン	2024/9/1 時点

※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	-
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	-
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	2
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 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	3
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	4
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	5
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	6
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	-
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	7
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	8
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	7
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	7
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	7
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	9
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	10
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	11
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	12
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	13
・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	13
・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	13
・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	-
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	14
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	15
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	16
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	17
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	18
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？	はい	**いいえ**	対象外	備考	18
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？	**はい**	いいえ	対象外	備考	19
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？(6.5.C3)	はい	いいえ	**対象外**	備考	20
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	21

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	22
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	22
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	23
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	23
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	24
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	-
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	-
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	25
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	26
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	27
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	28
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？（6.6.C1(1))	**はい**	いいえ	対象外	備考	29
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？（6.6.C1(2))	**はい**	いいえ	対象外	備考	30
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？(6.6.C1(3))	**はい**	いいえ	対象外	備考	31
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？（6.6.C2(1)a)	**はい**	いいえ	対象外	備考	32
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？（6.6.C2(1)b)	はい	いいえ	**対象外**	備考	33
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？(6.6.C2(1)c)	はい	いいえ	**対象外**	備考	34
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？（6.6.C2(1)d)	**はい**	いいえ	対象外	備考	35
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？(6.6.C2(2))	**はい**	いいえ	対象外	備考	36
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	37
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	37
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	37
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	37
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	38
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	38
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	39
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	40
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.C	**はい**	いいえ	対象外	備考	-
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？	はい	いいえ	**対象外**	備考	41
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	-
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	42
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	43
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	43
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	44
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	44
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	45
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	45
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	46

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	47
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	48
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	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.C1(	はい いいえ	**対象外**	備考	46
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	-
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	-
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	49
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	49
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	49
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	49
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	50
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	50
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	51
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	51
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	-
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	-
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	52
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	53
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	53
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	53
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	53
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	-
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	54
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	54
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	54
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	55
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	56
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	-
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	-
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	57
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	57
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	57
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	58
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	59
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	59
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	59
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？	**はい**	いいえ	対象外	備考	60
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	60
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	61
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	61
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	はい	いいえ	対象外	備考	-
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	-
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	62
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	63
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	63
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	63
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？	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	63
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？	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	63

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？	はいいいえ	**対象外**	備考	63
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？	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	63
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	はいいいえ	**対象外**	備考	63
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	63
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	63
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	63
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	63
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	63
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	63
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	63
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	63
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	63
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	63
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	63
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	はいいいえ	**対象外**	備考	63
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	63
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	63
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？	はいいいえ	**対象外**	備考	63
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	63
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	63
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	63
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	63
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	やくばと医療機関システムでは診療録および診療諸記録に該当する情報は取扱いません。
2	全社的な情報セキュリティ対策の責任者として、当社の技術責任者が担当しております。
3	個人情報を取り扱う業務の実施は、オフィスなど、来訪者の識別や入退室の制限が可能な場所でのみ実施することとしております。

4	やくばと医療機関システムの管理用システムを利用する際には、権限を持つ従業員個人に発行されたアカウントでのログインが必要です。また特に患者の個人情報は正社員の一部エンジニアが直接データベースを確認することでのみ参照可能となっております。これらの操作には記憶方式（IDとパスワード）と物理媒体方式（当社貸与の業務用情報処理端末からのVPN接続）による2要素認証が求められるものとして、厳格なアクセス制限を設けております。 また管理用システムやデータベースのへのアクセス、ならびに行った操作等はログとして記録に残しております。 これらの運用・管理の状況については、自部門での点検と、その結果を踏まえた内部監査を年1回の頻度で実施している他、ISMSの要求事項に沿った情報資産の棚卸しも実施しております。
5	やくばと医療機関システムの登録医療機関すべてに「やくばと医療機関システム利用規約」に同意いただいています。当該規約は、システム利用に必要な認証キーの取り扱い、利用環境のセキュリティ確保、患者情報の取り扱い、などの安全管理に関する規定を含んでいます。 https://yakubato.jp/terms/medical_institutions.html
6	外部委託を行っていないため対象外です。なお今後、再委託を行う場合には安全管理に関する条項を委託先との契約内に盛り込む必要性は認識しており、契約書の雛形に当該内容を含めております。
7	個人情報が保存されるサーバーはAWSを利用しています。AWSが当該条件をクリアしていることを確認済みです。 https://aws.amazon.com/jp/compliance/data-center/data-centers/
8	個人情報を取り扱う際はオフィスなどで実施することとし、公共の場所等では行わないよう定めております。
9	個人情報が保存されるサーバーはAWSを利用しています。AWSが当該条件をクリアしているか不明なため、対象外としております。 なおAWSでは重要機器のあるエリアへの入室は多要素認証による厳重な保護を行っている他、設置・修理・破棄に至るまで、厳格な基準のもと管理・運用されています。またその体制は外部の監査人が定期的に検査を行っています。 https://aws.amazon.com/jp/compliance/data-center/data-layer/ これらの管理体制を踏まえ、盗難防止用チェーン等の利用と同等以上のセキュリティが担保されているものと認識してございます。
10	やくばと医療機関システムは医療機関が任意の端末で利用されるものであるため、対象外となります。
11	当社では覗き見防止フィルタを装着することとしています。
12	やくばと医療機関システムでは項番17.1に記載する方式での利用者認証を備えており、かつ一定期間ごとに自動でログアウトされるため、定期的な再ログイン（再認証）が必要です。したがって正当な権限を持たないものがログイン・不正入力することは困難です。
13	やくばと医療機関システムへのログインは予め登録されたメールアドレスとパスワードによる記憶方式の認証を必要としています。 さらに登録メールアドレスに送付されるコードによる二段階認証、または医療機関のIPアドレスを用いた接続元による制限、もしくはその両方を利用可能です。医療機関のメールアドレスの受信やIPアドレスへの接続は、一般に医療機関により支給された業務用端末のみ可能であることから、これら二段階認証や接続元の制限が、物理媒体方式の認証の要件を満たすものと認識しております。 上述2点の認証方式（記憶方式、物理媒体方式）を活用することで、やくばと医療機関システムは2要素認証の要件を満たすことが可能です。
14	利用者識別にICカード等他の手段を併用する運用を提供していないため、対象外です。
15	やくばと医療機関システムのパスワードを設定・変更する場合、登録メールアドレスに自動送信されるメールに記載されたURLのクリックによる認証が必要です。 医療機関により登録されたメールアドレスでのメール受信は、一般に本人以外が受信することは不可能であるため、本人確認の要件を満たすものと認識しております。 なおやくばと医療機関システムにおけるパスワード設定や変更に際して、その実行記録をサーバーにログとして保存しております。
16	やくばと医療機関システムではパスワードの有効期限を定めておりません。
17	やくばと医療機関システムでは、英大文字、英小文字、数字を各1字以上含む、合計8文字以上のパスワード設定を必須としております。こちらのパスワードとあわせ、項番17.1に記載の通り2要素認証をご利用いただけます。
18	類推しやすい文字列の使用や、類似するパスワードの使用をチェックする機能はございません。医療機関のパスワードポリシーに則ってご設定をお願いいたします。
19	やくばと医療機関システムではパスワードが暗号化されるため、設定した本人以外がID（メールアドレス）とパスワードの組み合わせを知ることはできません。
20	セキュリティ・デバイス等を用いた認証を採用していないため、対象外です。
21	やくばと医療機関システムでは、プライマリオーナーアカウント、オーナーアカウント、メンバーアカウントの3種の権限でアカウントを発行できます。ご利用者の職種・担当業務に応じ、各アカウントを使い分けることでアクセス管理が可能です。
22	やくばと医療機関システムへのログインや各種操作をアクセス記録として保管しています。ご利用者様への開示は行っておりませんが、ご希望の場合はご提供可能な体制を整えてございます。
23	原則としてご利用の医療機関にアクセス記録は開示しておりませんので、対象外です。
24	アクセス記録を保存しているため、対象外です。
25	やくばと医療機関システムではメールの配信のみが行われます。仮に返信があった場合も、件名、本文、添付ファイル等は破棄されるため、外部からのメール受信にともない不正な処理が実行されることはありません。
26	やくばと医療機関システムは患者向けWebアプリや連携先医療機関から、処方せん画像送信機能等を通じてファイルの授受が可能です。これらの機能においては、送信可能なファイルを画像のみに制限しています。

27	やくばと医療機関システムは医療機関が任意の端末で利用するものであるため対象外です。無線LANご利用時のセキュリティ対策は、医療機関にてご対応をお願いしております。
28	IoT機器を使用しないため対象外です。
29	従業員（正社員以外の者も含みます）の雇用に際して秘密保持に関する誓約書等への署名を義務化しております。秘密保持に関する誓約書等には雇用の終了後も一定期間、秘密保持の義務が課せられる旨の条項を含めています。 派遣従事者や業務委託（該当がある場合）については、派遣契約、業務委託契約で守秘義務に関する内容を規定し、就業に際して秘密保持に関する誓約書への署名を取得しております。秘密保持に関する誓約書には就業の終了後も、秘密保持の義務が課せられる旨の条項を含めています。
30	個人情報の取り扱い・運用を中心に、就業開始時のオリエンテーションにて行っております。また、就業開始後も、年1回程度の頻度で全社研修等を実施しております。
31	正社員につきましては正社員就業規則において退職後の秘密保持義務を定めています。また、契約社員、パートタイマー及びアルバイトにつきましても就業規則（正社員以外）で退職後の守秘義務に関する内容を規定しています。 また、従業員（正社員以外の者も含みます）の離職に際して秘密保持に関する誓約書等への署名を義務化しております。秘密保持に関する誓約書等には雇用の終了後も、秘密保持の義務が課せられる旨の条項を含めています。
32	正社員については、守秘義務の違反に該当する事由を懲戒事由として賞罰規程で定めています。 契約社員、パートタイマー及びアルバイトにつきましては就業規則（正社員以外）で守秘義務違反に該当する事由を懲戒事由として規定しています。 派遣従事者や業務委託（該当がある場合）については、派遣契約、業務委託契約で守秘義務に関する内容を規定し、就業に際して秘密保持に関する誓約書への署名を取得しており、秘密保持に関する誓約書には就業の終了も秘密保持の義務が課せられる旨の条項を含めています。これに反した場合の損害賠償についても規定がございます。
33	医療機関等の事務、運用等の委託を受けていないため、対象外です。ただし以下の通り取り組みをしております。 やくばと医療機関システムのサーバーへの直接的なアクセスは、当社正社員の一部エンジニアのみが可能な体制となっております。直接アクセスした場合も、作業者、作業内容、作業結果が記録に残る環境を構築しており、医療機関等からの求めに応じて報告が可能です。
34	医療機関等の事務、運用等の委託を受けていないため、対象外です。
35	現在は個人情報が関わる業務の外部委託を行っておりません。また医療機関等の事務、運用等の委託を受けていないため、対象外です。 なお備考32に記載の通り、委託契約内で守秘義務に関する内容を規定し、修行に際し秘密保持に関する誓約書への署名を取得していることから、外部委託が可能な環境は整えております。
36	医療機関等の事務、運用等の委託を受けておりません。ただし患者向けアプリのご利用者様や医療機関等の求めに応じて、またはシステム障害の発生時等に、医療情報を含むデータへアクセスすることはございます。なお医療情報へのアクセスは正社員の一部エンジニアが、やくばと医療機関システムのサーバーに直接アクセスすることでのみ確認可能です。正社員については、備考32に記載の通り守秘義務の違反に該当する事由を懲戒事由として賞罰規定で定めております。
37	患者向けWebアプリのご利用者様の情報は、処方せん送信日や予約した診察日を起点に、必要最低限の期間をおいた後に論理削除されます。またやくばと医療機関システムをご利用の医療機関が退会・解約をした時点で、個人情報（医療情報を含みます）は論理削除されます。これらの情報は、一定期間をおいて自動で物理削除されるシステムとなっております。したがって、原則として各種情報を手動で削除することはございません。 ただしご利用者様本人の求めなど、特定の場合は、下記のような条件・手順で手動削除が可能としております。 ・ 対応可能な従業員は、やくばと医療機関システムの個人情報にアクセス可能な正社員の一部エンジニアのみとする ・ 事業部管理の個人情報管理台帳の規定に沿って実施 ・ 実施する際はその結果とともにワークフローで記録を残す ・ システム上で消去処理が走るような情報については、消去処理が間違いなくされる事を前検証しその履歴を残す。
38	情報処理機器は暗号化処理しているため、内部の情報を読み出すことは困難です。 また廃棄の際は専門知識を有する外部業者に委託し粉砕処理しております。 なお委託先とは守秘義務に関する条項を含む委託契約を締結しており、情報処理機器の廃棄についてはマニフェスト制度に則った運用体制を整備してございます。
39	個人情報はクラウド上にのみ保管することとし、各情報処理機器のローカルには保管しないこととしているため、対象外です。なおその上で、備考38に記載の通り、情報処理機器を含む各種媒体の破棄は社内ITにより取りまとめて行われております。
40	全社的に定める規定に基づき業務を遂行しております。また守秘義務については、備考29、31、32にそれぞれ記載の通りです。
41	医療情報システムの改造と保守を目的とした動作確認においてはダミーデータ等を用いることとしており、個人情報を含むデータを使用していないため対象外です。
42	やくばと医療機関システムの改造や保守の作業に伴っての個人情報へのアクセスは原則として行いません。しかし、仮に必要になった場合は、アクセスした対象・範囲等を提供できる体制を備えております。
43	医療情報や個人情報へのアクセスは、IPアドレスを用いて社内ネットワークからの接続に制限しているため、アクセスに必要なアカウント情報が外部流出したのみでは、外部流出等の不正使用ができない環境となっております。 また医療情報や個人情報は、正社員の一部担当エンジニアがデータベースに直接アクセスすることでのみ参照可能です。その際に必要となるアカウント情報は、担当エンジニアが離職・担当替え等をした場合にも、即座に削除できるよう体制を整備し運用しています。また情報処理端末を紛失した場合等の対応フローについても、全従業員向けに周知してございます。
44	外部委託していないため対象外です。

45	原則としてメンテナンス等は医療機関への影響がない形での実施となります。ただしサービスを停止する必要がある際など、規定の条件を満たした場合は事前に医療機関等に告知を行い、また終了後にも報告を行っております。これらの事前告知・報告には、やくばと医療機関システムに登録のメールアドレス等に宛てたメール連絡によって行われます。
46	外部委託していないため対象外です。ただし外部委託する場合の守秘義務契約の必要性については認識しており、契約書雛形に該当する内容を含めております。
47	個人情報を含むデータを組織外に持ち出すことを禁止しているため対象外です。
48	リモートメンテナンスとは医療機関等への情報処理端末を遠隔で操作してメンテナンスを行うことと認識しております。この前提において、リモートメンテナンスは行っていないため、対象外です。
49	・ 情報処理端末の持ち出し時の管理方法、注意点 ・ 情報処理端末の紛失や盗難にあった場合の緊急連絡先や対応フロー などの規定を社内ITにより定めています。これらの規定は個人情報の取り扱い・運用を中心に、就業開始時のオリエンテーションにて教育を行っており、就業開始後も年1回程度の頻度でセキュリティ実施教育を行っています。
50	情報処理端末の利用はログインを必須としており、その際に必要となるパスワードは全社的な以下のパスワードポリシーに従って設定されます。 ・ 英大文字、英小文字、数字、記号を各1字以上含む、合計10字以上の類推しづらい文字列とすること ・ パスワードはサービスごとに異なるものを設定し、使いまわしをしないこと ・ パスワードを再設定する際は、同じパスワードを再利用しないこと ・ パスワードは自分のみが知るものとし、他人には開示しないこと ・ パスワードが漏洩しまった（誤って他人に通知した場合も含む）、または漏洩した可能性がある場合は，直ちに新たなパスワードへ変更すること
51	業務で使用する情報処理端末には、セキュリティソフト等の導入、暗号化、外部記憶媒体への書き込み不可といった制限を行っております。 また備考49に記載のある教育を行った上で、自宅ネットワークで業務を行うにあたり推奨されるネットワーク環境を周知、徹底しております。 さらに公衆WiFiなどのネットワークへの接続は禁止しており、原則として貸与している業務用スマートフォンでのテザリングで対応するよう定めております。
52	ディザスタリカバリ体制を含め、BCP対策についてはサービス成長と共に継続的に強化する体制を整え実行しています。
53	医療機関等からの連絡に基づき、非常時用のアカウントを発行可能です。やくばと医療機関システムにおける非常時用アカウントは通常時のアカウントと同様であるため、IPアドレスを用いたアクセス制限を適用するなどの管理が可能です。 また利用終了時には、医療機関等からの連絡に基づき、非常時アカウントを停止いたします。
54	データベースのバックアップを14日分保管しており、復元手段をドキュメントとして整備しております。
55	インターネット経由で利用するサービスであることを明記しています。
56	やくばと医療機関システムはSaaSとしてのサービス提供となるため、システム側で規定した認証を用いてユーザーがサービスに接続します。
57	登録医療機関がやくばと医療機関システムとデータの送受信をインターネット経由で行う場合は、通信経路を全てTLS1.2で暗号化しており、登録医療機関と本サービス間のデータ送受信における機密度の低下を防止しています。
58	やくばと医療機関システムの利用には項番17.1に示すユーザー認証が必要です。また利用中はセッションをもとに利用者が認証されたユーザーであることを常に検証しています。
59	やくばと医療機関システムは医療機関が任意の端末で利用するものであるため対象外です。ルータなどのネットワーク機器の安全性は医療機関等にてご確認をお願いいたします。なおやくばと医療機関システムとの通信にはVPNは使用しておりません。
60	すべての通信でTLS1.2による暗号化を行っております。
61	やくばと医療機関システムの利用に伴い、医療機関等にはやくばと医療機関システム利用規約に同意いただいております。当該規約の中で、保証の範囲外となる次項ならびに、当社が負う損害賠償責任について規定をしております。 https://yakubato.jp/terms/medical_institutions.html
62	やくばと医療機関システムでは、医療機関が持つ固有の医療情報を患者に公開する機能は提供しておりません。そのため、患者に向けた説明資料等も提供しておりません。 ただし、やくばと医療機関システムのアカウントを持つ医療機関の職員から、患者等に対して自由にテキスト情報を送る機能を有しています。 患者等が利用するシステムとの通信はすべてTLS1.2で暗号化しており、また患者等から医療機関にむけたテキスト送信等の通信機能を持たないため、医療機関等の内部システムに不正に侵入することはできません。
63	やくばと医療機関システムでは保存が義務付けられる文書を扱わないため非該当・対象外です。