製造業者による医療情報セキュリティ開示書チェックリスト（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版対応）

作 成 日	
製造業者	株式会社プリズム・メディカル
製品名称	PrismPacs
バージョン	Ver1.0

※本開示書の適合性をJAHIS/JIRAが証明するものではありません。

医療機関における情報セキュリティマネジメントシステムの実践(6.2)					
1 扱う情報のリストを提示してあるか？(6.2.C1)	はい	**いいえ**	対象外	備考	1
物理的安全対策(6.4)					
2 個人情報が入力・参照できる端末の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	2
技術的安全対策(6.5)					
3 離席時の不正入力防止の機能があるか？(6.5.C4)	はい	**いいえ**	対象外	備考	3
4 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	-
4．1 アクセス管理の認証方式は？(6.5.C1)					
・記憶（ID・パスワード等）	**はい**	いいえ	対象外	備考	4
・生体認証（指紋等）	はい	**いいえ**	対象外	備考	4
・物理媒体（ICカード等）	はい	**いいえ**	対象外	備考	4
・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	4
・上記のうちの二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	4
4．1．1 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.C13(1)～(5))	**はい**	いいえ	対象外	備考	4
4．1．2 セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	**いいえ**	対象外	備考	4
4．2 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	5
4．3 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	6
4．3．1 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	6
4．3．2 アクセスログへのアクセス制限機能があるか？(6.5.C8)	**はい**	いいえ	対象外	備考	6
5 時刻情報の正確性を担保する機能があるか？(6.5.C9)	はい	**いいえ**	対象外	備考	7
6 不正ソフトウェア対策を行っているか？(6.5.C10)	はい	**いいえ**	対象外	備考	8
7 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.C14)	はい	**いいえ**	対象外	備考	9
情報及び情報機器の持ち出しについて(6.9)					
8 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.C9)	はい	**いいえ**	対象外	備考	10
9 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	11
10 管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能または暗号化機能があるか？(6.9.C6、6.9.C7)	はい	**いいえ**	対象外	備考	12
災害、サイバー攻撃等の非常時の対応(6.10)					
11 非常時アカウント又は、非常時機能を持っているか？(6.10.C4)	はい	**いいえ**	対象外	備考	13
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(6.11)					
12 「外部と個人情報を含む医療情報を通信する機能」や「リモートメンテナンス機能」を有するか？(6.11)	はい	**いいえ**	対象外	備考	14
12．1 なりすましの対策（認証）機能を有するか？(6.11.C3)	はい	いいえ	対象外	備考	-
12．2 データの暗号化（S/MIME、ファイル暗号化など）が可能か？(6.11.C5)	はい	いいえ	対象外	備考	-
12．3 ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？(6.11.C4)	はい	いいえ	対象外	備考	-
12．3．1 ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？(6.11.C4)	はい	いいえ	対象外	備考	-
12．3．1．1 対応している通信方式はいずれか？(6.11.C4、C10)					
・専用線	はい	いいえ	対象外	備考	-
・公衆網	はい	いいえ	対象外	備考	-
・IP-VPN	はい	いいえ	対象外	備考	-
・IPsec-VPN	はい	いいえ	対象外	備考	-
・TLS1.2以上 高セキュリティ型、クライアント認証	はい	いいえ	対象外	備考	-
12．3．2 ネットワークの経路制御・プロトコル制御に関わる機能の適正さ（回り込み対策を含む）を証明できる文書があるか？(6.11.C4、C10)	はい	いいえ	対象外	備考	-
12．4 リモートメンテナンス機能を有するか？(6.11.C7)	はい	いいえ	対象外	備考	-
12．4．1 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機能があるか？(6.11.C7)	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)

１３　記名・押印が義務付けられた文書を扱っているか？(6.12.C1)	はい	いいえ	**対象外**	備考	-
１３．１　HPKI対応又は認定認証局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	-
１３．２　HPKI対応又は認定認証局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	-
１３．３　日本データ通信協会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	-
１３．４　日本データ通信協会認定の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	-
１３．５　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	-

真正性の確保について(7.1)

１４　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	15
１４．１　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	5
１４．２　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	5
１５　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	-
１６　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	15
１６．１　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	15
１６．２　「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	15
１６．３　確定された記録に対して、故意による虚偽入力、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	15
１７　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	-
１８　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	15
１８．１　同じ診療録等に対して更新が複数回行われた場合、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	-
１９　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	-
１９．１　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	-
１９．２　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	-

見読性の確保について(7.2)

２０　目的に応じて速やかな検索結果の出力機能があるか？(7.2.C3)	**はい**	いいえ	対象外	備考	-
２１　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	16
２１．１　冗長化手段があるか？(7.2.C4)	はい	いいえ	対象外	備考	16
２１．２　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	13

保存性の確保について(7.3)

２２　いわゆるコンピュータウイルスを含む不適切な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するための防護機能があるか？(7.3.C1(1))	はい	**いいえ**	対象外	備考	8
２３　記録媒体及び記録機器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？(7.3.C2(1))	はい	**いいえ**	対象外	備考	-
２４　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	-
２５　システムが保存する情報へのアクセスについて、履歴を残す機能があるか？(7.3.C2(4))	**はい**	いいえ	対象外	備考	6
２５．１　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するための機能があるか？(7.3.C2(4))	**はい**	いいえ	対象外	備考	6
２６　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を用いて、き損前の状態に戻すための機能があるか？(7.3.C2(5))	はい	**いいえ**	対象外	備考	-
２７　記録媒体が劣化する前に情報を新たな記録媒体又は、記録機器に複写する機能があるか？(7.3.C3(1))	はい	**いいえ**	対象外	備考	17
２８　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に関しては標準形式で、標準形式が存在しない項目で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	-
２９　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を備えているか？(7.3.C4(2))	**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.)

３０　診療録などをスキャナなどにより電子化して保存する機能があるか？(9.1.C1)(9.4)	はい	いいえ	**対象外**	備考	18
３０．１　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	-
３０．２　電子署名・タイムスタンプ等を行える機能があるか？(9.1.C2)(9.4.C2)	はい	いいえ	対象外	備考	-

備考記載欄	
1	本製品は、DICOM形式で画像を保管します。画像には、データの他に患者情報や検査情報等が含まれます。
2	本製品は、画像ビューワソフトウェアであり、お客様が指定したサーバ等にインストールして使用し、参照端末およびサーバ等のハードウェアは、お客様の管理となります。お客様でセキュリティポリシーを決めていただき、運用・管理をお願いしております。 下記内容をご検討ください。 ・ディスプレイにのぞき見防止フィルムを張る ・ロック画面(Win + L)の使用 ・パニック画面を呼び出すソフトウェアの導入
3	ソフトウェアの起動は、IDとパスワードで管理されております。離席時にはログアウトを推奨しています。 下記内容をご検討ください。 ・Windowsのスクリーンセーバー(自動ロック)の設定を行う
4	IDとパスワードでログイン可能となっております。 生体認証、物理媒体、二要素認証を使用したい場合は、クライアントPCのWindows Helloの使用を検討してください。
5	管理の職種・担当業務別および利用者ごとの機能の利用権限の設定が可能です。
6	アクセスログを含むサーバーおよびクライアントの詳細な動作ログを記録しています。 管理者権限で閲覧することが可能です。
7	使用する端末の運用に関しては、本製品の提供範囲外となります。 装置から送信された画像のDICOMタグの検査時刻を表示します。装置側で時刻情報の正確性を担保する必要があります。 その他は、下記内容をご検討ください。 ・サーバーやクライアントPCがインターネットに接続できる場合は、公開タイムサーバー(NTPサーバー)との同期 ・イントラネット内での運用の場合は、タイムサーバーの導入 医療機関側の情報参照端末については、お客様にて無線LAN環境セキュリティポリシーを決めていただき、その徹底をお願いしております。
8	使用する端末の運用に関しては、本製品の提供範囲外となります。 下記内容をご検討ください。 ・ウィルス対策ソフトの導入
9	使用する端末の運用に関しては、本製品の提供範囲外となります。 下記内容をご検討ください。 ・ステルスモード、アクセス制限、暗号方式等の設定
10	使用する端末の運用に関しては、本製品の提供範囲外となります。 下記内容をご検討ください。 ・ソフトウェアのインストールの制限
11	使用する端末の運用に関しては、本製品の提供範囲外となります。 下記内容をご検討ください。 ・接続できるデバイスの制限
12	使用する端末の運用に関しては、本製品の提供範囲外となります。 下記内容をご検討ください。 ・ディスクの暗号化
13	非常時のユーザーアカウントは、お客様で管理・運用いただけます。 非常時の運用に関しては、本製品の提供範囲外となります。 下記内容をご検討ください。 ・システムが利用できなくなった場合の代替案の策定
14	リモートメンテナンスの運用に関しては、本製品の提供範囲外となります。 リモートメンテナンスを行う場合は、下記内容をご検討ください。 ・VPNワイドの導入 ・VPNルーターの導入 ・ソフトウェアVPNの導入 ・リモートアクセス用のソフトウェアの導入
15	本製品は、装置から転送されたDICOM規格を遵守した画像をそのまま保管および参照し、画像に関しては、入力および確定者の認証は、ありません。 管理者権限で情報を修正した場合は、修正ログが保存されます。 レポート機能に関して、入力権限および確定権限を設定し、修正や確定履歴を記録しています。
16	使用するサーバの運用に関しては、本製品の提供範囲外となります。 サーバは、RAID5以上を推奨しています。 その他、ネットワーク、ストレージは、ご施設のセキュリティポリシーに従って設定を御願いしております。
17	バックアップの運用に関しては、本製品の提供範囲外となります。 画像を保管するサーバは、RAID5以上の毀損を予防するハードウェアを推奨しています。 またバックアップデータの保管を推奨しており、バックアップから毀損前の状態に戻すことも可能です。
18	本製品は、参照端末およびサーバおよびその他のハードウェアは、お客様の管理となります。 ソフトウェア的に、スキャナーなどにより取り込んだ画像をDICOM変換して保存することは、可能です。
19	
20	
21	
22	