医療情報システムの安全管理に関するガイドライン 第３版
最低限のガイドライン遵守チェックリスト

本遵守チェックリストは、平成20年3 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３版 」の1 章～6 章における「最低限のガイドライン」の遵守状況のチェックリストである。

更新情報	最終更新日	平成21年6月29日

組織的安全管理対策

No.	チェック項目	実施済	実施内容
1.	情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行っている。	■	運用責任者を1名、担当者を2名設置
2.	個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めている。	■	入退館管理規程を定めている。
3.	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。	■	システム管理規程を定めている。
4.	個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めている。	■	業務委託契約書において、本ガイドラインに準拠した管理を遵守するよう定めている。
5.	運用管理規程等において次の内容を定めている。 (a)個人情報の記録媒体の管理（保管・授受等）の方法 (b)リスクに対する予防、発生時の対応の方法	■	システム管理規程、リスク認識および対応規程を定めている。

物理的安全対策

No.	チェック項目	実施済	実施内容
1.	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。	■	ICカードキーと暗証番号鍵を二重に設置。
2.	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、業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策を講じている。もしくは、同等レベルの他の取りうる手段がある。	■	ICカードキーと暗証番号鍵が二重に設置。
3.	個人情報の物理的保存を行っている区画への入退管理を実施している。	■	ICカードキーと暗証番号鍵が二重に設置。
4.	入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録している。	■	名札着用の義務化およびICカードの入退室ログ管理。
5.	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。	■	ICカードの入退室ログ管理および監視カメラによる常時監視。
6.	個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置している。	■	盗難防止用チェーンを設置している。
7.	離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施している。	■	①スクリーンセーバーの設定 ②ID、パスワードによるアクセス制御

技術的安全対策

No.	チェック項目	実施済	実施内容
1.	情報システムへのアクセスにおける利用者の識別と認証を行っている。	■	①パスワード ②アクセスログ管理
2.	動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意している。	■	動作確認等で使用するデータは原則としてダミーデータを用いる。
3.	医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行っている。	■	管理者とオペレーターでアクセス権限を分けている。
4.	アクセスの記録及び定期的なログの確認を行っている。	■	実施している。
5.	アクセスの記録に用いる時刻情報は信頼できるものである。	■	毎日正確な時刻情報を取込んで調整している。
6.	システム構築時や、適切に管理されていないメディアを使用したり、外部からの情報を受け取る際にはウイルス等の不正なソフトウェアの混入がないか確認している。	■	毎日最新のウィルスチェックプログラムを更新した上で外部情報の安全を確認している。

7.	パスワードを利用者識別に使用する場合			
	(1)	システム内のパスワードファイルでパスワードは必ず暗号化(不可逆変換)され、適切な手法で管理及び運用が行わっている。(利用者識別にＩＣカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること)	■	利用者のパスワードは暗号化している。ＩＣカードによる利用者識別は実施していない。
	(2)	利用者がパスワードを忘れたり、盗用される恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施している。	■	ローカルシステムでは本人に直接パスワードを手渡し、センターシステムでは申し込み用紙に記入して、セキュアな一時保管システムでパスワードを渡している。
	(3)	システム管理者であっても、利用者のパスワードを推定できる手段を防止している。(設定ファイルにパスワードが記載される等があってはならない。)	■	実施している。
	また、利用者は以下の事項に留意している。			
	(1)	パスワードは定期的に変更し（最長でも2ヶ月以内）、極端に短い文字列を使用しない（英数字、記号を混在させた8文字以上の文字列としている）。	■	実施している。
	(2)	類推しやすい、不注意によるパスワードの盗用は、盗用された本人の責任になることを認識している。	■	周知している。
8.	無線LANを利用する場合			無線ＬＡＮは使用していない。
	(1)	利用者以外に無線LANの利用を特定されないようにしている。	□	
	(2)	不正アクセスの対策を施ししている。少なくともSSIDやMACアドレスによるアクセス制限。	□	
	(3)	不正な情報の取得を防止している。例えば、WPA/TKIP、WPA2/AES等により、通信を暗号化し情報を保護する。	□	
	(4)	電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意している。	□	
	(5)	適用に関しては、総務省発行の「安心して無線LANを利用するために」を参考にしている。	□	

人的安全対策（従業者に対する人的安全管理措置）

No.	チェック項目	実施済	実施内容
1.	法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行っている。	■	雇用及び契約時に誓約書を取付けている。
2.	定期的に従業者に対し教育訓練を行っている。	■	個人情報保護に関する研修会を従業者全員に実施している。
3.	従業者の退職後の個人情報保護規程を定めている。	■	退職時に誓約書を取付けている。

人的安全対策（事務取扱委託業者の監督及び守秘義務契約）

No.	チェック項目	実施済	実施内容
1.	プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で病院事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行っている。		
	①	受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結している	■	業務委託契約書において守秘義務を規定している。
	②	保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなっている。	■	メール及び口頭（電話）で報告を実施している。
	③	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。	■	作業に立会い、システムに触れないよう監視している。
	④	委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件としている。	■	業務委託契約書において規定している他、直接再委託先とも内容を確認している。

2.	プログラムの異常等で、保存データを救済する必要があるとき等、やむをえ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づけられた守秘契約等の秘密保持の対策を行っている。	■	外部の保守要員が個人情報にアクセスすることは原則としてない。 障害時等で個人情報DBにアクセスする場合は罰則のある守秘契約等の秘密保持をしている要員で作業をしている。

情報の破棄

No.	チェック項目	実施済	実施内容
1.	「方針の制定と公表(同ガイドライン6.1）」で把握した情報種別ごとに破棄の手順を定めるている。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めている。	■	個人情報管理台帳にて管理し、規定に従って破棄している。
2.	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ものが行うこととし、残存し、読み出し可能な情報がないことを確認している。	■	外部事業者に委託し、証明書発行を義務付けている。
3.	外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策（事務取扱委託業者の監督及び守秘義務契約）」に準じ、さらに委託する医療機関等が確実に情報の破棄が行なわれたことを確認している。	■	外部事業者に委託し、証明書発行を義務付けている。
4.	運用管理規程において下記の内容を定めている。		
	(a) 不要になった個人情報を含む媒体の廃棄を定める規程の作成	■	機器の管理規程を定めている。

情報システムの改造と保守

No.	チェック項目	実施済	実施内容
1.	動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めている。	■	開発会社が個人情報を含むデータを扱う作業を行う場合は当社の立会い及び許可に基づいて実施している。
2.	メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、およびアクセスした場合は対象個人情報を含む作業記録を残している。	■	保守要員個人のアカウントで作業するようにしている。
3.	そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めている。	■	アカウント情報は台帳管理している。また、個人情報が保管されているサーバー・クライアントには外部ネットワークと接続されていない。
4.	保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えている。	■	アカウントを台帳管理しており、個人情報が保管されているサーバー・クライアントには外部ネットワークと接続されていない。離職や担当変えが有った場合はアカウントが盗まれてもアクセス不可能。
5.	保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めている。それらの書類は医療機関等の責任者が逐一承認している。	■	メール及び口頭（電話）で事前申請、報告を実施している。
6.	保守会社と守秘義務契約を締結し、これを遵守させている。	■	実施している。
7.	保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認している。	■	委託事業者が個人情報を当社外に持ち出すことは禁止している。
8.	リモートメンテナンスによるシステムの改造や保守が行なわれる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認している。	□	リモートメンテナンスは行っていない。
9.	再委託が行なわれる場合は再委託する事業者にも保守会社と同等の義務を課している。	■	実施している。

情報および情報機器の持ち出しについて

No.	チェック項目	実施済	実施内容
1.	組織としてリスク分析を実施し、情報および情報機器の持ち出しに関する方針を運用管理規程で定めている。	■	定めている
2.	運用管理規程には、持ち出した情報および情報機器の管理方法を定めている。	■	システム管理規程で定めている。
3.	情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めている。	■	緊急時対応規程で定めている。
4.	運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行っている。	■	個人情報保護に関する研修会を従業者全員に実施している。
5.	医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握している。	■	管理台帳にて管理している。
6.	情報機器に対して起動パスワードを設定している。設定にあたっては推定しやすいパスワードなどの利用を避けたり、定期的にパスワードを変更する等の措置を行っている。	■	実施している。
7.	盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにしている。	■	外部へ個人情報を持出す場合は必ず暗号化している。
8.	持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施している。なお、ネットワークに接続する場合は「6．11 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」の規程を遵守している。	■	外部との個人情報の交換は ①暗号化 ②ウィルスチェック ③電子証明書による認証 の安全対策を含む「セコムデーター時保管サービス」を利用して行っている。
9.	持ち出した情報を、例えばファイル交換ソフト（Winny等）がインストールされた情報機器で取り扱っていない。医療機関等が管理する情報機器の場合は、このようなソフトウェアをインストールしていない。	■	ファイル交換ソフトのようなソフトウェアはインストールしていない。
10.	個人保有の情報機器（パソコン等）であっても、業務上、医療機関等の情報を取り扱ったり、医療機関等のシステムへアクセスするような場合は、管理者の責任において上記の6、7、8、9と同様の要件を遵守させている。	■	個人保有の情報機器の事務所への持ち込みは禁止しており、医療機関等の情報の取り扱いおよびシステムへのアクセスはできない。

災害等の非常時の対応

No.	チェック項目	実施済	実施内容
1.	医療サービスを提供し続けるためのBCPの一環として“非常時”と判断する仕組み、正常復帰時の手順を設けている。	■	手順を設けている。
2.	正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意している。	■	規約がある。
3.	「非常時のユーザアカウントや非常時用機能」の管理手順を整備している。	■	整備している
4.	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にし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理および監査を行っている。	■	非常時用に切り替わる場合には監視にて検知する仕組みを整備している。
5.	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出来ないように変更している。	■	非常時用ユーザアカウントは使用しない。
6.	サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に支障が発生する場合は、別途定める所管官庁への連絡を行っている。	■	外部ネットワークには接続していない。

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

No.	チェック項目	実施済	実施内容
1.	ネットワーク経路でのメッセージ挿入、ウイルス混入などの改ざんを防止する対策、施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策、セッション乗っ取り、IPアドレス詐称などのなりすましを防止する対策をとっている。	■	外部ネットワークには接続していない。
2.	データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めている。	■	外部ネットワークには接続していない。
3.	施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとっている。	■	①パスワード ②アクセスログ管理 ③監視カメラによる常時監視
4.	ルータなどのネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPNの間で送受信ができないように経路設定されている。	■	外部ネットワークには接続していない。

5.	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などのセキュリティ対策を実施している。たとえば、SSL/TLSの利用、S/MIMEの利用、ファイルに対する暗号化などの対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用している。	■	外部ネットワークには接続していない。
6.	医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社など多くの組織が関連する。 そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にしている。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通または著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処	■	外部ネットワークには接続していない。
7.	また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。 ・交換した医療情報等に対する管理責任および事後責任の明確化。 ・個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。	■	機器や回線についての契約を締結し、責任を明確化している。 患者は業務の対象外。 専任の管理者を設置している。 業務委託契約書において健診・保健指導実施機関の責任を定義。 患者は業務の対象外。
8.	リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止している。	■	リモートメンテナンスは行っていない。
9.	回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認している。	■	サービス提供会社にて二重化を行ない、可用性を担保していることを仕様書などで確認している。
10.	患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施している。 また、情報の主体者となる患者等へ危険性や提供目的の納得できる説明を実施し、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。	■	保健指導対象者が閲覧する場合、個人認証を実施したうえで、SSL暗号化通信により参照可能としている。 インフラ環境として、ファイアウォール、アクセス監視を実施する。