

運営についての重要事項に関する規程の概要[保健指導機関]

- *健診と保健指導の両方を実施する者は、健診機関分とは別々に作成・掲出等すること。
- *多くの拠点を抱えている事業者の場合は、各拠点単位で別々にこれを作成・掲出等すること。
- *選択肢の項目については、□を■にするか、該当する選択肢のみ残す（非該当は削除）こと。

更新情報	最終更新日	2025 年 6 月 10 日
------	-------	-----------------

*下記事項に変更があった場合は速やかに変更し、掲載しているホームページ等更新し、更新日を明示すること。

機関情報	機関名 ^{注1)注2)}		株式会社メディカルリソース
	所在地 ^{注1)}	(郵便番号)	108 - 0014
		(住所)	東京都港区芝 5-33-11 田町タワー8階
	電話番号 ^{注1)}		03 - 6665 - 9160
	FAX番号		03 - 6665 - 9167
	保健指導機関番号 ^{注3)}		1322500024
	窓口となるメールアドレス		wd-info@nicho.co.jp
	ホームページ ^{注4)}		https://www.workersdoctors.co.jp/
	経営主体 ^{注1)}		株式会社メディカルリソース
	開設者名 ^{注1)}		小林 信幸
	管理者名 ^{注5)}		栗原 弘治
	保健指導業務の統括者名 ^{注6)}		井上 真結菜
	第三者評価 ^{注7)}		<input type="checkbox"/> 実施（実施機関： ） <input checked="" type="checkbox"/> 未実施
	認定取得年月日 ^{注7)}		2025 年 6 月 2 日
契約取りまとめ機関名 ^{注8)}			
所属組織名 ^{注9)}			

- 注1) 社会保険診療報酬支払基金（以下「支払基金」という）に届け出る（あるいは届け出ている）内容と同一の内容とする
- 注2) 正式名称で記載。複数拠点を持つ法人の場合は、正式名称が拠点名のみであれば拠点名、法人名+拠点名（例：「株式会社△△サービス〇〇店」「財団法人〇〇 △△健診センター」等）であればその通りに記載
- 注3) 届出により支払基金から番号が交付されている機関のみ記載
- 注4) ホームページを開設している機関のみ記載。複数ある場合は最も機関の概要がわかる情報が掲載されているサイト（例：自院ページ、地区医師会ページ、医療情報提供制度に基づく都道府県ホームページ等）のアドレスを記載
- 注5) 特定保健指導を実施する各拠点における常勤の管理者。但し、管理上支障がない場合は、保健指導機関の他の職務に従事し、又は同一の敷地内にある他の事業所、施設等の職務に従事することができるものとする。施設管理や人事管理、会計管理等を想定。従って管理者は必ずしも医師等でなくともよい（統括者との兼務は可）。
- 注6) 統括者とは、特定保健指導を実施する各拠点において、動機付け支援及び積極的支援の実施その他の特定保健指導に係る業務全般を統括管理する者（常勤の医師・保健師・管理栄養士）。各拠点において、当該拠点に配置されている保健師等の保健指導実施者を束ね、各実施者が担当する保健指導対象者への支援の実施状況等を包括的に管理している者を想定。拠点ごとに配置し、複数拠点の兼務は不可。
- 注7) 何らかの評価機関において、評価を受けた場合のみ記載
- 注8) 個別契約のみで、どこのグループにも属していない場合は記載不要
- 注9) 機関が支部・支店等の拠点の場合、所属する法人名（本部組織名）を記載（正式名称で）。所属組織とは、主として注2の例にあるような法人を想定（医師会は除く）。なお、契約取りまとめ機関名との包含関係としては、契約取りまとめ機関≧本部組織>機関（支部・支店等）となる。

協力業者情報	協力業者の有無 ^(積極的支援)	<input checked="" type="checkbox"/> 全て自前で実施 <input type="checkbox"/> 支援形態・地域等で部分委託	
	協力業者名・委託部分 ^{注10)}	業者名	委託部分
		業者名	委託部分

注10) 協力業者がある場合のみ、例に従って明瞭簡潔に記載。

スタッフ 情報 ^{注11)}	自機関内				協力業者 ^{注10)}	
	常勤		非常勤		総数	左記のうち一定の研修修了者数 ^{注12)}
	総数	左記のうち一定の研修修了者数 ^{注12)}	総数	左記のうち一定の研修修了者数 ^{注12)}		
医師	人	人	人	人	人	人
(上記のうち、日本医師会認定健康スポーツ医)	人	人	人	人	人	人
保健師	3人	人	人	人	人	人
管理栄養士	人	人	人	人	人	人
看護師(一定の保健指導の実務経験のある者)	人	人	人	人	人	人
専門的知識及び技術を有する者	歯科医師	人	人	人	人	人
	THP取得者	人	人	人	人	人
	健康運動指導士	人	人	人	人	人
事務職員	20人	人	人	人	人	人

注11) 特定保健指導に従事する者のみを記載。

注12) 一定の研修とは、「標準的な健診・保健指導プログラム」の巻末にある「健診・保健指導の研修ガイドライン」に準拠した研修等をいう。

保健指導 の実施体制		保健指導事業の統括者	初回面接、計画作成、評価に関する業務を行者	3ヶ月以上の継続的な支援を行う者			
				個別支援	グループ支援	電話	電子メール等 ^{注13)}
医師		<input type="checkbox"/> 常勤	<input type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者				
保健師		<input checked="" type="checkbox"/> 常勤	<input checked="" type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者	<input checked="" type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者	<input checked="" type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者	<input checked="" type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者	<input checked="" type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者
管理栄養士		<input type="checkbox"/> 常勤	<input type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者				
看護師(一定の保健指導の実務経験のある者)			<input type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者				
専門的知識及び技術を有する者	歯科医師			<input type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者			
	THP取得者			<input type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者			
	健康運動指導士			<input type="checkbox"/> 常勤 <input type="checkbox"/> 非常勤 <input type="checkbox"/> 協力業者			

*該当する項目を全て選ぶこと（複数選択可）

注 3) FAX や手紙等も含む

施設及び設備情報	利用者に対するプライバシーの保護 ^{注14)}	<input checked="" type="checkbox"/> 有	<input type="checkbox"/> 無
	個人情報保護に関する規程類	<input checked="" type="checkbox"/> 有	<input type="checkbox"/> 無
	受動喫煙対策	<input type="checkbox"/> 敷地内禁煙	<input type="checkbox"/> 施設内禁煙 <input checked="" type="checkbox"/> 完全分煙 <input type="checkbox"/> なし
	指導結果の保存や提出における標準的な電子的様式の使用	<input checked="" type="checkbox"/> 有	<input type="checkbox"/> 無

注 4) 保健指導時における、必要な箇所(個別面接の実施時等)への間仕切りやついたて等の設置、別室の確保等の配慮等が為されているかの有無

運営に関する情報	実施日及び実施時間 ^{注15)}	特定時期	通年	平日 9:00-18:00	
	実施地域 ^{注16)}	全国			
	実施サービス ^{注17)}	<input checked="" type="checkbox"/> 動機付け支援		<input checked="" type="checkbox"/> 積極的支援	
	実施形態 ^{注17)}	<input type="checkbox"/> 施設型		<input checked="" type="checkbox"/> 非施設型	
	継続的な支援の形態や内容 ^{注17)}	<input checked="" type="checkbox"/> 個別支援		<input type="checkbox"/> グループ支援 <input checked="" type="checkbox"/> 電子メール等 ^{注13)}	
	標準介入期間(積極的支援) ^{注18)}	<input checked="" type="checkbox"/> 3ヶ月		<input type="checkbox"/> 4ヶ月 <input type="checkbox"/> 5ヶ月 <input type="checkbox"/> 6ヶ月	
	課金体系	<input checked="" type="checkbox"/> 完全従量制(従量単価×人数)		<input type="checkbox"/> 固定費+従量単価×人数	
	標準的な従量単価 ^{注19)}	動機付け	15,000 円以下/人	積極的	30,000 円以下/人
		動機付け支援相当	円以下/人		
	単価に含まれるもの ^{注17・注20)}	<input checked="" type="checkbox"/> 教材費(紙類のみならず万歩計等機器類や血液検査キット等も含む) <input checked="" type="checkbox"/> 会場・施設費 <input checked="" type="checkbox"/> 交通費(指導者の) <input type="checkbox"/> 材料費(調理実習) <input checked="" type="checkbox"/> 通信費・事務費 <input checked="" type="checkbox"/> 一定回数の督促			
	単価に含まれない追加サービスの有無 ^{注17)}	<input type="checkbox"/> 調査・計画費 <input type="checkbox"/> データ分析費 <input type="checkbox"/> 各種案内代行費 <input checked="" type="checkbox"/> 特に無し			
	積極的支援の内容 ^{注21)}	合計 180 ポイント以上の継続支援を実施。特に、これまでの産業保健事業実績により蓄積したノウハウで、質の高いサービスを提供。			
	動機付け支援相当の内容	食事面や生活面の課題を明らかに 3ヶ月以上継続した生活習慣改善サポートを実施			
	救急時の応急処置体制 ^{注22)}	<input type="checkbox"/> 有		<input checked="" type="checkbox"/> 無	
	苦情に対する対応体制 ^{注23)}	<input checked="" type="checkbox"/> 有		<input type="checkbox"/> 無	
保健指導の実施者への定期的な研修	<input checked="" type="checkbox"/> 有		<input type="checkbox"/> 無		
インターネットを用いた保健指導における安全管理の仕組みや体制 ^{注24)}	<input checked="" type="checkbox"/> 有		<input type="checkbox"/> 無		

注 5) どちらだけでも、どちらも記載可

注 6) 非施設型の保健指導を実施している場合についてのみ記載

注 7) 複数回答可 (項目「単価に含まれない追加サービスの有無」において「特に無し」と他との複数選択は不可)

注 8) 最も標準的な支援メニューにおける所要期間 (対象者による遅延・延長は考慮に入れない)。いずれか一つを選択

注 9) 最も標準的な支援メニューの単価 (一つのメニューでも、契約人数の多少等により多様な契約単価がある場合は、そのうちの最高額) を記載

注 20) 営業費用、採用・研修等費用、その他間接コスト等は、単価の中の人件費に含まれる利益・技術料等から適宜配分するものとする

注 21) 項目「標準的な従量単価」の積極的支援の単価における標準的な支援内容を明瞭・簡潔に記載。

注 22) 緊急時に医師が迅速に対応できる体制の有無 (医師が常駐していない機関の場合は、医師と緊密に連携し緊急時に

は搬送もしくは医師が駆けつける体制となっているか)。※医療機関は原則として「有」と想定される

注2 3) 利用者や保険者による苦情が発生した場合に、それを受け付け、改善、申し立て者への結果報告等を行う窓口や担当等が設けられているか。※医療機関は原則として「有」と想定される

注2 4) インターネットを利用した保健指導（介入のみならず事務的なやり取りや記録等も含む）を行う機関のみ記載

その他	掲出時点の前年度 の特定保健指導の 実施件数	動機付け	年間	人	1日当たり	人
		積極的	年間	人	1日当たり	人
		動機付け支援担当	年間	人	1日当たり	人
	実施可能な特定保 健指導の件数	動機付け	年間	人	1日当たり	人
		積極的	年間	人	1日当たり	人
		動機付け支援担当	年間	人	1日当たり	人
	掲出時点の前年度の参 加率(参加者/案内者)・脱落 率(脱落者/参加者) ^{注2 5)}	動機付け	参加率	%	脱落率	%
		積極的	参加率	%	脱落率	%
		動機付け支援担当	参加率	%	脱落率	%
	特定健康診査の実施		<input type="checkbox"/> 有 <input checked="" type="checkbox"/> 無			

注2 5) 参加率については機関において案内発送まで受託している場合のみ記載可能

別添 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 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、令和4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5.2版」の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。

*代行機関の業務を実施する者は、本資料を作成しホームページ（自機関のWebサイトでも他のサイトでも可）に掲出すること。

*選択肢の項目については、「実施済」「実施予定」より一つ選び、□を■にすること。「実施予定」を選択した場合は、実施予定時期を明記すること。

更新情報	最終更新日	2025	年	6	月	10	日
------	-------	------	---	---	---	----	---

*下記事項に変更があった場合は速やかに変更し、掲載しているホームページを更新し、更新日を明示すること。

組織的安全管理対策

No	チェック項目	実施済	実施予定(実施時期)
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。	■	□()
2.	個人情報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。	■	□()
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。	■	□()
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。	■	□()
5.	運用管理規程等において次の内容を定めている。 (b) 医療機関等の体制 (c) 契約書・マニュアル等の文書の管理 (d) リスクに対する予防、発生時の対応の方法 (e) 機器を用いる場合は機器の管理 (f) 個人情報の記録媒体の管理(保管・授受等)の方法 (g) 患者等への説明と同意を得る方法 (h) 監査 (i) 苦情・質問の受付窓口	□	■(2025年6月)

物理的安全対策

No	チェック項目	実施済	実施予定(実施時期)
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。	■	□()
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、運用管理規定に基づき許可された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	■	□()
3.	個人情報の物理的保存を行っている区画への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。	■	□()
4.	個人情報の物理的保存を行っている区画への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。	■	□()
5.	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。	■	□()
6.	個人情報が入力・参照できる端末の覗き見防止対策を実施している。	■	□()

技術的安全対策

No	チェック項目	実施済	実施予定(実施時期)
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。	■	□()

No	チェック項目	実施済	実施予定(実施時期)
2.	本人の識別・認証にユーザIDとパスワードの組み合わせを用いる場合には、本人しか知り得ない状態に保つよう対策を行っている。	■	□()
3.	本人の識別・認証にICカード等のセキュリティ・デバイスを用いる場合には、ICカードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意している。	□	■()
4.	利用者が個人情報を入力・参照できる端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防衛策を講じている。	■	□()
5.	動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意している。 ^{注1)}	■	□()
6.	関係職種ごとに、アクセスできる情報の範囲を定め、そのレベルに沿ったアクセス管理を行っている。	■	□()
7.	アクセスの記録及び定期的なログを確認している。 ^{注2)}	■	□()
8.	アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を講じている。	■	□()
9.	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。 ^{注3)}	■	□()
10.	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。 ^{注4)}	■	□()
11.	メールやファイル交換にあたっては、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、無害化処理を実施している。なお、保守等でやむを得ずファイル送付等を行う場合、送信側で無害化処理が行われていることを確認している。	■	□()
12.	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)され、適切な手法で管理及び運用が行われている。 ^{注5)}	■	□()
13.	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。また、パスワード漏洩の恐れがある場合には、速やかにパスワードの変更も含む適切な処置を講じている。	■	□()
14.	システム運用担当者であっても、利用者のパスワードを推定できる手段を防止している。 ^{注6)}	■	□()
15.	パスワードは以下のいずれかの要件を満たしている。また、いずれの場合においても、他に講じられているセキュリティ対策等の内容を勘案して、全体として安全なパスワード漏洩対策を講じている。 <ul style="list-style-type: none"> ・ 英数字、記号を混在させた13文字以上の推定困難な文字列 ・ 英数字、記号を混在させた8文字以上の推定困難な文字列を定期的に変更している(最長でも2ヶ月以内) ・ 二要素以上の認証の場合、英数字、記号を混在させた8文字以上の推定困難な文字列(ただし、他の認証応訴として必要な電子証明書等の使用にPIN等が設定されている場合には、この限りではない) 	■	□()
16.	類推しやすいパスワードを使用せず、類似のパスワードを繰り返し使用していない。 ^{注7)}	■	□()
17.	適切な利用者以外に無線LANの利用を利用されないようにしている。	■	□()
18.	無線LANを利用する場合、不正アクセスの対策を施している。	■	□()
19.	無線LANを利用する場合、不正な情報の取得を防止している。	■	□()
20.	無線LANを利用する場合、電波を発する機器(携帯ゲーム機等)による電波干渉に留意している。	■	□()
21.	IoT機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規定を定めている。	□	■()

No	チェック項目	実施済	実施予定(実施時期)
22.	IoT 機器を利用する場合、セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと患者等が留意すべきことについて患者等に説明し、同意を得ている。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供している。	<input type="checkbox"/>	■ ()
23.	IoT 機器を利用する場合、システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用している。アップデートが困難な場合に代替措置を講じる方法を検討し、運用している。	<input type="checkbox"/>	■ ()
24.	IoT 機器を利用する場合、使用が終了した又は不具合のため使用を停止したIoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じている。	<input type="checkbox"/>	■ ()

注1:動作確認用データの情報管理を厳格に行い、動作確認終了後は適切に破棄を行うことを指す。

注2:アクセスの記録は少なくとも利用者のログイン時刻および時間、ログイン中に操作した情報が特定できることを指す。また、情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録(操作者及び操作内容)を以って代えることができる。

注3:代行機関の内部で使用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と操作事実の記録として問題のない範囲の精度を保つことを指す。

注4:適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用し、常時ウイルス等の不正ソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持(例えばパターンファイルの更新の確認・維持)を行うこと。

注5: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規程にて定めることを以って代えることができる。

注6:例として設定ファイルにパスワードを記載しないようにする等があげられる。

注7:類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。

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	実施予定(実施時期)
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。	■	<input type="checkbox"/> ()
2.	定期的に従業者に対し個人情報の安全管理に関する教育訓練を行っている。	■	<input type="checkbox"/> ()
3.	従業者の退職後の個人情報保護規程を定めている。	■	<input type="checkbox"/> ()

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	実施予定(実施時期)
1.	外部受託業者を採用する場合は、包括的な委託先の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。	■	<input type="checkbox"/> ()
2.	外部受託業者を採用する場合で、保守作業等の情報システムに直接アクセスする作業の際には、作業員・作業内容・作業結果の確認を行っている。	■	<input type="checkbox"/> ()
3.	外部受託業者を採用する場合は、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。	■	<input type="checkbox"/> ()
4.	受託する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受託する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。	■	<input type="checkbox"/> ()
5.	ソフトウェアの異常等でデータを救済する必要があるとき等、やむを得ない事情で受託する事業者の保守要員が医療情報にアクセスする場合に、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。	■	<input type="checkbox"/> ()

情報の破棄

No	チェック項目	実施済	実施予定(実施時期)
1.	情報種別ごとに破棄の手順を定めている。 ^{注8)}	■	□()
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。	■	□()
3.	外部保存を受託する機関に破棄を委託した場合は、委託元の医療機関等が確実に情報の破棄が行われたことを確認している。	□	■()
4.	運用管理規程において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を定めている。	■	□()

注8:手順は、破棄を行う条件、破棄を行うことができる従業員の特定、具体的な破棄の方法を含む必要がある。

医療情報システムの改造と保守

No	チェック項目	実施済	実施予定(実施時期)
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ともに、終了後は確実にデータを消去させている。	■	□()
2.	メンテナンスを実施するためにサーバに保守事業者の作業員がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無、およびアクセスした場合対象個人情報を含む作業記録を残している。 ^{注9)}	■	□()
3.	保守要員の専用アカウント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。	■	□()
4.	保守要員の離職や担当変え等に対して速やかに保守要員の専用アカウントを削除できるよう、保守事業者に報告を義務付けるとともに、それに対応できるアカウント管理体制を整えている。	■	□()
5.	保守事業者がメンテナンスを実施する際には、日単位で作業申請の事前提出させ医療情報システム安全解離責任者が承認している。 ^{注10)}	■	□()
6.	保守事業者と守秘義務契約を締結し、これを遵守させている。	■	□()
7.	原則、保守事業者に個人情報を含むデータを外部に持ち出させていない。やむを得ない場合には、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、医療情報システム安全管理責任者が承認している。	■	□()
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われる場合には、必ずアクセスログを収集し、当該作業の終了後速やかにアクセスログの内容を医療機関等の責任者が確認している。	■	□()
9.	リモートメンテナンスにおいて、やむを得ずファイルを医療機関等へ送付等を行う場合、送信側で無害化処理が行われていることを確認している。	■	□()
10.	再委託が行われる場合は再委託先にも保守会社と同等の義務を課している。	■	□()

注9:システム利用者を模して操作確認を行うための識別・認証についても同様である。

注10: 作業申請書の承認は、原則として保守作業の実施前に行う必要があるが、保守事業者と合意したメンテナンスについては、事後承認とすることができる。

情報及び情報機器の持ち出しについて

No	チェック項目	実施済	実施予定(実施時期)
1.	リスク分析を行い、情報及び情報機器の持ち出しや、BYODの実施に関する運用管理規程を定めている。	■	□()
2.	運用管理規程には、持ち出した情報及び情報機器の管理方法を定めている。	■	□()
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。	■	□()
4.	運用規程で定めた盗難、紛失時の対応を従業員等に周知・教育を行っている。	■	□()
5.	情報が格納された可搬媒体及び情報機器の所在を台帳等により管理している。	■	□()

No	チェック項目	実施済	実施予定(実施時期)
6.	情報機器に対して起動パスワードを設定している。	■	□()
7.	盗難、置き忘れの措置として、情報に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにしている。	■	□()
8.	持ち出した情報機器を外部のネットワークや外部媒体に接続する場合は、情報端末が情報漏洩、改ざん等の対象とならない対策を施している。特にモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LANは技術的安全対策の17～20の基準を満たさないことがあるため、公衆無線LANしか利用できない環境にあり、且つ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で述べられている基準を満たした通信手段を選択することができる場合に限り認めている。	■	□()
9.	持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールしている。	■	□()
10.	個人保有の情報機器であっても、業務上、医療機関等の情報を持ち出して取り扱う場合、管理者は上記1～5の対策を行うとともに、管理者の責任において上記6～9と同様の要件を遵守している。	■	□()

災害、サイバー攻撃等の非常時の対応

No	チェック項目	実施済	実施予定(実施時期)
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”と判断するための基準、手順、判断者等及び正常復帰時の手順を定めている。	■	□()
2.	非常時における対応に関する教育及び訓練を従業者に対して行っている。また、医療情報システムの障害時の対応についても同様に行っている。	■	□()
3.	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。	■	□()
4.	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。	■	□()
5.	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検知出来るよう、適切に管理及び監査を行っている。	■	□()
6.	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。	■	□()
7.	医療情報システムに不正ソフトウェアが混入した場合に備え、関係先への連絡手段や紙での運用等の代替手段を準備している。	■	□()
8.	重要なファイルは数世代バックアップを複数の方式で取得し、そ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手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備している。	■	□()
9.	サイバー攻撃で広範な地域での一部業務の停止等業務提供体制に支障が発生する場合は、所管官庁への連絡を行っている。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管省庁への連絡を行っている。	■	□()

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	実施予定(実施時期)
1.	ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策、施設間の経路上における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アドレス詐称等のなりすましを防止する対策を行っている。 ^{注1)}	■	□()
2.	データ送信元と送信先での、拠点の出入口ロ・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(認証)を行っている。 ^{注12)}	■	□()
3.	施設内において、正規利用者への成りすまし、許可機器への成りすましを防ぐ対策を行っている。	■	□()

No	チェック項目	実施済	実施予定(実施時期)
4.	ルータ等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。 ^{注13)}	■	□()
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等のセキュリティ対策を実施している。 ^{注14)}	■	□()
6.	電気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事業者等と、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。 <ul style="list-style-type: none"> 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 伝送情報の暗号化に不具合があった場合の対処 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 障害が起こった場合に障害部位を切り分ける責任 送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処 	■	□()
7.	医療機関内において次の事項において契約や運用管理規程等で定めている。 <ul style="list-style-type: none"> 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。 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及び事後責任の明確化。個人情報 ^{注15)} 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。	■	□()
8.	医療情報システムを内部ネットワークを通じて外部ネットワークに接続する際に、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定して、監視を行っている。	■	□()
9.	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。	■	□()
10.	電気通信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。	■	□()
11.	患者に情報を閲覧させる場合、内部システムに不正な侵入等が起こらないよう対策を実施している。 ^{注15)}	■	□()
12.	オープンなネットワークにおいて、IPsecによるVPN接続等を利用せずHTTPSを利用する場合、TLSのバージョンをTLS1.3のみに限定した上で、クライアント証明書を利用したTLSクライアント認証を実施している。(その際、TLSの設定はサーバ/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。) SSL-VPNを利用する場合は、具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、適切な手法の選択及び必要な対策を行っている。また、ソフトウェア型のIPsec又はTLS1.2以上により接続する場合、セッション間の回り込み(正規のルートではないクローズドセッションへのアクセス)等による攻撃への適切な対策を実施している。	■	□()

No	チェック項目	実施済	実施予定(実施時期)
13.	クローズドなネットワークで接続する場合でも、内部トラフィックにおける脅威の拡散等を防止するため、不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用している。	■	□()
14.	電子署名に用いる秘密鍵の管理は、認証局が定める「証明書ポリシー」(CP)等で定める鍵の管理の要件を満たして行っている。	■	□()

注 11: 例として IPSec と IKE を利用することによりセキュアな通信路を確保することがあげられる。

注 12: 採用する通信方式や運用管理規定により、採用する認証手段を決めること。また、認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用ワンタイムパスワード等の用意に解読されない方法を用いるのが望ましい。

注 13: 安全性が確認できる機器とは、例として、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が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 版に適合していることを確認できるものをいう。

注 14: 例として、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策があげられる。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すること。

注 15: 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 TLS 暗号化、PKI 個人認証等の技術を用いた対策を指す。