

運営についての重要事項に関する規程の概要[健診機関]

- * 健診と保健指導の両方を実施する者は、保健指導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法人の場合は、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	平成21年 12月 1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)}		高木内科クリニック	
	所在地 ^{注1)}	(郵便番号)	745 - 0801	
		(住所)	山口県周南市大字久米3198 - 6	
	電話番号 ^{注1)}		0834 - 25 - 2678	
	FAX番号		0834 - 25 - 2676	
	健診機関番号 ^{注3)}		3511510400	
	窓口となるメールアドレス		dtakaki@cotton.ocn.ne.jp	
	ホームページ ^{注4)}		http://	
	経営主体 ^{注1)}		医療法人社団 高木内科クリニック	
	開設者名 ^{注1)}		高木昭	
	管理者名 ^{注5)}		高木昭	
	第三者評価 ^{注6)}		実施（実施機関： ） 未実施	
	認定取得年月日 ^{注6)}		年 月 日	
	契約取りまとめ機関名 ^{注7)}		(例: 市医師会、結核予防会)	
所属組織名 ^{注8)}				

- 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。複数拠点を有する法人の場合は、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 店」「財団法人 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) 特定健康診査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、健康診査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（医師等による兼務は可）
- 注6) 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7) 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8) 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。

スタッフ 情報 ^{注9)}		常勤	非常勤
	医師		1人
看護師		3人	人
臨床検査技師		人	人
上記以外の健診スタッフ ^{注10)}		2人	人

- 注9) 特定健康診査に従事する者のみを記載。
- 注10) 医師・看護師・臨床検査技師以外で、特定健診の業務運営に必要な者（受付、身体計測、データ入力や発送、健診バスの運転等）

施設及び 設備情報	受診者に対するプライバシーの保護 ^{注11)}	有	無
	個人情報保護に関する規程類	有	無
	受動喫煙対策	敷地内禁煙	施設内禁煙

血液検査	独自で実施	委託（委託機関名：福山臨床）
内部精度管理 ^{注12)}	実施	未実施
外部精度管理 ^{注12)}	実施（実施機関：日本医師会）	未実施
健診結果の保存や提出における標準的な電子的様式の使用	有	無

注11) 健診時における、必要な箇所(問診・相談や脱衣を要する検査項目の実施時等)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

注12) 血液検査を外部に委託している場合には、委託先の状況について記載。

運営に関する情報	実施日及び	特定時期	(例: 6月第2週の平日 13:00-17:00)	
	実施時間 ^{注13)}	通年	平日 8:30 - 12:30	14:30 - 18:00
	特定健康診査の単価 ^{注14)}		円以下/人	
	特定健康診査の実施形態 ^{注13)}		施設型（要予約・予約不要）	巡回型（要予約・予約不要）
	巡回型健診の実施地域		(例: 岡山県全域 広島県福山市)	
	救急時の応急処置体制 ^{注15)}		有	無
	苦情に対する対応体制 ^{注16)}		有	無

注13) どちらだけでも、どちらも記載可

注14) 特定健康診査の「基本的な健診の項目」(いわゆる必須項目)の一式を実施した場合の単価(契約先によって多様な契約単価がある場合は、そのうちの最高額)を記載。なお、単価には消費税を含む。

注15) 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16) 受診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

その他	掲出時点の前年度における特定健診の実施件数 ^{注17)}	年間	人	1日当たり	人
	実施可能な特定健康診査の件数	年間	人	1日当たり	人
	特定保健指導の実施		有(動機付け支援)	有(積極的支援)	無

注17) 平成19年度・20年度の掲出については、事業主健診(労働安全衛生法)及び基本健康診査(老人保健法)の実施件数を記載(実績等のない機関については記載不要)。

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](案)

- * 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	年	月	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)}		
	所在地 ^{注1)}	(郵便番号)	-
		(住所)	
	電話番号 ^{注1)}		-
	FAX番号		-
	保健指導機関番号 ^{注3)}		
	窓口となるメールアドレス		@
	ホームページ ^{注4)}		http://
	経営主体 ^{注1)}		
	開設者名 ^{注1)}		
	管理者名 ^{注5)}		
	保健指導業務の統括者名 ^{注6)}		
	第三者評価 ^{注7)}		実施（実施機関： ） 未実施
	認定取得年月日 ^{注7)}		年 月 日
	契約取りまとめ機関名 ^{注8)}		(例 市医師会 結核予防会)
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 店」「財団法人 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)	全て自前で実施	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 (例:財団法人 埼玉支部)	委託部分	(例:埼玉県・運動指導)
		業者名 (例 株式会社九州ロ-ルセンター)	委託部分	(例:九州7県・電話)
		業者名	委託部分	(例:全国・電子メール)
		業者名	委託部分	(例:北海道・個別)
		業者名	委託部分	
		業者名	委託部分	
		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13)}
	総数	左記のうち一定の研修修了者数 ^{注13)}	総数	左記のうち一定の研修修了者数 ^{注13)}		
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	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 ^{注12)}	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	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) 医師、保健師、管理栄養士以外について記載。

注13) 一定の研修とは、「標準的な健診・保健指導プログラム(確定版)」にある「健診・保健指導の研修ガイドライン(確定版)」に定める研修をいう。

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う者	積極的支援における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	電話支援	電子メール支援 ^{注14)}
医師		常勤	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者
(上記のうち、日本医師会認定健康スポーツ医)		常勤	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者
保健師		常勤	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者
管理栄養士		常勤	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者
看護師(一定の保健指導の実務経験のある者)			常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者
専門的知識及び技術を有する者	THP取得者			常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者
	健康運動指導士			常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者	常勤 非常勤 協力業者

* 該当する項目を全て選ぶこと(複数選択可)

注14) 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15)}	有	無		
	個人情報保護に関する規程類	有	無		
	受動喫煙対策	敷地内禁煙	施設内禁煙	完全分煙	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	有	無		

注15) 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16)}	特定時期	(例: 6月第2週の平日 13:00-17:00)			
		通年	(例: 平日 9:00-17:00、土曜夜間)			
	実施地域 ^{注17)}	(例: 岡山県全域、広島県福山市)				
	実施サービス ^{注18)}	動機付け支援		積極的支援		
	実施形態 ^{注18)}	施設型		非施設型		
	継続的な支援の形態や内容 ^{注18)}	個別支援 電話支援	グループ支援 運動実習	電子メール支援 ^{注14)} 調理実習		
	標準介入期間(積極的支援) ^{注19)}	3ヶ月	4ヶ月	5ヶ月	6ヶ月	
	課金体系	完全従量制(従量単価×人数)		固定費 + 従量単価×人数		
	標準的な従量単価 ^{注20)}	動機付け	円以下/人	積極的	円以下/人	
	単価に含まれるもの ^{注18)・注21)}	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) 会場・施設費 交通費(指導者の) 材料費(調理実習) 通信費・事務費 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18)}	調査・計画費 特に無し	データ分析費	各種案内代行費		
	積極的支援の内容 ^{注22)}	(例: 合計240ポイントの継続支援を実施 特に、集団での栄養指導を実施)				
	救急時の応急処置体制 ^{注23)}	有	無			
	苦情に対する対応体制 ^{注24)}	有	無			
保健指導の実施者への定期的な研修	有	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25)}	有	無				

注16) どちらだけでも、どちらも記載可

注17) 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18) 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19) 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20) 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21) 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22) 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23) 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24) 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25) 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(「標準的な健診・保健指導プログラム(確定版)」第3編第6章(4)2)「保健指導の記録等の情報の取扱いに関する基準」の項目fを参照のこと)

その他	掲出時点の前年度の特定保健指導の実施件数 ^{注26)}	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
	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
	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26)}	動機付け	参加率	%	脱落率	%
		積極的	参加率	%	脱落率	%
	特定健康診査の実施		有		無	

注26) 平成19年度・20年度の掲出については、事業主健診の事後指導等類いの指導における実績値を記載(実績等のない機関については記載不要)。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

事業運営上開示すべき重要事項の概要[代行機関]

- * 代行機関の業務を行う者は、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）に掲載すること。
- * 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。
- * ガイドラインの遵守状況については別添指定様式に記載すること。

更新情報	最終更新日	年	月	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。

基本情報	機関名 ^{注1)}	
	所在地(住所) ^{注1)}	
	電話番号 ^{注1)}	- -
	FAX番号	- -
	ホームページアドレス	http://
	窓口となるメールアドレス	@
	代行機関コード ^{注2)}	
	代行機関の分類 ^{注3)}	医療保険者サイド 健診・保健指導機関サイド（健診機関グループ） 健診・保健指導機関サイド（健診機関グループ以外）

注1) 名称等は正式なもので記載する。

注2) 発行した代行機関コードを記載。

注3) いずれか一つを選択。「医療保険者サイド」とは、保険者の委託を受け、機関と保険者との間に入って第三者として代行処理をする代行機関の類型。「健診・保健指導機関サイド」とは健診機関とりまとめ機関（上記「健診機関グループ」）や福利厚生代行会社（上記「健診機関グループ以外」）等によりデータや決済をとりまとめる類型

施設及び設備情報	従事する職員の数 ^{注4)注5)}	専任	機関本体	人	協力・関係会社	人
		兼任	機関本体	人	協力・関係会社	人
	全職員の数 ^{注5)}		機関本体	人	協力・関係会社	人
	施設数(サポート拠点数)		箇所(都道府県名:)			
	財務基盤に関する資料または照会先 ^{注6)}					
	類似業務・サービスの提供実績 ^{注7)}		有(内容:) 無			
	提供するサービス	対象	保険者向け	健診・保健指導機関向け		
		内容	事務点検	請求・支払のとりまとめ・代行健診・保健指導データの受領・振分・送付 その他()		
	利用者によるサービスの選択	保険者	可(選択可能な機能:) 否			
		健診・保健指導機関	可(選択可能な機能:) 否			
ガイドラインの遵守 ^{注8)}		最低限のガイドラインを遵守済 最低限のガイドラインを遵守する予定 最低限のガイドラインを遵守していない				

注4) 当該機関のうち代行業務に従事する者のみを記載。

注5) 協力会社・関係会社等がない場合は記載不要(空欄)とし、あっても従事していない場合は0(ゼロ)人と記載。

注6) 貸借対照表等決算報告書の類をホームページで公開している場合はその URL 等を記載。財務情報を公開していない場合は照会先(連絡先及び担当者名等)を明記。

注7) 例として提供サービスの項を参照のこと。

注8) 別添指定様式「医療情報システムの安全管理に関するガイドライン 最低限のガイドライン遵守チェックリスト」に記載すること。チェックリストにおいて全項目「実施済」の場合は「最低限のガイドラインを遵守済」、1項目以上「実施予定」がある場合は「最低限のガイドラインを遵守する予定」を選ぶこと。

情報システムに関する情報	提供開始の年月日 ^{注9)}			
	システムの保有	自己導入	借用	
	システムの運用管理	自機関内	全部委託	一部委託
	システム専用区画・施設の有無	専用施設(機関所有) 機関建物内専用区画		専用施設(委託先) 特に無し
	システム管理技術者数	機関本体	人	委託先
処理可能件数(設計値)	年間	件	1日当たり	件

注9) 試用期間を除く。

運営に関する情報	サービス提供時間	拠点	(例:平日 9:00-17:00、除く 12/29-1/3)		
		システム	(例:24 時間 365 日稼働)		
		ヘルプデスク	(例:平日 9:00-17:00、除く 12/29-1/3)		
	データ授受の方法	外部から機関へ	オンライン(回線種別) オフライン(送付手段)		
		機関から外部へ	オンライン(回線種別) オフライン(送付手段)		
	データ授受におけるセキュリティ対策の方法	オンライン	(例:伝送相手の安全性を確保する SSL、IPSec と IKE の利用)		
オフライン		(例:盗難・紛失した場合に個人情報漏洩を防ぐためのファイル暗号化ツールの利用)			

事務手数料等 ^{注10)}			保険者	健診・保健指導機関
	初期費用		円	円
	経常経費	別途請求の有無	無(健診委託費に含まれる) 有(下記)	無(健診委託費に含まれる) 有(下記)
		固定費	円	円
		従量単価 ^{注11)}	円/あたり	円/あたり
代行機関利用に際し必要となる設備等 ^{注12)}				

注10) すべて消費税込みの金額を記載。委託機能によって費用が異なる場合はすべて記載。

注11) 単位あたり(例えばデータ1件あたり)の事務手数料を記載。取扱データの内容等によって単価が異なる場合はすべて記載。

注12) 保険者、健診・保健指導機関において必要となるハードウェア、ソフトウェア、ネットワーク回線等を記載。初期費用に含まれるものと、初期費用以外に各自の負担で導入しなければならないものを明記

その他	前年度の取扱件数 ^{注13)}	年間	件	1日当たり	件
-----	--------------------------	----	---	-------	---

注13) 平成21年度以降、前年度の実績を記載(当初は空欄)

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、平成19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2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。

* 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	年	月	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。 (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		()

物理的安全管理対策

No	チェック項目	実施済	実施予定(実施時期)
1.	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、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		()
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。		()
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。		()
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。		()
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。		()
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。		()

技術的安全管理対策

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。		()
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、漏洩等に十分留意している。 ^{注1)}		()
3.	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。		()
4.	アクセスの記録及び定期的なログを確認している。 ^{注2)}		()
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。 ^{注3)}		()

No	チェック項目	実施済	実施予定(実施時期)
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。		()
7.	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4)}		()
8.	利用者がパスワードを忘れて、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。		()
9.	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。 ^{注5)}		()

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: 代行機関の内部で利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: 利用者識別にICカード等其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5: 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。

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。		()
2.	定期的に従業者に対し教育訓練を行っている。		()
3.	従業者の退職後の個人情報保護規程を定めている。		()

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。		()
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、作業内容・作業結果の確認を行っている。		()
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。		()
4.	委託先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先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。		()

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6)}		()
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.	破棄を外部事業者に委託した場合は、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6: 手順は、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む必要がある。

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する等の処理を行うことを求めている。		()
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。		()
3.	保守要員個人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更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た、それに応じるアカウント管理体制を整えている。		()
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、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。		()
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。		()
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。		()
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、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認している。		()
9.	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。		()

災害等の非常時の対応

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”と判断する仕組み、正常復帰時の手順を設けている。 ^{注7)}		()
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。		()
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。		()
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。		()
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。		()
6.	サイバー攻撃で広範な地域での一部業務の停止など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。		()

注7:判断するための基準、手順、判断者、をあらかじめ決めていることを指す。

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、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。 ^{注8)}		()
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(認証)を行っている。		()
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とっている。		()

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。 ^{注9)}		()
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。 ^{注10)}		()
6.	<p>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。</p> <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.	<p>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。</p> <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結果責任の明確化。 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。 		()
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。		()
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。		()

注8: 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9: 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2版に適合していることを確認できるものをいう。

注10: 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など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していなければならない。