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	令和８年８月 19 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)]		加東市民病院
	所在地[注1)]	(郵便番号)	673－1451
		(住所)	兵庫県加東市家原 85 番地
	電話番号[注1)]		0795－42－5511
	FAX番号		0795－42－4740
	健診機関番号[注3)]		2812500722
	窓口となるメールアドレス		hosp-iji@city.kato.lg.jp
	ホームページ[注4)]		https://www.city.kato.lg.jp/hospital/
	経営主体[注1)]		加東市
	開設者名[注1)]		加東市長　岩根　正
	管理者名[注5)]		加東市病院事業管理者　金岡　保
	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	人
	看護師	1 人	人
	臨床検査技師	1 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　□完全分煙　□なし

	血液検査	■独自で実施　□委託（委託機関名：　　）
	眼底検査	■独自で実施　□委託（委託機関名：　　）
	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　臨床検査精度管理調査、日本臨床衛生検査技師会　日臨技臨床検査精度管理調査、兵庫県臨床検査技師会　臨床検査精度管理調査） □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）血液検査や眼底検査等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	実施日及び実施時間[注13)]	特定時期	(例: 6 月第 2 週の平日 13:00-17:00)
		通年	平日 8:30-12:00 (例:平日 9:00-17:00、土曜夜間)
	特定健康診査の単価[注14)]		8,405 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」であると想定される
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」であると想定される

その他	掲出時点の前年度における特定健診の実施件数	年間　51 人	1 日当たり　2 人
	実施可能な特定健康診査の件数	年間　100 人	1 日当たり　2 人
	特定保健指導の実施	□有(動機付け支援)　□有(積極的支援)　■無	

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	令和８年８月 19 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。	■	□(　　)
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	■	□(　　)

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 等の重要な機器にチェーン等の盗難防止対策を実施している。	■	□(　　)
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.	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。	■	□(　　)
4.	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)	■	□(　　)
5.	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。	■	□(　　)
6.	アクセスの記録及び定期的なログを確認している。注2)	■	□(　　)
7.	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。	■	□(　　)
8.	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)	■	□(　　)
9.	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)	■	□(　　)
10.	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。	■	□(　　)
11.	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)	■	□(　　)
12.	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。	■	□(　　)
13.	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)	■	□(　　)
14.	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。 ・ 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)	■	□(　　)
15.	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)	■	□(　　)
16.	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。	■	□(　　)
17.	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。	■	□(　　)
18.	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。	■	□(　　)
19.	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。	■	□(　　)

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:アクセスの記録はすく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なることを指す。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: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。	■	□( )
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。	■	□( )
3.	従業者の退職後の個人情報保護規程を定めている。	■	□( )

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者の特定、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。

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.	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。	■	□(　　)
5.	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。	■	□(　　)
6.	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11)]	■	□(　　)
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。[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。	■	□(　　)
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。 • 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	■	□(　　)

No	チェック項目	実施済	実施予定(実施時期)
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。 • 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.	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。	■	□(　　)
12.	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。