地域医療介護情報連携サービスの安全管理（運用編）評価項目

項番	分類	項目	項目概要（何のために、何を評価するのか）	評価内容
1	A:方針公表	サービス全体を把握し、提示できる資料があるか	地域医療連携組織を運用する「目的」「運用方針」「加入者・患者のメリット」などが示されているかを評価する。	サービス概要説明書相当があり、「目的」「運用方針」「加入者・患者のメリット」相当が記されていること。
2		個人情報保護方針を策定し公開しているか	取得した個人情報を地域連携サービスの中でどの様に取り扱うかについて、法などに沿った形で策定しているかを評価する。	個人情報保護方針を広く公開していること。 「個人情報保護法」だけでなく、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に沿っているかがポイントとなる。
3		患者データに対して、利用目的（診療・分析など）・取り扱い方法（第三者提供型または共同利用型、利用範囲・利用方法など）についてポリシーに沿って加入者の同意を取る仕組みがあるか	加入者、ケースによっては患者に対して目的、取り扱い方法を明示し、同意をとる為の体制、プロセスがなされているかを評価する。	同意取得文書のひな形相当があり、データ取得や利用に関する目的、取り扱い方法等の項目が適切に設定されていること。
4		患者データおよび分析情報を、加入者の同意や正式な手続きなく、第三者に提供をしていないか	同意なくデータの第三者提供をしていないことを評価する。	同意取得文書のひな形相当があり、加入者の同意外の第三者提供を行わないことおよび、提供範囲や目的が変更される際の同意の取得方法について明示されていること。
5	B:責任分界の明確化	どのようなシステムが稼働しているか、責任分界点を含め提示できる資料があるか	各システムの仕様が文書化され、サービス内で担当する機能が確認可能となっているかを評価する。	稼働する各システムの仕様書相当があり、システム概要、機能概要及び責任分界点が明確に記述され、参照可能となっていること。（事故時の責任分界の原則や対応策検討・調査・改善、等の記載がある）
6		情報・データの所在場所を把握できているか	加入者にとっては、提供したデータの所在場所を知る必要があり、データが法的保存義務があるならば、国内法適用箇所であることを評価する。 外部保管に該当するならば「経産省GL」に従っていることを評価する。	情報・データの所在場所説明書相当があり、左記要件が守られていること。 また、外部サービス提供事業者を利用する場合は、運用営主体側との間に契約書相当があり左記要件が確認可能となっていること。また、外部サービス提供事業者による主体的な情報の利用を禁止する契約条項があること。 可搬媒体へのデータの記録を許可する場合は、可搬媒体記録要領書相当があり、記録者・対象データ・媒体の管理状況等について管理することとしていること
7		端末の取り扱いなどの規定が整備されているか	データのアクセスに用いる端末の不正操作防止策をとっているかを評価する。	運用管理規程定相当があり、「端末の取り扱いや盗難・紛失時の対応」、「サービスにアクセス可能な端末について、非権限者の操作がされないよう、技術的・物理的対策がとられていること。」および「用いる端末はすべて登録制としていること。」について明文化されていること。
8		リスクの分析・評価・対応策・残留リスクの検討がされているか	システムにあるリスクについて、特に個人情報保護の観点を中心として検討され、その対応法について規定されているかを評価する。	リスク分析説明書相当があり、扱う情報をすべてリストアップし、重要度に応じて分類するとともにリスク分析をしていること。運用によりカバーすることを想定したリスクについては、その内容および運用方法及びその監査について規定していること。 情報のリストやリスク分析結果についてすべて文書化していること。 外部サービス提供事業者を用いる場合はシステムおよび運用形態について適宜見なおし、その改善について運用営主体とで検討する体制がつくられていること。
9		免責となる事項について明確化しているか	加入者、運用主体および外部サービス提供事業者についての責任範囲と免責事項が明確であるかを評価する。	免責事項説明項目相当があり、加入者、運用主体および外部サービス提供事業者の担う業務や責任分界点に適合する内容で、免責事項について明文化されていること。
10		事業者が免責となる事項と加入者への責務、患者同意取得内容で矛盾が生じていないか	加入者および委託業者の責務・免責事項が合理的かつ矛盾のないものとなっているかを評価する。	患者への説明同意書相当があり、加入者、運用主体および外部サービス提供事業者の責任範囲・免責事項が明記され、患者への同意内容と矛盾しないこと。(内容によっては掲示等による確認ができることでも可)
11	C:組織・運用管理規程	運用管理規程が適切に作成されているか	組織として、運用をどの様に実施するかについて明示的に示されているかを評価する。	運用管理規程が存在し、厚生労働省「医療情報システムの安全管理に関するガイドライン 第4.2版」に沿った適切な項目設定がされていること。また、意思決定プロセスが明確化されていること。
12		組織体制が作成され明確になっているか	何かあった場合の責任体制、受付窓口などが明確化されていることを評価する。	組織体制図が作成されており、公開されている、もしくは求めに応じて公開できること。対外的な説明責任が発生した場合の対応体制等が明確化されていること。
13		アクセスポリシーが有り適切なアクセス管理がなされているか	情報へのアクセスを適切に行う為にアクセスポリシーがありそれに沿って管理されていることを評価する。	アクセスポリシー説明書、アクセス制御を行うための設定書、取扱説明書等相当があり、それぞれが安全管理のガイドラインに沿った形で、職種に応じたアクセス制御が明示されていること。
14		運用に対する教育がなされているか	組織で関わる者に運用の教育が行っているかについて評価する。	関係者を教育するための資料相当があり、運用管理規程を基として作成されていること。

項番	分類	項目	項目概要（何のために、何を評価するのか）	評価内容
15		委託管理契約が明確に交わされているか	運用に組織外の人間が含まれている場合に、明確に委託契約を結んだ者であることを示せるか評価する。	委託管理契約のひな形相当があり、通常運用の責任、事後責任について記載してあり、適切な項目を有していること。
16		秘密保持契約が適切に交わされているか	運用に携わる者に対して、守秘義務を課すために秘密保持契約を結んでいるか評価する。	秘密保持契約のひな形が存在し、対象情報、対象範囲等、適切な項目を有していること。
17		データの管理に対して規定が作成されているか(持ち出し等含む)	データを適切に取り扱うための規定があり、管理体制、プロセスが適切になされているか評価する。	データ管理のマニュアル相当があり、データ取り扱い時の管理体制、プロセス等が適切に定められていること。
18		加入者が組織から退会するときの規定の存在	加入者から提供されたデータの処分方法などの規定の存在を評価する。	加入者の退会規定があり、加入者から提供されたデータの処分方法などの規定が存在していること。
19		加入者への運用情報（会計、システム構成、事故等）の開示	組織の透明性のため、運用状況を加入者に適宜知らせているかを評価する。	運用状況報告書相当を定期的に発行し、公開または加入者の求めに応じて開示する規定があること。
20		加入者へのサービスレベルの開示	システムの対応内容の加入者への開示がなされているかを評価する。(開示内容例) 稼働時間帯、問い合わせ対応、データ保管責任内容、等。	SLA(service level agreement)が通知または説明書として存在し、内容が妥当であること。
21	D:システム	システムについて各省のガイドライン(※)に準拠していることを確認しているか	システムの安全管理の為にガイドライン準拠を確認しているかを評価する。	システムの安全管理の為にガイドライン準拠性確認書があり、「サービス提供事業者を利用するならば、カタログ等での準拠性確認」または「自開発、あるいはガイドライン準拠を標榜していないサービスを用いる場合は、その部分のチェックリスト提出等による準拠性確認」がなされていること。
22	E:モニタリング・監査	アクセスログを取得し、定期的に監査を行っているか	データアクセスが”業務とアクセス権限設定”に沿って妥当であることの確認を取っていることを評価する。（＊ドメイン外からのアクセスも含む。）	アクセスログ規定があり、監査証跡の取得方法、保存期間の規定と保管・管理、証跡に基づく監査が規定されていること。
23		定期的にシステムの見直しを実施し、改善点について対策が取られているか	システムの運用・動作が正常であることの確認や、改善点の確認と改善活動の規定の存在しているかを評価する。	システムの見直し規定があり、運用規約、監査規約の存在、定期的見直しの実施規定、問題点の加入者との共有体制が規定されていること。
24	F:事業継続性	BCPについて適切に規定され対策が準備されているか	災害等の事故が発生してもサービスが継続して実施される為の準備がされている事を確認していることを評価する。	BCP規定があり、災害時等事故発生時加入者の対応を含め適切な対策が規定されていること。
25		加入者との情報交換のインターフェースおよびデータフォーマットは標準的なものあるいは公開可能なものを使用しているか。	機種やメーカが変更されてもサービスが継続できる為に機器間のインターフェースがデータが相互運用性があることを確認していることを評価する。	インターフェースおよびフォーマット仕様書相当があり、加入者とのインタフェースおよびデータフォーマットの標準化対応あるいは公開可能であることを規定していること。
26		サービス契約終了時の、データ移行等データの取り扱いに対する規定が作成されているか	サービス契約が終了した場合安全に他のサービス運用主体に引き継げる為にデータの取扱いが決めているか確認していることを評価する。	サービス契約終了時の、データ移行等データの取扱いに関する適切な規程があること。
27	G: 加入者に対する運用主体の責務（加入者の実施義務の明確化） ＊「加入者」には「加入希望者」を含む	加入者が負うべき責務およびリスクについて明確にしてあるか	加入者が自己の責任範囲を知るための事項を示していることを評価する。	ポリシー合意、主要契約書内容の提示文書相当があり、加入条件・資格、負担資金、責任分界、組織体制、連携組織発行文書への知財権、加入者のデータ利用権、有効・更新期限、退会時の規定、等が明記されていること。
28		加入者が整備すべきシステム機能＆環境について明確にしてあるか	地域連携システムに接続した目的を果たすための加入者側システム要件の明示していることを評価する。	加入者に要求されるシステム条件説明書相当があり、プラットフォーム、セキュリティ機能、パフォーマンス、レポジトリ機能の実装など必須事項等が明記されていること。 （端末毎の利用・操作記録（ログ）の記録、加入者による端末設定変更やアプリケーションのインストール禁止、モバイル端末内に許可外のデータを保存しない等も含む）
29		加入者が実施すべき職種別アクセス管理について明確にしてあるか	システム全体がセキュアであるために、加入者において必要なアクセス制御（職種とアクセス権限）を示していることを評価する。	加入者に対する職種別アクセス制御説明書があり、システムに対する実施事項、人的管理事項が明記されていること。
30		加入者が作成すべき運用管理規程の内容が明確にされているか	システム全体が安全に動作するために、加入者の守るべき規定を示していることを評価する。	加入者が運用管理規程を作るための説明書相当があること。
31		加入者における従業員への教育が適切に実施されるように教育内容を提供しているか	システム全体が支障なく動作するために、加入者での従事者の守るべき規定を示していることを評価する。	加入者の従事者へ要求する教育内容の提示書があり、適切な内容であること。

項番	分類	項目	項目概要（何のために、何を評価するのか）	評価内容
32		加入者による、患者への同意の取り方について、明確に指定がされているか	加入者に対して同意取得の方法を明示しているかを評価する。（患者自身の責任についても必要な記載が求められる。）	「患者への同意の取り方について」相当の文書があり、 加入者への周知文書あるいは雛形文書が提示され必要事項が明示されていること。

※各省のガイドラインとは、下記のガイドラインのことを指す。
・厚生労働省「医療情報システムの安全管理に関するガイドライン 第4.2版」
・総務省「ASP・SaaSにおける情報セキュリティ対策ガイドライン」
・総務省「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン第1.1版」
・経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」
・経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン第2版」