平成 25～26 年度地域医療連携の普及に向けた

健康情報活用基盤実証事業

セキュリティポリシー

Ver.1.2

平成 26 年　8 月 22 日

公益社団法人　石川県医師会

目次

1. 総則

1.1 目的

本セキュリティポリシーは、「平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業」（以下「本事業」という。）のシステム（以下「本システム」という。）において、実証を行うにあたり、事業運営主体である石川県医師会がシステムの運用と管理の安全に係わる基本事項を規定し、本システムの安全かつ適正な管理を図ることを目的として定めるものとする。

1.2 適用範囲

本セキュリティポリシーは、本システムの運用と管理に係る事項に適用する。

2. 管理体制

2.1 責任者の選任と管理体制

（1）事業管理者

公益社団法人　石川県医師会長をこれに充てる。

事業管理者は、実証事業の円滑な推進を目的とし、本事業の統括・管理を行う。

（2）事業実施責任者の設置

事業管理者が選任する者を、事業実施責任者に充てる。

事業実施責任者は、正副の任命を妨げない。

事業実施責任者は、本事業の運営が円滑に執り行われるよう各種調整業務を行う。

事業実施責任者は、参加機関の登録に関する事務取扱を実施し、登録状況について事業管理者に報告する。

（3）運用管理責任者の設置

事業実施責任者が選任する者を、運用管理責任者に充てる。

運用管理責任者は、正副の任命を妨げない。

本事業では、能登北部地域・中部地域の 2 地域で事業を推進するため、事業の円滑な推進を目的として、各地域にそれぞれ本システムの運用管理業務に責任を持つ、運用管理責任者を置く。

（4）システム管理者の設置

運用管理責任者は、本システムの安全かつ円滑な運用の実施責任をもつシステム管理者を任命するものとする。

システム管理者は、正副もしくは複数の任命を妨げない。

（5）その他の責任者の設置

運用管理責任者は、本システムの安全かつ円滑な運用の実施を行う、その他の責任者を任命するものとする。

その他の責任者は、各々正副もしくは複数の任命を妨げない。

責任分担の詳細については、運用管理規程にて別途定める。

2．2　サポートセンターの設置

(1) 運用管理責任者は、個人情報の取り扱いおよび本システムの運営等に関して、利用者等からの相談、苦情を受け付け、適切かつ迅速な対応を行うためサポートセンターを設置し、運営するものとする。

(2) サポートセンターは、以下のサポート業務を行うものとする。

① 以下の問い合せへの対応
- ・本システムの利用に関する事項
- ・本システムの内容に関する事項
- ・本システムの利用者登録、変更、解消に関する事項
- ・本システムの障害に関する事項
- ・本システムの操作に関する事項
- ・個人情報の保護、取扱いに関する事項

②以下の実施
- ・本システムの利用者登録、変更、解消
- ・利用者向け個人情報の保護、安全管理に関する教育
- ・利用者向けシステム利用に関する教育

(3) サポートセンターの問い合わせ対応日時は、以下のとおりとする。

9:00～17:00 （除く 土日、祝日および年末年始、その他休業日）

(4) サポートセンターの場所等

	能登北部地域	能登中部地域
相談窓口	電算輪島事務所内サポートセンター	恵寿総合病院内サポートセンター
住所	石川県輪島市河井町 24-11　輪島産業会館 3F	石川県七尾市富岡町 94 番地
電話番号	0768-22-5010	0767-52-2300
FAX	0768-22-5015	0767-52-1270
メール	support@notohoku.net	supportcenter@keiju.co.jp

2．3　災害・事故対策体制

運用管理責任者は、緊急時および災害時の連絡、復旧体制等を定め、文書化し、運用管理に携わる関係者に周知をするものとする。

2．4　教育・訓練

(1) 運用管理責任者は、本システムの取り扱いについてマニュアルを整備し、運用管理に携わる関係者に周知を行うものとする。

(2) 運用管理責任者は、本システムの運用に携わる関係者に個人情報の保護に関する教育を行うものとする。

(3) 運用管理責任者は、本システムを利用する病院、診療所、歯科診療所、薬局（以下これらを「医療機関等」という。）の責任者がその所属員に行う個人情報保護および安全管理に関する教育に関し、協力の依頼があった場合はこれに協力するものとする。

2．5　運用管理規程などの整備

運用管理責任者は、本システムに係わる各地域における運用について運用管理規程などを整備し、安全かつ円滑な運用を図るものとする。

事業全体に係わる運用管理規程などについては、別途定めるものとする。

3．本システムの安全管理事項

3．1　データセンターの設備環境

本システムの主要な機器であるサーバ等を設置するデータセンター要件は下記を満たすものとする。

(1) 1981年の建築基準法に規定する構造耐力等の基準に適合しており、高い耐震性を有していること。
(2) 浸水・漏水対策が施されていること。
(3) 2系統以上の安定した電源供給設備を有し、冗長化された自家発電設備、非常用電源設備（UPS）を備えていること。
(4) 冗長化された空調設備を有すること。
(5) 建築基準法に規定する防火区画であり、消防法施行令に規定した自動火災報知器および消火器を有していること。
(6) 本システムの構成機器はセンター内のセキュリティ区画に設置すること。
(7) セキュリティ区画は、常に施錠され、事務室等から隔離されていること。
(8) セキュリティ区画は、作業者を監視可能な監視カメラを備え、録画できること。
(9) サーバ等の情報機器は、ラックの施錠等により許可された者以外はアクセスできない構造であること。

3．2　データセンターの入退管理

(1) データセンターへの入退室は事前に入退室者登録を行い、許可された者のみができるものとする。
(2) 入退室が許可されていない外部の者は、システム管理者の許可があり、入退室が許可されたセンタースタッフの同行時のみ許可されるものとする。
(3) センターへの入退者は、入館許可書を着用し、入退の記録を残すこととする。
(4) 本システムの構成機器は、データセンター内のセキュリティ区画内に設置されるものとする。

3．3　データセンター設備の保守点検

保守点検のため、本システムの利用に影響が生じる場合は、予め日程と時間を本システムの利用者に伝えるものとする。

3．4　データセンターシステムの運用監視

(1) 安全かつ正常な稼働を確保するため、本システムの運転状態を常に監視する対策を実施し、異常なシステムの動作、不適切なシステムへのアクセス等の検知に努めるものとする。
(2) システムの稼働監視は、死活監視、システムアプリケーション応答監視を行うものとする。
(3) ファイアーウォール等のアクセスログの定期的チェックを行うものとする。

３．５ ネットワークの管理

(1) システム管理者は、安全かつ正常な稼働を確保するため、ネットワークの稼働状態を常に監視する対策を実施し、異常な動作、不適切なシステムへのアクセス等の検知に努めるものとする。
(2) システム管理者は、定期的にログの収集を行い、ログを保管するものとする。
(3) 利用するネットワークは、以下のものとする。
医療機関等においては、閉域網（IP-VPN）または、IPSec+IKE方式のVPNネットワーク
患者またはその代理者（以下「患者等」という。）の利用においては、SSL暗号化通信

３．６ 医療機関等の利用者と患者等のアクセス管理

(1) 本システムへアクセスする場合は、診察で使用している端末を用いることとする。医療機関等のポリシーにより、診察で使用する端末とは別の端末を用いることも可とする。
(2) HPKI 認証局が発行した医師、歯科医師（※）、薬剤師、看護師（※）、管理栄養士（※）用のHPKIカードを利用し、HPKI鍵用パスワードによるアクセス管理に加えて、医師、歯科医師、薬剤師を識別するアクセス管理を行うものとする。
（※）歯科医師用、看護師用、管理栄養士用 HPKI カードは現在発行されていないため、日本医師会認証局にてテスト用 HPKI カードの発行を行う。テスト用カードであっても、発行に係わる本人確認、免許証等による有資格者であることの確認は、日本医師会医師資格証審査に準じて行うものとする。
(3) 医師・歯科医師・薬剤師・看護師・管理栄養士以外の医療従事者が本システムへアクセスする場合は、PKI カードを用いることとする（PKI カードを用いて本システムへアクセスする者を、以下「補助作業者」という。）。PKI カードには、医療機関（組織）を示す証明書を格納し、補助作業者が当該医療機関の従事者であることを確認するものとする。どの従事者が本システムへアクセスしたかについては、医療機関内で適切に管理する。（例えばアクセスに使用した PKI カードとカードを使用した従事者名を台帳等で管理する。）
(4) 補助作業者による入力補助を行う場合は、医師の指示の下に実施すること。入力補助を許可された者であることをシステム上で識別可能とするため、補助作業者は、入力補助を指示する医師と関連付けをした PKI カードを用いることとする。補助作業者を特定できるよう、医療機関内で適切に管理することを前提とする。補助作業者による入力行為の後、医師による確定操作によって、情報がデータセンターに登録されるものとする。
(5) 本事業で構築するシステムの一部である、電子版疾病管理手帳システムの利用について、患者の情報を医療従事者が参照したり、情報を登録したりする（補助作業者による入力を含む）際は、原則として、患者と医療従事者が対面している際に限ることとする。ただし、補助作業者による入力の確定操作前の修正等についてはその限りではない。
(6) 患者等は、ID/パスワードを利用し、予め本システムへの参加同意を行うことでサポートセンターから患者等宛に ID と初期パスワードを通知し、患者等は自身で初期パスワードを利用パスワードに変えて本システムの利用を開始するものとする。

3．7　保守・運用者の電子記録媒体の管理

(1) システム管理者の許可を得た場合を除き、CD，USBメモリ、磁気テープ等（以下「可搬型記録媒体」）という。）への個人情報の複写を禁止するものとする。
(2) 可搬型記録媒体を利用する場合は、事前に利用方法を明確化した上で、システム管理者の許可を得ることとし、確認した方法以外での利用を禁止するものとする。
(3) システム管理者から許可を得た場合において、個人情報が格納された可搬型記録媒体は、施錠付キャビネット等に保管し、システム管理者は、台帳に記録し、管理するものとする。

3．8　保守・運用者の情報の廃棄

(1) 紙媒体の廃棄は、原則シュレッダーによる粉砕処理によるものとする。
大量廃棄する場合は、溶融廃棄証明書を受領することで、外部業者に委託することができるものとする。
(2) 電子媒体の廃棄は、原則粉砕処理によるものとする。
(3) 粉砕処理をしないPC等は、データの再生ができない方法で消去するものとする。なお、消去証明書を受領することで、データの消去処理を外部業者に委託することができるものとする。
(4) 事業管理者が指定した重要な情報を廃棄する場合は、廃棄の結果の報告受け、運用管理責任者が確認するものとする。

3．9　データのバックアップ

(1) サーバのシステムファイルおよびデータのバックアップを自動または手動で実施するものとする。
(2) バックアップの作業に当たる者は、その作業の記録を残すものとする。

4．情報の取り扱いおよび利用範囲

4．1　本システムでの情報の取り扱い

(1) 本システムが保存する情報は、複製情報として取り扱うものとし、情報の原本は情報を作成した病院、診療所、歯科診療所、薬局が法令に従い別途管理するものとする。
(2) 本システムが取り扱う複製情報の内容は、事業管理者、事業実施責任者、医療機関等において、その完全性、正確性、適用性、有用性等のいかなる面からの保証をするものではないものとする。

4．2　本システムにおける情報の利用範囲

本実証システムで収集した情報は、将来計画される同様システムの検討、将来の事業のためおよび厚生労働省への実証事業結果の報告書に使うことができるものとする。
ただし、個人が識別できる情報を報告または公表することはないものとする。

5．業務委託の安全管理

5．1　委託契約における安全管理

業務を外部に委託する場合は、委託契約書に以下の措置を実施するものとする。

① 委託契約書には、守秘事項を含むものとし、契約先の契約署名者は代表者とするものとする。
② 委託契約書には、再委託先に関する事項を加えるものとする。
③ 委託契約書の付帯条件として、サービス提供にあたって保障する品質と、事故・障害等が発生した際の補償について明確にするものとする。

5．2　再委託の安全管理

委託先が委託業務を外部に再委託する場合は、本ポリシーと同等の個人情報保護、安全管理に関する対策および契約がなされるものとする。

6．セキュリティポリシーの公開

本セキュリティポリシーは、本事業に参加する医療機関等および医療機関等の利用者、患者等及び本システムの運営と構築等に係わる団体、法人等とその関係者に公開するものとする。

7．セキュリティポリシーの見直し

事業管理者は、システムの機能、運用状況等に問題がある場合には、必要な是正の実施および予防の実施を行うため、事前の了解なく本セキュリティポリシーを見直しすることができるものとする。

8．セキュリティポリシーの施行日

本セキュリティポリシーは、平成26 年　8 月　1 日より施行する。

以上