能登北部医療圏地域医療連携システム

セキュリティポリシー

Ver.1.0

平成 24 年 8 月 23 日

石川県医師会

能登北部医師会

株式会社電算

目次

1. 総則

1.1 目的

本セキュリティポリシーは、石川県医師会・能登北部医師会（以下、「当会」という。）が「シームレスな健康情報活用基盤実証事業」（以下、「本事業」という。）において、情報連携（共有）システム及びどこでもＭＹ病院システムで構成される「能登北部医療圏地域医療連携システム」（以下、「本システム」という。）の実証又は試行を行うにあたり、システムの運用と管理の安全に関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

石川県医師会会長及び能登北部医師会会長をこれに充てる。

（2）事業実施責任者

株式会社電算　代表取締役社長が選任する本システムの運用管理責任者をこれに充てる。

（3）運用管理責任者の設置

事業実施責任者は、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設置するものとする。

（4）運用管理責任者は、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。

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及び実証システムに関して、利用者からの相談、苦情を受け付けて、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、以下の利用者向けのサポート業務を行うものとする。

① システムの利用に関する問い合せへの対応
② システムの内容に関する問い合せへの対応
③ システムへの利用者登録、変更、解消に関する問い合せへの対応
④ システムの障害に関する問い合せへの対応
⑤ システムの操作に関する問い合せへの対応
⑥ 個人情報の保護に関する利用者向け教育の支援

（3）サポートセンターの利用者向けサポート日と時間は、以下のとおりとする。

月曜日～金曜日の9:00～17:00 （除く 祭日及び年末年始）

（4）サポートセンターの場所等

名称：株式会社電算　輪島事務所内サポートセンター
住所：〒928-0001　石川県輪島市河井町24部11番地
合同会社　輪島産業会館3F
電話：0768－22－5010
FAX：0768－22－5015
メール：support@notohoku.net

2．3　災害・事故対策体制

運用管理責任者は、緊急時及び災害時の連絡、復旧体制等を定め、文書化し、運用管理に関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、システムの取り扱いについてマニュアルを整備し、運用管理に関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関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、病院、診療所、薬局の責任者がその所属員に行う個人情報保護に関する教育に関し、協力の依頼があった場合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、システムに係る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。

3．センター設備及び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及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を生じる場合は、予め日程と時間を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するため、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、生死監視、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のアクセル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) システム権利者は、定期的にログの収集を行い、ログを保管すること。
(3) 利用するネットワークは、
医療機関、薬局においては、IPSec+IKE方式のVPNネットワーク
本人（患者等）においては、SSL暗号化通信を利用する。

3．6 利用者のアクセス管理

(1) 日医認証局又は日薬認証局が発行した医師又は薬剤師用のHPKI カードを利用し、PKI鍵用パスワードによるアクセス管理に加えて、医師、薬剤師資格を識別するアクセス管理を行うものとする。
(2) 医療機関等の医師、薬剤師を除く従事者は、PKIカードを利用し、予め所属する医療機関、薬局の責任者（組織）が所在確認、本人確認を行った上でカードの発行を申請し、施設内従事者にカード配布する。ICカードに格納されたPKI鍵とパスワードによるアクセス管理を行うものとする。
(3) 医療機関等の施設認証を、IPSec+IKE ネットワークの PKI 鍵を利用して行う。ネットワークの利用申込において、保険医療機関又は保険薬局の存在性を確認の上で PKI 鍵を格納した機器を院内または薬局内に設置し使用するものとする。

（4）患者またはその代理者がアクセスするどこでもMY病院システムは、ID+パスワード+マトリクス認証方式とするものとする。

３．７　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メモリ等の記録への個人情報の複写を禁止するものとする。

（2）許可を得た場合において、個人情報が格納された電子記録媒体（CD、USB メモリ、磁気テープ等）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　情報の廃棄

（1）紙媒体の廃棄は、シュレッダーによる粉砕処理するものとする。
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、原則粉砕処理とするものとする。

（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）重要な情報を廃棄する場合は、管理者が立ち会いの上、廃棄・消去作業を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及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．情報の取り扱い及び利用範囲

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、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、病院、診療所、薬局、事業実施責任者において、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、将来の事業のため及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することも公表されることもないものとする。

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。

５．２　再委託の安全管理

業務を外部に再委託を行う場合は、本ポリシーと同等の個人情報保護に関する対策及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、本事業に参加する病院、診療所、薬局およびその利用者、患者又はその代理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

当会は、本セキュリティポリシーを、システムの利用者等からの苦情、緊急事態の発生、運営委員会、その他からの指摘等で、システムの機能、運用状況等に問題がある場合には、必要な是正の実施及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すことがある。

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24年　8 月　23 日より施行する。

以上