能登北部医療圏地域医療連携システム

運用管理規定

Ver.1.1

平成 24 年 10 月　10 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

「シームレスな健康情報活用基盤実証事業」(以下、「実証事業」という。)において「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。)に関する事業管理者である石川県医師会・能登北部医師会、事業実施責任者である株式会社電算は、実証に係るシステムの運用と管理に関わる事項を規定し、本システムの安全かつ合理的な運用と適正な管理を図ることを目的とする。

1.2 適用範囲

本運用管理規程は、本システムの運営と管理に係る事項に適用する。

1.3 事業管理者及び事業実施責任者の責務

(1)　事業管理者の責務

事業管理者は、本規程の遵守及び事業実施責任者に対する本規程の遵守を管理する責務を負うものとする。

(2)　事業実施責任者の責務

事業実施責任者(以下、「(株)電算」という。)は、本規程の遵守及び事業管理者への適切な報告を行う責務を負うものとする。

1.4 保護対象情報と利用目的・利用範囲

本システムで取り扱う個人情報保護対象となる情報、利用目的と利用の範囲を、以下の表に示す。

別表1 「保護対象情報と利用目的・利用範囲」

別表2 「取扱個人情報と取扱者」

1.5 対象とするシステムと業務

(1)対象システム

① 本システムを構成する機器、ソフトウェア等及びネットワークサービス

② 本システムを設置するデータセンター

③ リモート保守及び運用監視システム

④ サポートセンターシステム

⑤ 本システムにおける各種サービス

a) HPKI 認証局から発行される HPKI カードの利用に関する事項

b) PKI 認証局から発行される PKI カードの申請受付と利用に関する事項

c) タイムスタンプサービスの利用に関する事項

d) 患者またはその代理者(以下、「本人(患者等)」という。)に提供される会員カードの発行と利用に関する事項

(2)対象としないシステム

① 医療機関及び薬局(以下、「医療機関等」という。)が準備するインターネット及びシステム

② HPKI 認証局のシステム
③ PKI 認証局のシステム
④ タイムスタンプサービスのシステム
⑤ 医療認証サービスのシステム
⑥ 本人（患者等）が準備する、インターネットサービス
⑦ 本人（患者等）が準備する PC、携帯端末機等

(3)対象とする業務
① 医療機関等からサポートセンターに提出される、利用の申請・撤回等に関わる申請書受理業務、受理後に行うシステムへの利用登録、変更登録、データの削除等の業務
② 本人（患者等）からサポートセンターに提出される申請・撤回等の申請書受理業務、受理後に行うシステムへの利用登録、変更登録、撤回登録等の業務
③ サポートセンター業務
④ その他　関連する業務

（4）対象としない業務
① 本システムに登録する患者情報、診療情報、調剤情報等の作成業務
② どこでも MY 病院における、本人（患者等）が自身の PC,携帯端末等に保存した情報の取り扱い業務

1．6 ガイドライン及び標準規格等参照文書

本システムは、以下の文書に準拠または参照する。

別紙1:「ガイドライン及び標準規格等参照文書一覧表」

2.（株）電算の管理体制と管理者の責務

2.１ 責任者の選任と管理体制

（1） 運用管理責任者の設置

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。

運用管理責任者は、その業務を補佐する副運用管理責任者を置くことができる。

（2） システム管理者の任命

運用管理責任者は、その配下に、システムの管理を行うシステム管理者を任命する。

システム管理者は、その業務を補佐する副システム管理者を置くことができる。

（3） 各部門責任者の任命

システム管理者は、その配下にサポートセンター責任者を置く。

システム管理者は、その配下にリモート保守責任者を置く。

システム管理者は、その配下に相談・苦情受付窓口を担当する責任者を置く。

（4） 責任者の兼任

副運用管理責任者、システム管理者、副システム管理者、サポーセンター責任者、リモート保守責任者、相談・苦情受付担当責任者の兼任は妨げないものとする。

（5） 運用管理体制図の制定

運用管理責任者は、運用管理体制図を作成し制定する。

別紙2:「運用管理体制図」

2.２ 運用管理責任者の責務

（1） システムが円滑に運用される環境を整備し、その実施を管理する責任を持つ。

（2） 運用管理責任者の職務の一部を、副運用管理責任者、システム管理者に委任することは妨げない。

（3） システム管理者の報告を受け、必要な措置を講じる。

（4） 契約書類、マニュアル等を整備し、従業員に周知し利用可能な状態に置く。

（5） 必要な教育を実施する。

（6） 運用管理責任者は、次の事項を含む運用状況記録を作成し、保管するものとする。

- ・システムの障害記録とその是正処置
- ・システムの設定変更内容
- ・ログの保存記録
- ・バックアップの実施記録
- ・保守、セキュリティ対策の実施情報
- ・その他　必要なもの

（7） 運用管理責任者は、定期的に運用状況の記録を確認し、不適切な事項、対処を要する事項等が発見された場合、必要な是正をシステム管理者に指示する。

（8） 運用管理責任者は、重大な是正を要する事項が発見された場合、事業管理者に報告し、是正措置、対処の協議を行う。

2．3 システム管理者の責務

（1） 本システムの運用が支障なく行われるよう、実施の責任を持つ。
（2） システムの安全性を確保し、安全性の継続的な確保に努める。
（3） システムの開発者、保守作業者の登録を管理し、そのアクセス権限を管理し、不正な利用を防止する。
（4） 医療機関等の利用者及び本人（患者等）の利用者の登録を管理し、そのアクセス権限を管理し、不正な利用を防止する。
（4） システムの障害、バグ等の発生を運用管理責任者に報告すると共に障害の解決を行う。
（5） 作業手順の整備を行い従業員の教育と訓練を行う。
（6） サポートセンター業務、リモート保守業務、相談・苦情受付窓口業務、教育担当業務の管理を行う。
（7） 障害の発生を防止すること及び障害発生時には、運用管理責任者に報告すると共に、問題の解決を行う。
（8） 運用管理責任者に、システムの運用状況を報告する。
（9） 本システムに関わる従業員に対し、個人情報保護に関する教育を実施する。

2．4 運用管理規程の制定と報告

運用管理責任者は、運用管理規程の制定及び改訂に際し、事業管理者に報告するものとする。

3. 一般管理事項

3.1 文書管理体制

（1）運用管理責任者は、各種規定、様式、記録、契約文書、マニュアル等の文書の管理を行い、最新の状態を保つ。

（2）外部との個人情報の交換を行う場合、医療機関等、本人（患者等）、通信事業者、委託先事業者などとの間で、責任分解点や責任の所在を契約書で明確にする。

3.2 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、復旧体制等を予め文書化し、従業員に周知を行う。

別紙3:「緊急時、障害、災害時等の対応規定」

3.3 サポートセンターの設置

運用管理責任者は、サポートセンターを設置する。

3.4 教育・訓練

（1）システム管理者は、本システムに関わる従業員、委託先事業者に対し、システムの取り扱い及び個人情報保護に関する教育を行う。

（2）医療機関等から個人情報保護に関する教育の実施に関し、協力の依頼を受けた場合、これに協力する。

3.5 保守作業と報告の確認

（1）保守作業等の外注

システムの改造及び保守作業において、作業管理・監督、作業報告確認のため、システム管理者は、保守会社における保守作業に関し、以下のような確認を実施する。

作業者・作業内容・作業結果の確認

① 保守契約における個人情報保護の徹底

② 責任分界点、責任の所在等の契約書の確認

（2）従業員による保守作業

システムの改造及び保守作業おける作業管理・監督、作業報告確認のため、システム管理者は、保守作業に関し、以下のような確認を実施する。

① 作業者・作業内容・作業結果の確認

② 保守契約における個人情報保護の徹底

（3）従業員によるリモート保守を行う場合

システムの改造及び保守作業における作業管理・監督、作業報告確認のため、システム管理者は、社外からのリモート保守作業に関し、以下のような確認を実施する。

① 適切なアクセス権限管理と保守要員用の PKI カードの使用

② 安全なネットワーク（IPSec+IKE）の利用

③　作業者・作業内容・作業結果の確認
④　保守作業が安全に行われたかについてログによる確認

(4) 外部の保守会社からリモート保守を受ける場合の安全管理事項
前(3)項に加え、以下の項目の確認を行う。
① 外部の保守会社、通信事業者、運用委託業者等との間で、責任分界点や責任の所在が契約書等で明確にされていること。
② 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する。
③ 保守作業が安全に行われたかについてログによる確認
④ 上記契約状態が適切に維持管理されているか定期的に確認する。

別表3 「システム運用者のアクセス許可要件」

3.6 情報記録媒体の管理

(1) システム管理者が特に許可した場合を除き、CD, USBメモリ等への個人情報の複写を禁止する。
(2) システム管理者が許可した場合で、個人情報を記録した CD,USB メモリ等の媒体は、施錠できるキャビネットに保管し、記録に残し管理する。
(3) システム管理者が許可した場合で、個人情報を記録媒体で授受する場合は、暗号化をしたうえで行うこと及び記録に残し管理する。

3.7 紙情報及び情報記録媒体の廃棄

(1) システム管理者は、個人情報を格納した媒体(紙媒体、CD, USBメモリ等媒体、情報機器を含む)の廃棄が、安全かつ確実に行われるよう管理を行う。
(2) 紙媒体の廃棄は、シュレッダーによる粉砕処理を行う。
外部の廃棄業者に委託する場合は、溶融廃棄証明書を受領する。
(3) 電子媒体の廃棄は、原則粉砕処理とする。
(4) 情報機器のハードディスク等のデータについては、消去したデータを復元できない方式で消去を行う。
ハードディスク等のデータの消去を外部事業者に委託する場合は、消去証明書を受領する。
(5) 特に重要な情報の廃棄においては、システム管理者が廃棄、消去の作業に立ち会い確認する。

3.8 盗難、紛失時の対応

(1) 内部で保管中の個人情報が含まれる情報格納媒体及び機器、システム管理者の許可を得て外部に持ち出しした個人情報が含まれる可搬型媒体等に、盗難、紛失等が発生した場合、システム管理者は速やかに運用管理責任者に届け出をする。
(2) 運用管理責任者は適切な対処を行うと共に事業管理者に報告を行い、その取り扱いに関し

協議の上対応を定める。

3．9 従業員の守秘義務

従業員は、在職中、退職後に関わらず業務上に知り得た個人情報に関する守秘義務を負う。

4．サポートセンターの業務と運営

4．1 サポートセンターの業務

（1）本人（患者等）及び医療機関等の利用者（以下、「システムの利用者」という。）への相談、苦情等の窓口および医療機関の利用者、本人（患者等）からの申請に関わる登録・変更等業務を行うサポートセンターを設置する。

（2）サポートセンターは、以下の業務を行う。

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 システムの障害に関する問い合せへの対応
④ システムの操作に関する問い合せへの対応
⑤ システムの保守、障害、緊急時等の対応
⑥ 個人情報の取り扱いに関する相談、苦情等への対応
⑦ 利用者のシステムへの登録、変更、撤回等の業務

（3）サポートセンターの運用日と時間

サポートセンターの営業日と時間は、以下のとおりとする。
月曜日～金曜日の9:00～17:00（除く 土、日、祝祭日及び年末年始）

（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

4．2 サポートセンターの安全管理

（1）システム管理者は、サポートセンター責任者を任命し、個人情報保護及び情報の取り扱いに関する教育を行うものとする。

（2）サポートセンター責任者は、その構成員に個人情報保護及び情報の取り扱いに関する教育を行うものとする。

（3）サポートセンター責任者が実施する安全管理事項

① サポートセンターで、個人情報を含む情報を取り扱う場合の取り扱い場所は、外部の者に目が触れない場所とする。
② システムの利用者の登録、変更等に関わる業務を行う PC は専用とし、他の業務に使用する PC と共用をしない。
③ システムの利用者の登録、変更等に関わる業務を行う PC は、盗難、不正な持ち出しを防

ぐため施錠付ワイアーを利用する等の対策を講じる。

④ 個人情報に関わる書類は、鍵のかかるキャビネットに保管し、センター責任者が鍵を管理する。

⑤ 廃棄する紙媒体は、シュレッダーにより粉砕処理する。

⑥ 使用する PC は、少なくとも PC ログインパスワードを必須とする。

⑦ 使用する PC は、ウィルス対策を実施する。

⑧ 本システムにログインする場合は、PKI カードを用いる。

⑨ 本システムにアクセスした結果のログを残し、保存する。

⑩ 個人情報を含む情報のネットワーク利用は、安全なネットワーク（IPSec+IKE）を使用する。

⑪ システム管理者の許可を受けた場合を除き、可搬型記憶媒体は使用しない。

5. リモート保守の安全管理

5．1 リモート保守の実施

（1） リモート保守責任者は、システムの安全かつ迅速に対応するためリモート保守を行う。

（2） リモート保守は、以下の業務を行う。

① システムの稼働状況を把握する。

② システム障害からの回復措置を講じる。

③ ソフトウェアの保守、改修等を行う。

④ システムへの不正侵入、ウィルス等の検知とその対応を行う。

5．2 リモート保守の安全管理

（1） システム管理者は、リモート保守責任者を任命し、情報の取り扱いに関する教育を行う。

（2）リモート保守責任者は、その従事者に情報の取り扱いに関する教育を行う。

（3）システム管理者はリモート保守の手順を管理し、リモート保守責任者に、その遵守を徹底させるものとする。

（4） リモート保守責任者が実施する安全管理事項

① リモート保守は、外部の者の窃視を防ぎ、外部の者の入室を管理できる場所で行う。

② 利用する PC は、本システム専用とし、他のシステムと共用をしない。

③ 本システムの個人情報へはアクセスしない。

④ 廃棄する紙媒体は、シュレッダーにより粉砕処理する。

⑤ 使用する PC は、ウィルス対策を実施する。

⑥ 本システムにログインする場合は、PKI カードを用いる。

⑦ アクセスした結果のログを残し、保存する。

⑧ 安全なネットワーク（IPSec+IKE）を使用する。

⑨ システム管理者の許可を受けた場合を除き、情報記録媒体は使用しない。

別表3 「システム運用者のアクセス許可要件」

6. システムの利用者の責務

6.1 医療機関等とその利用者の責務

医療機関等とその利用者は、以下を遵守するものとする。

「能登北部医療圏地域医療連携システム　個人情報保護方針」

「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」

「能登北部医療圏地域医療連携システム　システムの利用規約」

「医療機関・薬局の安全管理規定」

「利用申請書」、「利用の撤回届」、「PKI カード利用申請書」等

6.2 本人（患者等）のシステム利用の責務

本人（患者等）は、以下を遵守するものとする。

「患者さんの参加にあたっての説明書」

「患者さんの安全な利用の手引き」

「参加同意書」、「内容変更申請書」、「参加の撤回届」等

7. 利用者の認証とシステムの利用開始

7.1 保険医療機関の組織の認証

医療機関等が使用するIPSec+IKE ネットワークにおけるPKI 鍵を利用して、利用申請のある施設の申請責任者からの申請書類と医療機関等番号で、保険医療機関又は保険薬局の実在性を確認する施設の認証を行う。

7.2 医師又は薬剤師の認証

（1）システム管理者は、医師又は薬剤師のシステム利用者の登録を管理し、そのアクセス権限を管理し、不正な利用を防止する。

（2）医師又は薬剤師が所属する施設の申請責任者から利用者申請書をサポートセンターで受理することで、当該医師又は薬剤師のシステム利用の登録がなされる。

（3）前（2）項に加え、医師又は薬剤師が HPKI カードを保有する及びその利用パスワードを保有することをもってシステムの利用ができる。

7.3 施設の従事者の認証

（1）システム管理者は、医療機関等の医師、薬剤師以外の従事者のシステム利用者登録を管理し、そのアクセス権限を管理し、不正な利用を防止する。

（2）システム管理者は、PKI 認証局の審査責任者を兼ねることができ、医師又は薬剤師を除く施設に所属する従事者が使用するPKI カード発行申請の審査業務を行うことができる。 兼任しない場合は、別途の審査責任者がこれを行う。

（3） 施設の申請責任者からの利用者リストを含む利用申請書をサポートセンターで受理することをもって、審査責任者は PKI カードの発行審査を行い、PKI カードを発行する。
（4） 施設の責任者は、PKI カードを利用する従事者に対し適切な使用を指導し管理する責任を持つ。
（5） 前（3）項に加え、従事者は、PKI カードの保有及びその利用パスワードを保有することをもってシステムの利用ができる。

7．4 患者本人の認証

（1） システム管理者は、システムへの患者の利用者登録を管理し、そのアクセス権限を管理し、不正な利用を防止する。
（2） サポートセンターが本人（患者等）から参加同意書を受理することで、当該本人（患者等）のシステム利用の登録が可能となる。
（3） 前（2）項に加え、本人（患者等）は利用 ID+パスワード+マトリクス認証をもってシステムの利用ができる。
（4） 本人（患者等）は、会員カードの券面に記載された ID と医療機関等名称、患者氏名を提示することで本実証に参加している本人（患者等）であることを示すことができる。
（5） 本人（患者等）が、会員カードを医療機関等に提示する場合、医療機関等で本システムを用いて患者の IDm番号を利用し当該患者の必要情報を検索する用途にも利用する。

7．5 患者の代理者の認証

患者本人がシステムを利用したこと同じとする。

8．利用者のアクセス制御

8．1 医療機関等の利用者のアクセス制御

情報の種別と作業単位で

医師、薬剤師の HPKI カードを利用した本システムのアクセス制御条件

医療機関等の従事者の PKI カードを利用した本システムのアクセス制御条件

を、以下の表に示す。

別表4 「HPKI,PKI カードを利用したアクセス制御条件」

8．2 どこでも MY 病院の利用者のアクセス条件

① どこでも MY 病院を利用する本人（患者等）
② 本人（患者等）の代行作業でどこでも MY 病院システムへ電子おくすり手帳情報を登録する医薬局の利用者

の2ケースにおける作業ごとのアクセス条件を以下の表に示す。

別表5 「どこでも MY 病院の本人（患者等）及び医療機関等の作業とアクセス条件」

9. 電子署名の利用

9.1 システムでの電子署名利用対象者

本システムにおける電子署名の利用は、次の要件を満たす対象者において、利用が可能である。なお、ここでいう電子署名にはタイムスタンプの付与を含むものとする。

① 医師又は薬剤師で、日医認証局又は日薬認証局から、HPKI カードが発行され、利用可能な状態になっていること。

② システムの利用申請が受理され、システムの利用の登録が完了している者であること。

9.2 本システムでの電子署名の対象

本システムの電子署名対象情報は、以下のとおりとする。

① 医療機関においては、処方情報及び紹介状

② 薬局においては、調剤結果情報

10. センター設備及びシステムの安全管理事項

10.1 データセンターの設備対策

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。

10.2 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入退できること。

（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ス

タッフの同行時のみ許可されること。

（3）従業員は、常に名札を着用すること。

（4）外部からの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。

10．3 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、予め日程と時間を事前に登録した連絡先へ連絡すること。

10．4 データセンターシステムのウィルス対策

（1）セキュリティ対策のため、全てのサーバ及び端末にウィルス対策ソフトを導入し、パターンファイルは常に最新なものに維持する。

（2）定期的にウィルスのチェックを行ない、感染の有無を確認する。

（3）定期的に脆弱性の検査を行い、脆弱箇所が判明した場合はその対策を講じる。

（4）ウィルス対策ソフトは、常に動作状態におく。

10．5 データセンターシステムの運用監視

（1）システム管理者は、サーバの運転状態を常に監視する対策を行い、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、Ping による5分ごとの生死監視、15分ごとのサーバの応答監視を行うものとする。

（3）システム管理者は、ファイアーウォールのアクセルログの定期的なチェックを行うものとする。

10．6 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定期的又は自動で実施する。

（2）手動でのバックアップの場合

- バックアップ作業に当たる者は、その作業記録を残す。

（3）サーバ等のログを確認し、不具合の発生が無いかを確認する。

10．7 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）ネットワークの稼働監視は、Ping による5分ごとの生死監視を行うこと。

（3）定期的にログの収集を行い、そのログを保管すること。

（4）利用するネットワークは、

医療機関等においては、IPsec+IKE方式のVPNネットワーク

本人（患者等）においては、SSL暗号化ネットワーク

を利用する。

11. 業務委託における安全管理

11．1 外部との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。

① 守秘事項を含む業務委託契約を結ぶ。

② 業務委託契約は、責任の分界点、責任の範囲、サポートの範囲、個人情報の取り扱いに関する事項等を含む契約を交わすものとする。

11．2 再委託の安全管理

委託先事業者が再委託を行う場合において、委託先と同等の個人情報保護に関する契約がなされることとする。

12. 運用管理規程の見直し

12．1 セキュリティポリシー等の見直し

（1） 本システムに係るセキュリティポリシー等の見直しが、本運用管理規程に影響を与える場合、運用管理責任者は、直ちに本運用管理規程の見直しを行う。

（2） 見直し後の運用管理規程について、運用管理責任者は事業管理者に報告する。

12．2 利用者等からの指摘による見直し

（1） 運用管理規程を、本人（患者等）、医療機関等の利用者、従業員等からの申し出、障害等の発生、緊急事態の発生、システム運営委員会等からの指摘で、運用管理等に問題がある場合、本運用管理規程を見直すことがある。

（2） 見直しを行う場合、運用管理責任者は事前に事業管理者に報告し、見直し後の運用管理規程の報告を行う。

12．3 例外事項

（1） システム管理者は、運用上の問題、その他で、本規程の各事項を守れない状況が発生した場合は、運用管理責任者に報告し、その指示を受ける。

（2） 運用管理責任者は、事業管理者に報告し、その取り扱いを協議するものとし、その内容に応じて規程の見直し又は例外適用事項の決定を行う。

13. 運用管理規程公開、改訂の管理

13．1 運用管理規程の公開

（1）本運用管理規程は、以下の範囲に公開する。

① 事業管理者
② 厚生労働省
③ 運営委員会
④ 運営管理部会及びシステム開発部会
⑤ 利用する医療機関等
⑥ 本システムを運用管理する(株)電算及びその従業員

(2)その他の者に対しては、非公開とする。

13．2 運用管理規程の改訂の管理

本運用管理規程の改訂管理は、運用管理責任者が行う。

14．運用管理規程の施行

本運用管理規程は、平成24年 8 月 23 日より施行する。

修正履歴

Ver.	日付	作成者	内容	備考
1.0	2012-8-23	電算	初版の制定	
1.1	2012-10-10	電算	本文書の公開範囲に、「利用する医療機関等」を追加	

以上

別表・別紙リスト

（1）別表

別表1 「保護対象情報と利用目的・利用範囲」

別表2 「取扱個人情報と取扱者」

別表3 「システム運用者のアクセス許可要件」

別表4 「HPKI,PKI カードを利用したアクセス制御条件」

別表5 「どこでも MY 病院の本人（患者等）及び医療機関等の作業とアクセス条件」

（2）別紙:

別紙1:「ガイドライン及び標準規格等参照文書一覧表」

別紙2:「運用管理体制図」

別紙3:「緊急時、障害、災害時等の対応規定」