認定事業医療情報等の取扱いに関する安全管理指針

第1章 総則

第1条　（基本理念）

1. ICI 株式会社（以下、「当社」という。）は、当社の事業の用に供するすべての医療情報等及び匿名加工医療情報（以下、「認定事業医療情報等」という。）を適切に取扱うため、当社全役職員が遵守すべき行動基準として認定事業医療情報等の取扱いに関する安全管理指針（以下、「本指針」）を定め、その遵守の徹底を図ることとする。
2. 当社は、認定事業医療情報等の漏洩、毀損、滅失等のリスクからこれら情報資産を保護することの重要性を認識し、すべての役職員を挙げて本指針を遵守し、情報資産の機密性、完全性、可用性といった情報セキュリティを維持するための活動を実践する。

第2条　（基本方針）

1. 当社は、医療分野の研究開発に資するための匿名加工医療情報に関する法律（以下、「次世代医療基盤法」という。）、及び個人情報保護法をはじめとする、個人情報及び認定事業医療情報等の取扱いに関する法令、国が定める指針その他の規範を遵守する。
2. 当社は、認定事業医療情報等の取り扱いに関し、組織的、人的、物理的、技術的安全管理措置を策定し、取り扱う情報についてリスク分析を行い、リスクに応じた総合的かつきめ細かい対策を講ずるとともに、その実施並びに運用について定期的な評価・改善を行う。
3. 当社は、次世代医療基盤法第 17 条に基づき、事業の内容及び規模を考慮した適切な認定事業医療情報等を取得し、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保ち、利用及び提供を行う。本取り扱いにあたっては、法令に基づく場合又は人命の救助、災害の救援その他非常の事態への対応のため緊急の必要がある場合を除いて、認定事業の目的の達成に必要な範囲を超えて、認定事業医療情報等を取り扱わないこと及びそのための措置を講じる。
4. 当社は、認定事業医療情報等の漏えい、滅失又は毀損の防止及び是正のための措置を講じる。
5. 当社は、認定事業医療情報等の取扱いに関する苦情及び相談への対応にあたり、相談センターを設置し、適切かつ迅速な対応に努める。
6. 第 5 項における相談センターは、一般財団法人日本医師会医療情報管理機構及び当社の共同で設置し、当社への委託により運営する。相談センターの問合せ先は次のとおりとする。
    - 一般財団法人日本医師会医療情報管理機構 認定事業医療情報等相談センター（担当：宍戸、木島）
      電話番号：03-5981-9579
      E メール：soudan@j-mimo.or.jp

7. 本指針は当社の公式ウェブサイト上に公開する。

第2章 体制

第3条 （安全管理措置体制）

1. 当社の認定受託事業における安全管理措置の確保のため、以下の体制を定める。

(ア) 認定事業医療情報等に関する情報管理委員会（以下、「情報管理委員会」という。）

認定事業医療情報等に関する情報管理の取扱い、安全管理措置を統括する。

(イ) 認定事業医療情報等に関する情報セキュリティ責任者

規則第 6 条第 1 号ロの基準に適合する者。認定事業医療情報等を取り扱う業務における情報セキュリティに関する責任を負う。必要に応じて定期開催以外の情報管理委員会を招集し、また、委員会における議事の内容及び活動の状況について、必要に応じて役員に報告する。

(ウ) 認定事業医療情報等に関する上級情報セキュリティ管理者（以下、「上級情報セキュリティ管理者」という。」）

情報セキュリティ管理者による管理状況を監督し、情報セキュリティ責任者に報告する。必要に応じて情報管理委員会への参加者を指名する。必要に応じて情報セキュリティ責任者に代わり定期開催以外の情報管理委員会を招集する。

(エ) 認定事業医療情報等に関する情報セキュリティ管理者（以下、「情報セキュリティ管理者」という。）

上級情報セキュリティ管理者の監督の下、情報セキュリティの管理を実施する。

(オ) 認定事業医療情報等に関する上級システム管理者（以下、「上級システム管理者」という。上級情報セキュリティ責任者もしくは情報セキュリティ管理者との兼務を認める）

システム管理者によるシステム管理状況を監督し、情報セキュリティ責任者に報告する。

(カ) 認定事業医療情報等に関するシステム管理者（以下、「システム管理者」という。上級情報セキュリティ管理者もしくは情報セキュリティ管理者との兼務を認める）

上級システム管理者の監督の下、システムの管理を実施する。

2. 当社における安全管理措置の実施に関する評価及び改善のため、当社における情報セキュリティマネジメントシステムの定めに従い、以下のとおり内部監査を行う。

(ア) 内部監査の目的

安全管理措置の取組みが、当社の規定した要求事項に従って実施されているか、次世代医療基盤法並びに個人情報保護法及び関連する法律や規則、ガイドライン等の要求事項に適合しているか、有効な実施及び継続的な維持が行われているかを評価し、その結果を踏まえ、情報管理委員会委員長の指示の下、必要な管理策を講ずるため。

(イ) 内部監査の対象

医療情報取得・整理部／匿名加工・解析部／匿名加工医療情報提供部／相談センター。

(ウ) 内部監査の頻度

毎年度実施するものとし、情報セキュリティマネジメントシステムにおける認証機関による審査の１ヶ月程度前を目安とする。

(エ) 内部監査員

被監査部門と独立した部門より選任するものとする。また、当該監査員においては、被監査部門との併任でないこととする。

3. 当社が認定事業医療情報等の取扱いに関する業務を外部に委託する際の安全管理措置の実施に関する評価及び改善のため、当社における情報セキュリティマネジメントシステムの定めに従い監査を行う。

(ア) 監査の目的

委託先における安全管理措置の取組みが、当社の規定した要求事項と同等以上の水準で実施されているか、次世代医療基盤法並びに個人情報保護法及び関連する法律や規則、ガイドライン等の要求事項に適合しているか、有効な実施及び継続的な維持が行われているかを評価し、その結果を踏まえ、当社における情報管理委員会委員長の指示の下、委託先として適切か否かを判断し、適切でないと判断した場合は他の委託先への切替え等を検討するため。

(イ) 監査の対象

認定事業医療情報等を取り扱う委託先。

(ウ) 監査の頻度

少なくとも年 1 回以上実施するものとし、原則として情報セキュリティマネジメントシステムにおける認証機関による審査の 2 ヶ月乃至 3 ヶ月程度前を目安とする。また、事業継続上のリスクとなりうる事項が発生した場合等、必要に応じて委託先の評価を行い、前記の定められた時期によらず監査を行うこととする。

(エ) 監査員

当社における情報管理委員会委員長の指示の下、監査員を選任する。

(オ) その他

前各号に定めるほか、当該監査に関する事項は、当社の別紙 D 添付３委託先管理規程第 3 章から第 6 章までに定めるとおりとする。

第4条　（情報管理委員会）

1. 情報管理委員会の設置

当社における安全管理措置を統括するため、情報管理委員会を設置する。

2. 委員の構成

情報管理委員会の構成は以下のとおりとする。

(ア) 情報管理委員会委員長

(イ) 情報セキュリティ責任者

(ウ) 上級情報セキュリティ管理者

(エ) 上級システム管理者

(オ) 上級情報セキュリティ管理者が指名する者

(カ) また、必要に応じ役員等が同席する。

① 委員の氏名及び役職を公表する。

② 委員長に事故等のある場合には、予め指定した代行権限者が代行する。

3. 情報管理委員会の役割は以下のとおりとする。

(ア) 平時における、方針の規定、管理状況の把握、課題への対応（関係者への周知・教育含む）の指示等

(イ) 有事における、トリアージ、事実関係と影響範囲の調査、原因の究明、各種対応の指示等（当社における Computer Security Incident Response Team (CSIRT) としての役割）

4. 情報管理委員会の開催は、月次程度の頻度で定期的に開催するほか、必要に応じて委員長が招集する。

5. 委員長は、委員会を開催したときは、速やかに要点をまとめた議事の概要を作成し、2年間これを保管する。

6. 委員長は、委員会における議事の内容および活動の状況について、必要に応じて役員に報告する。

第3章 安全管理のための規程類の整備

第5条　（内部規則等の整備）

1. 認定事業医療情報等並びにそれらを取り扱うシステムの安全管理のための規定類として、「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」及び「技術的安全管理措置」について規定した内部規則等を整備するとともに、その運用の評価及び改善を行う。また、必要に応じこれらの下位規程類を定める。

第4章 認定事業医療情報等のための研修の実施

第6条　（研修・訓練の実施）

1. 情報管理委員会は、認定医療情報等を取り扱う役職員等に対して、認定事業医療情報等の適切な取扱いの理解を深めるための教育及び訓練を実施する。

2. 情報管理委員会は、予め作成した研修・訓練実施計画にしたがい、年に１回程度、認定医療情報等を取り扱う全役職員等を対象とした認定事業医療情報等の安全管理のための研修を定期的に実施する。

3. 研修は、認定事業医療情報等の安全管理の基本的な考え方、安全管理指針、情報セキュリティ基準、及び事故防止の具体的な手法等について、認定医療情報等を取り扱う全役職員等に周知徹底することを通じて、役職員個々の安全意識の向上を図る。
4. 認定医療情報等を取り扱う全役職員等は、研修が実施される際には、極力、受講するよう努めなくてはならない。
5. 情報管理委員長は、本条３号の定めにかかわらず、ICI 内部で重大事故が発生した後など、必要があると認めるときは、臨時に研修を行うものとする。
6. 情報管理委員会は、研修を実施したときは、その概要（開催日時、出席者、研修項目）を記録し、２年間保管する。

第7条　（研修・訓練の実施方法）

1. 研修・訓練の実施方法については、別途研修・訓練実施計画を策定し、本計画に基づき実施する。

第5章 認定事業医療情報等の漏えい、滅失または毀損の発生時の対応

第8条　（漏えい、滅失または毀損の発生時の対応）

1. ICI において認定事業医療情報等を取り扱う者が、認定事業医療情報等の漏えい、滅失または毀損の発生等の関係法令等に違反している事実又はその徴候を把握した場合、下記の順序を基本とする報告連絡体制により、速やかに ICI の情報セキュリティ責任者に報告する。報告を受けた ICI の管理者は ICI における上位の管理者又は責任者に報告を行い、必要に応じて ICI における情報管理委員会を招集する。
   ① 認定事業医療情報等を取り扱う者を管理する ICI の管理者
   ② ICI の上級情報セキュリティ管理者
   ③ ICI の情報セキュリティ責任者
2. ICI の情報管理委員会は、ICI の各関係部門、認定事業者並びに ICI が認定受託事業に関する業務を委託する認定医療情報等取扱受託事業者（以下、「認定受託事業者」という。）たる NSSOL と連携し、トリアージ、事実関係と影響範囲の調査、原因の究明及び各種対応の指示等を行う。このとき、ICI の情報管理委員会は ICI における CSIRT (Computer Security Incident Response Team) としての役割を担うものとする。ICI の情報管理委員会において、ICI 及び認定事業者並びに ICI が認定事業医療情報等取扱い業務を委託する認定受託事業者たる NSSOL のみでの調査等が困難であると判断された際は、第三者調査を行うものとする。なお、当該判断が為される例としては、マルウェア感染等の詳細調査、システムにおける不正な動作等の原因究明、また内部不正の可能性があるとき等が考えられる。
3. ICI の上級情報セキュリティ管理者は、ICI の上級システム管理者が、いつでも１時間以内に高セキュリティエリアに赴き、オープンなネットワーク環境から切り離された

環境で認定事業医療情報等を取り扱うシステムにアクセスし緊急時の対応が可能な体制を確保する。

4. ICI の上級情報セキュリティ管理者は、再発防止策の検討及び策定を行う。
5. ICI の情報セキュリティ責任者は、事案発生時及び発生後における逐次対応状況、並びに収束後における事実関係及び再発防止策等の報告を行う。当該報告においては、「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第１号）における「２．漏えい等事案が発覚した場合に講ずべき措置」に基づく内容を別紙 Q に示すとおり行うものとし、同じく別紙 Q に示すとおり「３．個人情報保護委員会等への報告」に基づき主務省庁のほかに個人情報保護委員会への報告を行うものとする。なお、当該報告にあたっては、下記の優先順位にて行うものとする。
   ① ICI 各関係部門及び認定事業者並びに ICI が認定事業医療情報等取扱い業務を委託する認定受託事業者
   ② 主務省庁及び個人情報保護委員会（原則として J-MIMO の情報セキュリティ責任者を通じて行うものとし、ICI からの報告が求められる場合のみ ICI の情報セキュリティ責任者が行う）
   ③ その他の各関係機関等（原則として J-MIMO の情報セキュリティ責任者を通じて行うものとし、ICI からの報告が求められる場合のみ ICI の情報セキュリティ責任者が行う）
6. 前項までの事案対応における役割は下記のとおりとする。なお、ICI の上級情報セキュリティ管理者が不在又は ICI の上級情報セキュリティ管理者に事故があるときは、予め上級情報セキュリティ管理者が指名した情報セキュリティ管理者、または上級システム管理者のいずれかが代行するものとする。また、現場指揮及び現場対応（主担当・支援担当）について、同一の者が複数の役割を兼ねないものとする。
   - ICI における全体指揮（NSSOL の全体指揮者への指示を含む）: ICI の上級情報セキュリティ管理者
   - ICI における現場指揮 : ICI の情報セキュリティ管理者又は ICI の上級システム管理者
   - ICI における現場対応 : ICI の上級システム管理者又はシステム管理者（主担当）、システム管理者及び事案発生部署の管理者等（支援担当）
   - 主務省庁等及び認定事業者への連絡等 : ICI の情報セキュリティ責任者
7. 前項までの対応を適切かつ迅速に行うため、ログの収集・監視・分析を行うものとする。

第6章 認定事業医療情報等の授受時の対応

第9条 （医療情報の提供を受ける方法及び安全管理措置）

1. 認定事業者が医療機関等（医療情報取扱事業者）から医療情報の提供を受ける際には、

医療情報取扱事業者が医療情報の提供にあたり安全管理のための措置を適正に行いうることを確保することを明記した契約書を認定事業者と医療情報取扱事業者側との間で締結し、当社は認定事業者の指示に従って医療情報を取り扱うこととする。

第10条 （匿名加工医療情報の提供方法及び安全管理措置）

1. 認定事業者（J-MIMO）が匿名加工医療情報を提供する際には、J-MIMO と匿名加工医療情報取扱事業者の間で契約を締結する。当社は、認定事業者の指示に基づき、匿名加工医療情報の提供を行う。
   (ア)J-MIMO が、提供する情報が匿名加工医療情報である旨の明示及び安全管理措置を適切に講ずること
   (イ)匿名加工医療情報取扱事業者が匿名加工医療情報の利活用条件に反した匿名加工医療情報の取扱いを行った場合の制裁措置

第7章 その他

第11条 （本指針の周知）

1. 本指針の内容については、代表取締役社長、情報安全管理委員会等を通じて、全役職員に周知徹底する。

第12条 （本指針の見直し、改正）

1. 情報管理委員会は、少なくとも毎年１回以上、本指針の見直しを議事として取り上げ検討するものとする。
2. 本指針の改正は、取締役会の決議により行う。

附則

第1条 （制定日）

1. この規則は、令和２年５月 18 日に取締役会の決議により制定した。

第2条 （施行日）

1. この規則は、令和２年６月１日に施行する。