別添４

オンライン資格確認等システム及びレセプトのオンライン請求システムに係る安全対策の規程例

○○医院（又は病院、薬局、訪問看護ステーション）

１　目的

・　本規程は、○○医院（以下「当医院」という。）がオンライン資格確認システム、診療情報閲覧機能、薬剤情報閲覧機能、特定健診情報閲覧機能及びレセプト振替機能に関わるシステム（以下、「オンライン資格確認等システム」という。）及び診療報酬明細書・調剤報酬明細書・訪問看護療養費明細書（以下「レセプト」という。）等の請求データをオンラインで受け渡す仕組みを整備したシステム（以下「オンライン請求システム」という。）を適切に運用するために必要となる基本的な事項を定めるものである。

・　オンライン資格確認等システム及びオンライン請求システム（以下「本システム」という。）の運用に当たって使用される機器、端末、ソフトウェア等の適正な取扱いに関して必要な事項を定めるとともに、本システムで取り扱う患者の資格情報、診療・薬剤情報、特定健診情報等の個人情報の適正な管理に関して必要な事項を定めるものである。

２　組織・体制

・　当医院に、オンライン資格確認等システム管理者（以下「システム管理者」という。）を置き、医院長をもって、これに充てる。

・　医院長は、必要な場合、システム管理者を別に指名することができる。

・　本システムを円滑に運用し、責任の所在を明確にするために、本システムに関する情報管理及び運用について、それぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。

・　情報管理責任者及び運用責任者は、医院長が指名することができる。

・　システム管理者は、緊急時及び災害時の連絡、復旧体制及び回復手順を定めるとともに、非常時においても当該文書等を参照できるよう適切に保管する。

3　システム管理者の責務

・　システム管理者は、本システムに関する送信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うものとする。

・　システム管理者は、送信機器やソフトウェアに変更があった場合においても、利用者がオンライン資格確認等業務の遂行を継続的にできるよう環境を整備するものとする。

・　システム管理者は、本システムを正しく利用させ、個人情報及び重要情報の思わぬ漏えいを防ぐために、運用方法について、教育・訓練計画等を定めた上で、利用者の教育と訓練を行うものとする。

4　情報管理責任者の責務

・　情報管理責任者は、本システムで取り扱う患者の個人情報の適正な管理に関する責任を負う。

・　情報管理責任者は、本システムで取り扱う情報について、組織内で重要度の度合いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類を定義する。

厳秘	機密性が極めて高い情報の種別（例：薬剤情報、特定健診情報）
秘密	特定の範囲に限り開示することができる機密性が高い情報の種別 （例:実施手順（マニュアル)）
公開	広く一般に公開可能である情報の種別

・　情報管理責任者は、特に、本システム導入時、適切に管理されていないメディア使用時、又は外部からの情報受領時においては、コンピュータウイルス等の不正なソフトウェアが混入していないか確認する。

5　運用責任者の責務

・　運用責任者は、本システムの運用に当たって使用される機器、端末、ソフトウェア等の適正な取扱いに関する責任を負う。

・　本システムの送受信機器は、以下の業務に使用する。したがって、運用責任者はこれらの業務に必要とするソフトウェア以外のソフトウェアはインストールされていない事を点検する。

- オンライン資格確認等業務
- オンライン資格確認等業務の遂行上必要となる業務
- オンライン請求業務（レセプト作成業務等を含む。）
- オンライン請求業務の遂行上必要となる業務

・　運用責任者は、本システムで使用する送信機器にコンピュータウイルス対策ソフトウェアをインストールするとともに、定期的にコンピュータウイルスのチェックを行い、感染の防止に努める。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施するものとする。

・　運用責任者は、本システムの取扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておくものとする。

・　運用責任者は、本システムで取り扱う情報、本システムを構成する機器・ソフトウェアをリストアップした上で重要度に応じた分類を行い、必要に応じて情報の分類を表示する。また、常にリストを最新の状態に維持する。
・　本システムに関する送受信機器は、関係者以外の者による覗き見を防止するため、スクリーンフィルタを設置する等の対策を施す。

6　利用者の責務

・　利用者は、本規程及び本システムの実施手順（マニュアル）に定められている事項を遵守するものとする。
・　利用者は、システム管理者の許可を得ず、送信機器等を部屋外への持ち出しをしないものとする。
・　利用者は、本システムを正しく利用するための教育と訓練を受けるものとする。
・　利用者は、職務上知り得た個人情報を漏らさないものとする。その職を辞した後も、同様である。
・　利用者は、個人情報の漏えい及び改ざんが生じた場合及びそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うものとする。
・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報管理責任者に相談するものとする。
・　利用者は、本システムで取り扱う情報については、当医院内において定義した機密性分類に従って、取扱いを行う。
・　利用者は、関係者以外の者が不正に本システムを利用できないようにユーザ ID 及びパスワード等を、本人しか知り得ない状態に保つように適切に管理する。
・　本システムで取り扱うシステムにおいて、２要素認証を採用している場合を除き、利用者は、パスワードを定期的に変更する。（最長でも２か月以内に変更する）
・　利用者は、パスワードについて、類推しやすい文字列、極端に短い文字列、類似の文字列を繰り返し使用しない。

7　規程に対する違反への対応

・　システム管理者は、本規程に定める事項及び本機関で別に定める事項に対する違反があった場合の対処方法について明確にするとともに、それに従って、厳正に対応する。

8　評価・見直し

・　システム管理者は、本規程に定める事項及び本機関で別に定める事項を評価し、必要に応じて、定期的に見直す。

9　その他

・　適切なセキュリティ対策を図るために、当医院は「別表：本システム導入のために特に留意すべきセキュリティ対策」に示す技術的対策等を行う。

・　その他、本規程の実施に関し必要な事項がある場合については、医院長がこれを定める。

10　適用年月日

・　本規程は令和〇年〇月〇日より適用する。

別表：本システム導入のために特に留意すべきセキュリティ対策

1	本システムへのアクセスについては、利用者の識別と認証を行うこと。
2	本システムを導入する際は、オンライン請求ネットワークを利用し、ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざんを防止する対策を行うこと。
3	本システムを導入する際は、コンピュータウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
4	本システムの運用に当たって使用される機器、端末等において、接続できる外部記憶媒体（USB 機器等）の制限を実施すること。
5	本システムを導入する際は、外部ネットワークから本システムへのアクセスを制限する仕組みを導入し、ネットワーク事業者に対して外部ネットワークからのアクセスを制限する仕組みが導入されていることを確認すること。
6	本システムを導入する際は、医療機関等内部ネットワークにおいても、セキュリティ要件の異なるシステム間や安全管理上の重要部分との境界にはファイアウォール等を設置し、ネットワークを物理的又は論理的に分割すること。
7	本システムの導入に当たり無線 LAN を利用する場合は、以下の対策を実施すること。 ・利用者以外に無線 LAN の利用を特定されないようにすること ・関係者以外のアクセスを禁止する対策を施すこと。 ・通信を暗号化し情報を保護すること。
8	本システムを導入する際は、ネットワーク事業者に対して、医療機関間の通信を制限する仕組みを導入していることを確認すること。