ORCA プロジェクト

サポート事業所向け　セキュリティポリシー

2005 年 3 月 30 日

1．「個人情報の保護に関する法律[1]（略称：個人情報保護法）」の趣旨を十分理解するとともに「不正アクセス行為の禁止等に関する法律[2]（略称：不正アクセス禁止法）」ならびに「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律[3]（略称：プロバイダ責任法）」等を厳格に遵守し、日医標準レセプトソフトの認定サポート事業所に求められる対策を立て、組織的かつ定期的に遵法状況の確認を行うこと（医療機関の実データに当該機関からの許可なくアクセスすることは不正アクセス行為であることを改めて認識されたい）。

2．関連法令に違反する行為又は関連法令の趣旨に反する行為により個人の情報の漏洩や漏洩の危険性が高いと判断される状態があれば、速やかに防止・改善に努めるとともに、当該危険状態を発見した日を含め、３営業日以内に日医総研への報告を行うこと。当該危険状態を看過したり、発見したにもかかわらず放置することや、報告の著しい遅延などを認めた際には、認定サポート事業所の認定を取り消すことがある。

3．日医標準レセプトソフトを含むシステムの設定や保守管理を受託している医療機関との間には、必ず個人情報保護のための守秘義務と罰則規定等を含めた契約を締結すること。契約の雛形は、添付してある「守秘義務に関する業務委託契約の条項」を参考にされたい。

4．日医標準レセプトソフトのホームページに掲示された「ネットワークとセキュリティの設定[4]」を遵守すると共に各所から出ている安全管理指針[5]を熟知し、医療機関のエンドユーザーへの教育・啓発に努めること。

1　内閣府　個人情報の保護に関する法律
http://www5.cao.go.jp/seikatsu/kojin/

2　総務省　不正アクセス行為の禁止等に関する法律
http://www.soumu.go.jp/joho_tsusin/security/kiso/k05_09.htm

3　総務省　プロバイダ責任の概要
http://www.soumu.go.jp/joho_tsusin/top/denki_h.html

4　ORCAプロジェクトホームページ　「ネットワークとセキュリティの設定」
http://www.orca.med.or.jp/orca/tec/network_cecurity/security.rhtml

5　厚生労働省　「医療情報システムの安全管理に関するガイドライン」
http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html

５．日医標準レセプトソフトを含むシステムにおいて使用している OS やアプリケーションのセキュリティアップデートに関しては常に最新のものを入れ、安全を計ること。

６．ベンダーから日医標準レセプトソフトを含むシステムの設置された医療機関へのネットワーク接続は、日医標準レセプトソフトの維持・保守にかかわるものに限り、必要最小限にすること。

７．ベンダーから医療機関へのネットワーク接続を行う者の権限をベンダーの機関内ルールなどにより明確にし、どの従業員が何時どこに接続し、何を行ったかなどのログを記録しておくこと。VPN 等で医療機関に接続する場合も同様とする。

８．医療機関の日医標準レセプトソフトを含むシステムへのアクセス権限のある担当者が権限変更・転勤・配置転換・退職などにより変更された場合、すみやかにそのアカウントやパスワードを削除・変更し、権限を失った者がネットワークやシステムにアクセスできないような措置をとること。

９．日医標準レセプトソフトを含むシステムの検証等に患者データが必要な場合は、ダミーのテストデータを用いること。患者の実データは必要最小限の時にかぎって、取り扱うものとし、実データを用いる場合は、書面により医療機関の承諾を得ること。また、実データ使用後には削除・返却等の責任を持って行い、医療機関側に報告をしておくこと。

１０．患者の実データは原則として当該医療機関のシステムからいかなる方法でも移動させないこと。最も個人情報漏洩の事故の多いノートパソコンや USB メモリなど移動可能な媒体に格納しないこと。やむを得ず格納して移動する場合には暗号化をしておくなど対策を立てておくこと。

１１．患者の実データを公開されたネットワーク領域に置かないこと。無線 LAN も公開されたネットワークであると考えること。

以上

守秘義務に関する業務委託契約の条項

以下では、甲を医療機関、乙を事業者としています。

第〇条（再委託）

乙は、本件業務の一部又は全部を第三者へ再委託してはならない。ただし、甲が他の事業者（乙と同程度又はそれ以上の水準でセキュリティ対策及び個人情報保護対策を講じている事業者であって、乙がそのことを保証する場合に限る）に再委託することを事前に承諾した場合は、この限りではない。

第〇条（秘密保持）

1　秘密情報とは、契約の有効期間中に本件業務に関連して、乙が甲から開示を受ける業務管理等（技術上のものも含む）に関する有形無形の情報（本件業務に関連して、甲から直接的または間接的に乙に開示されるすべての情報を含む）であり、次の各号のいずれかに該当するものをいう。

（１）患者情報等個人のプライバシーに関する情報

（２）秘密である旨告知されたうえで開示された業務管理情報、技術資料、図面及びその他の関係書類並びに電子媒体を含む有体物により開示された情報

（３）本件業務に関して作成された議事録

（４）本件業務に関する、ＦＡＸ・電子メール・郵便等による通信内容

（５）本件業務に関し口頭で伝えられた情報で、事前又は事後に、甲が秘密であることを通知した情報

2　前項の規定にかかわらず、次の各号の一つに該当する情報については、秘密情報として取り扱わないものとする。

（１）開示時に既に公知であった情報、又は既に乙が保有していた情報

（２）開示後、乙の責によらず公知となった情報

（３）乙が正当な権限を有する第三者から適法に入手した情報

（４）乙が独自に開発・知得した情報

（５）法令に基づき政府機関や裁判所に開示する必要のある情報

3　本件業務に基づき甲が乙に開示する秘密情報について、乙は、次の各号の義務を負う。

（1）乙は、善良な管理者の注意義務をもって秘密情報を管理すること

（2）甲の承認なく秘密情報を複写、又は、第三者に提供若しくは貸与しないこと

（3）本件業務の目的以外に秘密情報を使用しないこと

（4）本件業務が終了した場合又は甲が要請した場合、当該秘密情報に関する一切資料及び媒体を遅滞なく返却または破棄すること

第〇条（個人情報の保護）

1　本契約における「個人情報」とは、個人に関する情報であって、当該情報に含まれる氏名､生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む｡）をいう。

2　乙は、本件業務に関して、本人の同意なく、当該個人情報を収集したときの目的の範囲（甲から明示された場合はその範囲、それ以外の場合は社会通念上合理的と考えられる範囲）を超えて、個人情報を使用してはならない。

3　乙はいかなる場合であっても甲から提供された個人情報を第三者提供してはならない。

4　乙は、個人情報の漏えい、滅失及び毀損防止その他の個人情報の適正な管理のために必要な措置を講じなくてはならない。

5　その他個人情報の取り扱いについて、乙は甲から指示を受けて適切に対処するものとする。

第〇条（損害賠償）

乙が、前３条に違反して甲又は第三者に損害を生じせしめた場合、その損害（当該紛争に係る一切の費用であって、賠償金、訴訟費用及び弁護士費用を含むがこれに限定されない）を賠償する責を負う。乙の従業員又は乙の再委託先（甲の事前の了解があったか否かは問わない）による行為を原因とする場合も乙はその責を負うものとする。

以上