ORCA プロジェクト

医療機関向け　セキュリティポリシーについて

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）」、「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）」等について、理解を深め、情報システムを利用する医療機関に求められる対策をたて、組織的かつ定期的に遵法状況の確認を行ってください。

2．もし上記３法に抵触する等、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、速やかに保守契約を行っている認定サポート事業所への報告を行い、再発防止の対策を講じてください。

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契約している認定サポート事業所との間で、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してください。契約の雛形は、例として、添付してある「守秘義務に関する業務委託契約の条項」にありますので参考にしてください。

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「エンドユーザー向けセキュリティの設定[4]」や各所から出ている安全管理指針[5]を充分に理解し、従業員への教育・啓発に努め、セキュリティポリシーを遵守してください。職員共通のアカウントやパスワードなどは決して使用しないでください。

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、認定サポート事業所と連携して常に最新のものを入れ、安全を計ってください。

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#01_00

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（案）」（策定中）
http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=495040159

６．診療業務の途中でも、日医標準レセプトソフトの端末の設置されている席を外すときには必ず、ログアウトして、引き続き他の人に利用されないように注意してください。

７．日医標準レセプトソフトを搭載しているサーバーや端末には、その他のアプリケーションをなるべくインストールしないでください。やむをえず、インストールが必要なアプリケーションについては、認定サポート事業所等と相談して自己責任において当該新規アプリケーションの利用を決定してください。

８．日医標準レセプトソフトの接続されている LAN 内には、診療にかかわらない機器を接続しないよう注意してください。

９．従業者（派遣を含む）に対して、個人情報保護法等に関する教育ならびに指導監督を定期的に行ってください。

１０．日医標準レセプトソフトの端末にアクセスできる職員は必要最小限に留めておき、利用の日誌を記録してください。

１１．個人情報保護のためには、インターネットに接続していなくても日常運用は可能ですので、単体での利用を認定サポート事業所と相談して行ってください。ただし業務メニュー画面のニュースやお知らせは見えなくなりますので、ホームページやメーリングリストによって最新情報を取得してください。

１２．日医標準レセプトソフトの動作や表示に関して異常や不安を感じたときには速やかに契約している認定サポート事業者に連絡をして、対策を立ててください。

以上

守秘義務に関する業務委託契約の条項

以下では、甲を事業者、乙を医療機関としています。

第〇条（再委託）

甲は、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、乙が他の事業者（甲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、甲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、甲が乙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、乙から直接的または間接的に甲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、乙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、又は既に甲が保有していた情報

（２）開示後、甲の責によらず公知となった情報

（３）甲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）甲が独自に開発・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　本件業務に基づき乙が甲に開示する秘密情報について、甲は、次の各号の義務を負う。

（1）甲は、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）乙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乙が要請した場合、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　甲は、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（乙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　甲はいかなる場合であっても乙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　甲は、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、甲は乙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）

甲が、前３条に違反して乙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。甲の従業員又は甲の再委託先（乙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甲はその責を負うものとする。

以上