

# 佐久総合病院小海分院個人情報保護規定

平成17年4月1日制定

個人情報保護法が施行され、当院をはじめ医療機関は「個人情報取扱事業者」として個人情報の紛失、破壊、改ざん及び漏えいなどを防止するために以下の義務が課せられました。

- ・個人情報の安全管理措置義務（個人情報保護法第20条）
- ・従業者に対する監督義務（個人情報保護法第21条）
- ・委託先に対する監督義務（個人情報保護法第22条）

当院をはじめ医療機関はセンシティブ（機微）情報と言われております高度の守秘義務が要求されている個人情報を患者様からの依頼により保有しております。これを受けまして、当院は「個人情報の紛失、破壊、改ざん及び漏えいなどを防止するため、適切な情報セキュリティ対策を講じる」ことを宣言し、ホームページ上に公表しております。

つきましては、当院が保有する個人情報等の秘密情報の秘密保持について、今まで以上にご留意くださいますようお願い申し上げます。

## 1 外来・病棟における情報セキュリティマナー

秘密情報を記録した書類や記憶媒体は、それを使用しない時、特に業務時間外には、放置したままにしてはいけません。机の引き出しやキャビネットなどにきちんと保管してください。

不要となった書類は速やかに廃棄してください。廃棄する時は、焼却またはシュレッダーにかけてください。不要となった書類の裏面の利用は行ってはいけません。

帰宅時や外出時に机の上に秘密情報が記録された書類がない状態にしてください。

診療録は診療録管理マニュアルにしたがって利用し、使用が済んだら速やかに返還してください。診療録を院外に持ち出すことは原則として認めません。

患者様の症状等は当該患者様の診療等の関係者以外には開示しないでください。勤務室外などで患者様の情報を話す際にはよく注意してください。

診療録等の秘密情報はコピーしてはいけません。コピーが必要であれば、管理者の許可を得るか、個人情報がわからないようにして下さい。

患者様の症状等を電話・PHSで話すときは、周辺に部外者がいないか確認してください。

勤務室・診察室内に見知らない人がいたら、必ず声をかけてください。

FAXではダイヤルミスまたは記憶間違いなどにより、間違った番号を呼び出して文書やメッセージを誤配信することに注意してください。

休憩時等に勤務室内に誰もいなくなるような環境をつくらないようにしてください。

電話での患者様の入院に関する問い合わせ・病状に関する問い合わせには応じないようにして下さい。警察や家族と名乗ってもプライバシー保護の観点から答えられないことを話してください。

患者様の病状に関する説明は、患者様本人及び患者様が認める特定の家族・代理人に対してのみ行います。病状に対して明らかに問題がある場合には考慮しますが、患者様本人に話すのが原則です。患者様に意識がない場合・幼児の場合・精神科疾患での医療保護入院などでは、特定の家族・代理人に説明します。

## 2 コンピュータシステムおよびパソコンの取り扱いについて

### (1) パソコン利用の基本ルール

パソコンの電源を入れたときに通常の表示画面と異なるなど、画面の様子に異常がないか、変わったところがないか、確認してください。

許可なく外部ネットワークへ接続するための通信機器をパソコンに付けてはいけません。不正に入手したプログラム、使用許諾契約に違反するプログラムをインストールしてはいけません。

パソコンは利用者 ID とパスワードを入力しなければ利用できないようにしてください。パスワードは6文字以上の英数字記号を含むものとします。

メモにパスワードを書いて壁などに貼っておくことをしないでください。最低でも6カ月に1回はパスワードの変更を行うようにしてください。

暗号化の鍵としてカードなどを用いる場合、この管理・保管に細心の注意をはかってください。

出力結果はプリンターからすぐに取り出してください。

保守のために装置を事務所外に搬送する場合には、秘密情報を完全に消去してください。個人情報管理者の許可を得ないで秘密情報を CD-R 等の可搬媒体にコピーすることはできません。

## (2) コンピュータウィルスの防御

コンピュータウィルスや不正ソフトウェアから情報資産を保護するために、ネットワークに接続するすべてのパソコン(携帯パソコンも含む)には最新のワクチンプログラムを導入しなければなりません。パソコンを利用するときは、パソコン起動時からメモリーに常駐する形式でワクチンプログラムを稼動しなくてはなりません。

ワクチンソフトは、最新パターンファイル、最新バージョンのプログラムファイルが自動的に配信されるように設定しなければなりません。

コンピュータウィルスによって実害が生じたときは、遅滞なく個人情報管理者に連絡してください。

信頼できないあるいは不明な発信元の電子メール、添付ファイルは開かないでください。また、信頼される発信元からの添付ファイルであっても、表題などを読んでなりすましでないかを疑い、利用する前にワクチンソフトで検査(ワクチンソフトが自動的にチェックするように設定してください)をしなくてはなりません。

電子メールのプレビュー設定はしないでください。

外部ネットワーク経由で、あるいは、他の媒体よりファイルやソフトウェアを入手する場合には、作成元を確認してください。作成元が不明あるいは信頼できない場合には、入手してはいけません。入手した場合は、利用する前にコンピュータウィルスの検査を必ず行ってください。

## (3) 離席時のセキュリティについて

業務終了時には必ずシステムを終了させてください。

パソコンを使用中に長時間離席する場合も処理を終了して画面をクリアーにしてください。パスワードによる保護対策を実施してください。

## (4) 携帯用パソコンの運用について

暗号化していない秘密情報を記録した携帯パソコンの院外への持ち出しはできません。

暗号化に関しては、システム課で対応いたします。

秘密情報を登録した携帯パソコンを他人が容易に手の届くような場所に放置しないでください。また、必ずログイン・パスワードによるセキュリティ管理をして、他人が容易に秘密情報を入手できることのないようにして下さい。

## 3 電子情報の管理運用について

### (1) パソコンの制限

秘密情報は特定のコンピュータにだけ記録できます。

許可なく外部ネットワークへ接続するための通信機器を特定パソコンに付けてはいけません。

公開サーバーに秘密情報を記録してはいけません。

## (2) バックアップ

秘密情報は公開サーバー以外にバックアップしてください。

更新した秘密情報は1日1回バックアップをしてください。

## 4 秘密情報の送受信・運搬

大量の個人情報の交換は暗号機能付きの電子メールで行います。

個人情報の可搬媒体による運搬では暗号化して記録します。

院外に持ち出す場合は二重の封筒に入れて、中の封筒には拾得者に対する依頼事項（届け出てほしい旨および連絡先、氏名を書きます）を書きます。

レセプトの提出は担当職員が対応します。

他医療機関との患者情報のやり取りには、封書・FAXなどを利用します。詳細は管理事務室管理マニュアルに沿って行います。

## 5 電子メールの利用について

本文中では「半角カナ」文字や特殊文字を使わないようにしましょう（文字化けが起き、場合によっては本文全体が読めなくなることもあります）。

大きすぎるファイルを送ることは避けましょう（メールツールによっては、1MBクラスの文書でも受け付けることができないものがあります。また、相手方のメールボックスの許容サイズを超えてしまったりして迷惑をかけることがあります）。

大きなサイズのファイルや大量のデータを送る場合は、次のような方法を検討し、利用しましょう。

- ファイルを圧縮して送付

- ファイルを分割して送付

他の人の電子メールを転送などにより別の人に送付することを避けましょう（文書情報の中にはメール宛先の相手以外の人に知られたくないものが含まれている場合もあります。また、メールの送付者が、自分が送付したメールを無断で他人に転送されることを不快に思うこともあります）。

電子メールは文章が未熟なまま発信してしまうことがよくあります。送信する相手だけでなく、他の人が読んでも誤解されないよう、また不快に思われないようなきちんとした文章を作らなくてはなりません。発信する前に一度相手の立場になって読み返してください。

電子メールの送信先について誤りがないか送信時に再チェックしてください。

表題は具体的に日本語で発信者および内容が一目で分かるように付けてください。

## 6 研究などへの利用

学会発表・看護研究発表などへの医学的な利用は個人が特定されない形であれば問題ありません。ただし、一例報告・顔写真の使用などでは可能な限り文書での本人の了解が望ましい。各々の領域において、学会などでの規定があればそれに準拠します。

本来の診療以外への秘密情報の利用は患者さん本人の同意を得て、分院長と相談し、必要に応じて管理者会議の審査を受けます。

## 7 その他

不明な点は、事務管理課へ問い合わせてください。

秘密情報の取り扱いについて

ケース	すべきこと	物件例
保管媒体 / 印刷物へのラベル表示	すべてにラベル表示を行う。	診療録等
使用者	特別の権限者	診療録等
閲覧者	特別の権限者から許可された者	診療録等
保管	施錠できる部屋のキャビネット等に保管する。	診療録等
コピー	原則として禁止。 やむを得ないときは管理者の承諾を得る。	診療録等
ファクシミリによる伝送	診療録は原則として禁止。 やむを得ないときは管理者の承諾のもと細心の注意をもって行う。 相手先番号を確認する。	診療録等
電話による会話	周囲に患者等の部外者がいないことを確認する。	診療録等
廃棄処分(文書情報)	シュレッダー処理を行う。 大量の場合は焼却・溶解処理を委託する。現場に立ち会う。または廃棄の状況をビデオ撮影してもらい、廃棄証明書とともに受領する。	診療録、レセプト情報等
廃棄処分(電子情報)	ハードディスクの物理的破壊、特別のソフトによって上書きする	レセプト情報等
研究等のための院外持ち出し	原則として診療録等の院外への持ち出しは禁止。 やむを得ないときは管理者の承諾のもと細心の注意をもって行う。	診療録等
診療録等の内容の電子メール送信(ファイル添付)	個人名、住所が明記されているものは原則として禁止。	診療録等
院内での移転	権限者間で受け渡しをする。	診療録等
院外への移転	二重封筒を使い、拾得者への依頼事項を内側封筒に付記する。 医療費請求の場合は、事務職員が運ぶ。	診療録、レセプト情報等
送付	簡易書留にする。 緊急の場合は指定のバイク便。 宅配便、バイク便を利用する場合は、特定の1社に絞り、特別の契約を交わす。権限者が受取人に手渡しして、その際に伝票とは別に受領書を受領し、注意を促す。	診療録等
システムに格納されたデータへのアクセス許可	アクセス許可を個人単位で承認する。 全アクセス履歴を記録する。	レセプト情報等
個人情報記録された携帯パソコンの院外持ち出し	原則として禁止。暗号化等の事実上開示されない策を講じる。	診療録、レセプト情報等
個人情報リストの電子メールでの送信	原則として禁止。暗号化する。	症例データ、レセプト情報等
外部発表	管理者の承諾のもとに行う。	
患者による持ち出し	台帳および袋に記載する。	X線フィルム等