

【いつつばし連絡帳利用上の留意事項】

1) いつつばし連絡帳のセキュリティ対策

2) 参考資料

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第4.3版
6.9 情報及び情報機器の持ち出しについて

1) いつつばし連絡帳のセキュリティ対策

利用機器（パソコン、タブレット端末、スマートフォン）とパスワードについて

- ・施設の管理者は、「いつつばし連絡帳」を利用するスタッフと利用機器について把握し、台帳に記載して、適正に利用されているか確認をしてください。
- ・OS、ブラウザは、最新のものにして、ウイルス対策ソフトを導入してください。ファイル交換ソフトはインストールしないでください。
- ・「いつつばし連絡帳」（メディカルケアステーション）のパスワードは、保存しないでください。パスワードは、2ヶ月に一度程度、変更してください。
- ・機器を起動する際のパスワード（画面ロック）は、8文字以上の英数字混じりのものに設定してください。
- ・機器を他者（自分の家族も含む）に渡す（機種変更する、譲渡する、リースを終えて返却するなど）場合には、必ず、内容を徹底的に消去し、他者が「いつつばし連絡帳」を利用したり、機器内に残っているデータが閲覧できないようにしてください。

利用機器の紛失・盗難の際の対応

- ・直ちに他の機器を使い、メディカルケアステーションにアクセスし、自分のパスワードを変更してください。
- ・直ちに、いつつばし連絡帳事務局に、詳しい状況を電話やメールで通知してください。必要により、いつつばし連絡帳事務局から運営会社である株式会社日本エンブレースに連絡し、その利用者の利用を一時停止してもらいます。
- ・直ちに機器の携帯電話会社に連絡し、可能なら、機器のリモートロックなどの処置をしてもらってください。

他の連携方法との使い分けや併用

「いつつばし連絡帳」は連携手段の一つであり、万能ではありません。必ず、状況に応じて、他の連携方法との使い分けや併用をしてください。

- ・急ぐ場合は、電話で連絡を。
- ・規則上、文書が必要な場合は、紙の文書を。
- ・デリケートな内容の場合は対面などで。

「いつつばし連絡帳」で利用するスマートフォン・タブレット端末のセキュリティ対策

盗難・紛失対策

- 1) メディカルケアステーションのパスワードは保存しない
- 2) パスワードで、画面をロックする（8桁以上の英数字&記号の組み合わせで）
- 3) 携帯電話会社のリモートロックやデータの強制消去サービスを利用する

ウイルス感染対策

- 1) OS やアプリは常に最新の状態にアップデートする
- 2) 不要なアプリはインストールしない
- 3) アプリは信頼できる場所（メーカーやキャリアが用意する正規のアプリケーション・ストア）からインストールする
Android 端末の設定画面で「提供元不明のアプリ」という項目のチェックを外しておく
- 4) Android 端末では、アプリをインストールする際にアクセス許可を確認する
不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止する
- 5) メール の添付ファイルや URL リンク を不用意に開かない
- 6) セキュリティソフトを導入する。携帯電話会社のセキュリティ対策サービスを利用する

情報漏洩対策

- 1) 安全な回線（携帯電話の回線や施設内の無線 LAN）を使う。街中などの無線 LAN スポット（Wi-Fi 環境）は利用しない
- 2) 許可されたスタッフ以外とは、機器の共有をしない（自分の家族にも使わせない）

2) 参考資料

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第4.3版
6.9 情報及び情報機器の持ち出しについて

C. 最低限のガイドライン

1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
3. 情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
4. 運用管理規程で定めた盗難、紛失時の対応に従業者等に周知徹底し、教育を行うこと。
5. 医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。
6. 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的に変更する等の措置を行うこと。
7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LANは6.5章C-11の基準を満たさないことがあり、使用する場合は6.11章で述べている基準を満たした通信手段を使うこと。
9. 持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。
10. 個人所有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は1～5の対策を取るとともに、管理者の責任において上記の6、7、8、9と同様の要件を順守させること。

D. 推奨されるガイドライン

1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。
2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせる用いること。
3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。
4. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。
 - ・個人の所有する、あるいは個人の管理下にある端末は原則として使用せず、機器の設定の変更は管理者のみが可能とすること。
 - ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化するなどの対策を行うこと。

- いくつかの連絡帳のグループごとに、常に誰が参加しているのか判断しやすくするため、いくつかの連絡帳の個人設定で、スタッフごとにプロフィール及び顔写真を登録する。
- 自分が担当から外れた時は、該当するグループから速やかに「サポーター解除」を行う。
- 事業所を辞めた時や、事業所が廃止・休止になるなど、いくつかの連絡帳を利用する必要がなくなった時は、事業所から貸与されている端末があれば返却し、スタッフ誓約書に基づいて、必要な手続きを行う。
- いくつかの連絡帳ユーザーは、書き込みに際して、確定操作（入力情報が正しい事を確認する操作（例えば了解ボタンなど））を行って、入力情報に対する責任を明示すること。
- いくつかの連絡帳ユーザーは、与えられたアクセス権限を越えた操作を行わないこと。
- いくつかの連絡帳ユーザーは、不正アクセスを発見した場合、速やかに岩国市医師会事務局内のいくつかの連絡帳事務局に連絡し、その指示に従うこと。
- 端末の紛失や盗難により、どこでも連絡帳への書き込み等が外部の第三者に漏れる恐れがある場合には、速やかに岩国市医師会事務局内のいくつかの連絡帳事務局に連絡を行い、利用の停止等適切な措置を行うこと。