【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 5.1 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又は情報機器の盗難、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、紛失時の対応を従業者等に周知徹底するとともに、教育を実施すること。
5. 情報が格納された可搬媒体及び情報機器の所在を台帳等により管理すること。
6. 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けるとともに、定期的なパスワードの変更等の対策を実施すること。
7. 盗難、置き忘れ等に対応する措置として、情報に対する暗号化やアクセスパスワードの設定等、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について、外部のネットワークや他の外部媒体に接続したりする場合は、コンピュータウイルス対策ソフトやパーソナルファイアウォールの導入等により、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実施すること。なお、ネットワークに接続する場合は 6.11 章の規定を遵守すること。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.14.の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。
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又は停止するか、業務に対して影響がないことを確認すること。
10. 個人保有の情報機器（ノートパソコン、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、医療情報システム安全管理責任者は 1～5 の対策を行うとともに、医療情報システム安全管理責任者の責任において上記の 6、7、8、9 と同様の要件を遵守させること。

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漏えいを避けるため、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て用いること。
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. ノートパソコン、スマートフォン、タブレット等を持ち出して使用する場合、次に掲げる対策を実施すること。
   (1) BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。
   (2) 紛失、盗難の可能性を十分考慮し、可能な限り端末内に医療情報を置かないこと。やむを得ず医療情報が端末内に存在する場合や、当該端末を利用すれば容易に医療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に端末を初期化する等の対策を行うこと。

※BYOD（Bring Your Own Device）：私物の情報端末に業務で利用するソフトウェアの導入や設定を行い、外出先から社内システムにアクセスして業務に必要な情報の閲覧や入力を行うこと