

# 情報システム運用管理規程

医療法人以和貴会西崎病院

## 【目次】

はじめに

### 第1章 電子保存に関する管理規定

1. 総則
2. 責任
3. 運用
4. 懲罰
5. その他

### 第2章 電子保存に関する情報の範囲

1. 電子媒体による保存を認める文書等
2. 電子保存対象システム
3. 電子保存対象情報
4. 電子保存期間

### 第3章 管理組織

1. システム管理者
2. システム管理組織・委員会

### 第4章 安全管理

1. 利用者管理手順
2. 資産管理
3. データ管理手順
4. ドキュメント管理
5. 入退室管理
6. 情報システム障害対策
7. ネットワーク管理
8. 無線LANに関する対策
9. コンピュータウイルス感染対策

### 10. 個人情報の取り扱い

### 第5章 管理者マニュアル

1. はじめに
2. 管理者およびシステム委員会
3. 義務
4. 利用者への指導および管理
5. システムの利用
6. 業務の管理者の管理項目
7. 運用責任者の管理項目
8. 運用責任者と監査責任者

9. システム委員会の管理項目

10. 事件または異常事象の報告

11. 教育・訓練

12. マニュアル整備

## 第6章 利用者マニュアル

1. はじめに

2. 情報システムの利用

3. 義務と懲罰

4. 情報システムの利用時のセキュリティ

5. 情報システム運用管理面でのセキュリティ

6. 電子カルテシステムの利用時のパスワードセキュリティ

7. 法的に利用される電子カルテ情報の管理

8. 事件または異常事象の報告

9. 教育・訓練

## 第7章 医用画像運用・保守管理

1. 画像情報の確定操作と作成責任者の記録

2. 画像管理責任者

3. 検像

4. 時刻同期

5. 画像情報の保存期間と画像圧縮

6. 可搬記憶媒体、フィルムへの出力

はじめに

この規程は、医療法人以和貴会西崎病院（以下「当病院」という。）において、法令に保存義務が規定されている診療録及び診療諸記録（以下「保存義務のある情報」という。）の電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般（以下「情報システム」という。）について、その取扱い及び管理に関する事項を定め、当病院において、保存義務のある情報を適正に保存するとともに、適正に利用することを資することを目的とする。

## 第1章 電子保存に関する管理規定

### 1 総則

#### 1) 第1条（目的）

この規定は、医療法人以和貴会西崎病院における情報システム（以下、「情報システム」という。）にて、法令に保存義務が規定されている診療記録および診療諸記録（以下、「保存義務のある情報」という。）の電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般（以下、「電子保存システム」という。）について、その取扱い及び管理に関する事項を定めることにより、当院にて保存義務のある情報を適正に保存するとともに、適正な取扱いをするとともに、適正な取扱いをすることで患者の権利、利益の侵害の防止を行い、利用者及び管理者の正当性を確保することを目的とする。

#### 2) 第2条（情報システムのデータ保護の規定等）

当病院の情報システムのデータは、この規定の定めるもののほか、「安全管理」、「管理者マニュアル」および「利用者マニュアル」の定めるところにより保護されるものとする。

（1）前項に規定する情報システムのデータ保護規定等の内容は、以下のとおりとする。

##### ① 「安全管理」（第4章）

情報の管理や保護のため技術的な対策

##### ② 「管理者マニュアル」（第5章）

情報システムの管理者が注意すべき事項を規定

##### ③ 「利用者マニュアル」（第6章）

情報システムの利用者が注意すべき事項を規定

#### 3) 第3条（データおよび秘密情報の保護）

電子カルテを中心とした情報システムの診療情報等を含むデータおよび秘密情報は、機密性、一貫性、可用性の欠如に起因する保護されなければならない。

#### 4) 第4条（電子保存に関する理念）

この規定は、以下の基本原則に則った上で、「診療録及び診療諸記録の電子媒体による保存について」(平成 11 年 4 月 22 日付健政発 517 号厚生省健康政策局長、医薬発第 587 号医薬安全局長、保発第 82 号保険局長)に規定されているとおり、電子媒体に保存された保存義務のある情報が患者の診療や病院の管理運用上必要とされるときに、信頼性のある情報を迅速に提供できるよう、協力して環境を整え、適正な運営に努めなければならない。

#### (1) 自己責任の原則

自己責任とは、当病院が運用する情報システムの電子保存システムについて説明責任、管理責任、結果責任を果たすことを意味する。なお、電子保存システムとは、法令に保存義務が規定されている診療録および診療諸記録の電子媒体による保存のために資料される機器、ソフトウェアおよび運用必要な仕組み全般をいう。

説明責任とは、このシステムが電子保存の基準を満たしていることを第三者に説明する責任である。管理責任とは、このシステムの運用面の管理を施設が行う責任である。結果責任とは、このシステムにより発生した問題点や損失に対する責任である。

#### (2) 真正性・保存性・見読性の原則

真正性とは、正当な人が記録し確認された情報に関し第三者から見て作成の責任と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性の記録内容を誤ることをいう。

見読性とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。なお、“必要に応じて”とは、『診療、患者への説明、監査、訴訟等に関してその目的に応じて』という意味であり、“容易に”とは、『目的にあった速度、操作で見読を可能にすること』を意味する。保存性とは、記録された情報が、法令等で定められた期間にわたって、真正性を保ち、見読可能にできる状態で保存されることをいう。

#### (3) 周知原則

利用者は情報システムへの信頼を高めるために、診療情報等の保護対策、手続き、規則の存在およびその範囲について適切な知識を得ることができ、管理者はそれについて周知を図る。

#### (4) 倫理原則

情報システムの保護対策は、他の者の権利および利益を尊重して提供され利用されるべきである。

#### (5) 一貫性の原則

診療情報等の保護のための対策、手続き、規則には、技術、管理、組織、運営、教育、法律を含めた範囲での関連する考え方を考慮に入れて院内の対策、手続き、規則の緩和を図るべきである。

#### (6) 再評価原則

情報システムの保護施策の要求は、運用形態、利用形態および技術と共に変化するため、診療情報等保護のため対策、手続き、規則は定期的に再評価する。

#### (7) 患者のプライバシー保護の原則

診療情報の二次的利用（診療や病院管理を目的としない利用）についても、患者のプライバシーが侵害されることのないように注意しなければならない。

## 2 責任

### 1) 第5条（業務の明確化）

業務の管理者は、情報システムを利用する業務内容を、以下の範囲において明確にしておかなければならない。

- (1) 業務の名称
- (2) 業務の目的
- (3) 業務の管理者とその者の権限の範囲
- (4) 利用者とその者の権限の範囲・診療情報等の記録の内容

### 2) 第6条（利用者権限の付与の決定）

- (1) システム委員会（以下、「委員会」という。）は、利用者権限の付与規定を決定しなければならない。
- (2) システム運用責任者は業務の管理者と協議して、その権限付与について委員会に諮問することができる。
- (3) 診療情報等の取扱い権限を決定した委員会は、各利用者にその内容を周知し、その徹底を図らなければならない。

### 3) 第7条（診療情報等の取扱い規定）

システム管理者は、診療情報等に対して、以下の方針に則り取扱い権限の付与に関し、協議を行うものとする。

- (1) 診療情報等の登録、参照、更新の各権限は、原則として分離されること。
- (2) 利用者への権限の付与規定の決定は、システム委員会のみで行うこと。

(3) 業務上不必要な権限は付与しないこと。

### 3. 運用

#### 1) 第8条 (情報システムの監査)

(1) 運用責任者は、診療情報等の登録、参照、更新、削除を行う際の、ログ情報を収集し、定期的にその結果を監査責任者に提出し、監査責任者、システム管理者はシステム委員会に報告しなければならない。

(2) ログ情報は、以下の情報とする。

- ①利用者ID
- ②操作内容 (端末ID・患者ID)
- ③操作年月日と時刻

#### 2) 第9条 (教育および訓練)

システム委員会は、利用者あるいは利用者になるものに対して、診療情報等を保護する目的とその必要性を十分に理解させ、その対策を推進するために、教育訓練を行うものとする。

#### 3) 第10条 (廃棄)

システム委員会は、ハードコピーを取った資料などの不要となった診療情報等を安全な方法で、かつ速やかな廃棄・消去することを各部門に指導しなければならない。

#### 4) 第11条 (協力)

各業務の管理者は、この規定の実施および診療情報等の保護のための対策、手続きおよび規則を可能な限り有効なものにするため、委員会を構成する各管理者と協議し、調整し、協力しなければならない。

### 4. 懲罰

#### 1) 義務と懲罰

診療情報については、秘密を守る義務を課するとともに、これに違反した場合には就業規則に則り懲罰を科する。

### 5. その他

#### 1) 規定の見直し

この規定は、業務の大幅な変更や情報システムの構成変更時には、見直されるものとする。

## 第2章 電子保存に関する情報の範囲

当病院において、保存義務のある情報を電子保存にする際に対象とする情報の範囲については、システム委員会の審議を経て、病院長がそれを定める。

### 1. 電子媒体による保存を認める文書等

- 1) 医師法（昭和23年法律第201号）第24条に規定されている診療録
- 2) 歯科医師法（昭和23年法律202号）第23条に規定されている診療録
- 3) 保健婦助産婦看護婦法（昭和23年法律203号）第42条に規定されている助産録
- 4) 医療法（昭和23年法律第205号）第21条、第22条及び第22条の2に規定されている診療に関する諸記録及び同法第22条、第22条及び第22条の2に規定されている病院の管理及び運営に関する諸記録
- 5) 歯科技工士法（昭和30年法律第168号）第19条に規定されている指示書
- 6) 薬剤師法（昭和35年法律第146号）第28条に規定されている調剤録
- 7) 救命救急士法（平成3年法律第36号）第46条に規定されている救命救急処置録
- 8) 保険医療機関及び保健医療養担当規則（昭和32年厚生省令第15号）第9条に規定されている診療録
- 9) 保険薬局および保険調剤師療養担当規則（昭和32年厚生省令第16号）第6条に規定されている調剤録
- 10) 歯科衛生士法施行規則（平成元年厚生省令第46号）第18条に規定されている歯科衛生士の業務記録
- 11) 診療放射線技師法（昭和26年法律第226号）第28条第1項の規定による照射録

### 2. 電子保存対象システム

電子保存を行う対象のシステムは、以下のとおりである。

- 1) オーダリングシステム
- 2) 電子カルテシステム
- 3) 看護支援システム
- 4) 画像保管通信システム
- 5) 画像読影レポートシステム
- 6) 医用動画画像システム
- 7) 栄養管理システム
- 8) 医事会計システム
- 9) 健診システム

- 1 0) リハビリテーション支援システム
- 1 1) 心電図システム 1 2) 透析通信システム
- 1 3) 調剤システム 1 4) 服薬指導管理システム
- 1 5) 栄養指導システム 1 6) 放射線情報システム
- 1 7) インシデントレポートシステム

### 3. 電子保存対象情報

電子保存を行う対象情報は、全ての診療に関わる情報である。

- 1) 外来診療録
- 2) 透析診療録
- 3) 入院診療録

### 4. 電子保存期間

電子保存を行う診療に関わる情報の保存期間は、西崎病院診療記録管理規定 第2条第9項に定められた保存期間とする。

## 第3章 管理組織

### 1. システム管理者

当病院は情報システム管理者（以下、「システム管理者」という。）を置き、病院長をもってこれに充てる。

#### 1) システム管理者

全システムの管理責任者

必要な場合、病院長はシステム管理者を別に指名することができる。

- (1) 機器及びソフトウェアの導入に当たって診療録等の保存義務に適合するように留意する。
- (2) システムの機能が支障なく運用される環境を整備する。
- (3) 電子保存された情報の安全性を確保し、常に利用可能な状態におく。
- (4) 機器ソフトウェアに変更があっても情報が継続時に利用できるよう維持する。
- (5) 利用者の登録を管理し、不正利用を防止する。
- (6) 患者または利用者からの苦情を受け付ける窓口を設ける。
- (7) 事故対策：緊急・災害時の連絡、復旧体制及び回復手順、媒体管理する。
- (8) マニュアルの整備：取扱いマニュアルを整備し、利用者に周知の上、利用可能にする。
- (9) 教育と訓練：利用者に対し、取扱い並びにプライバシー保護に関する研修を行う。
- (10) 監査：監査責任者に年1回実施させ、必要な処置を講じる。

## 2) 運用管理者

情報システムの運用を円滑に行うために運用責任者を置く。

運用責任者は病院長が指名する。

- (1) システム運用の管理：情報システムを円滑に運営し、情報システム全体の管理を行う。情報システムが常に効率の効率化及び円滑化のために、情報収集し、合理的な運営を指針するために適切なシステム委員会に諮問しなければならない。
- (2) 機器の管理：サーバ室の施設管理、院内情報システム端末機器管理、OA端末機器管理、院内情報システムおよびOA端末機器に接続する外付けデバイス管理
- (3) ソフトウェアの管理：ソフトウェアを使用前に診査を行い安全性の確認を行うネットワークや可搬型媒体により情報を受け取る機器を限定するウィルスチェックを行い感染の防止に努める
- (4) ネットワーク管理：利用履歴の管理を行い、不正利用のチェック及び対策を実施するネットワーク負荷検査を行い、効率的な運用を維持する医療法人以和貴会の拠点間および医療法人以和貴会地域医療連携システムネットワークのネットワーク接続におけるセキュリティ管理を万全に行い、接続拠点間の安定運用を維持する

## 3) 監査責任者

システムが問題なく動いているか、また、不正に使用されていないか確認を監査するために、監査責任者を置く。

## 2. システム委員会

- 1) システム委員会システム委員会はシステム管理・運用に関して検討をする目的にて定期的に開催する。
- 2) 各科・各部署システム責任者各部署の問題点の管理及びシステム委員会への報告・検討を行う。
- 3) 運用責任者  
運用責任者は、必ずシステム委員会に属し、システム委員会の報告・検討課題に対して、管理・運用・対処処置を行う。

## 第4章 安全管理

### 1. 利用者管理手順

#### 1) 利用者管理の目的

利用者権限は、情報システムを利用する上で、利用資格の識別およびプログラムやデータファイル等への不正アクセスを制御し、データの変更等において利用者の真正性を高めることを目的とし、利用者情報区分によりアクセス権を設定するものである。

#### 2) 利用者権限の管理

新規	・ 病院に着任した時点
変更	・ 院内の部署が変わった時点 ・ 氏名が変更になった時点 ・ 業務が変更され、権限の内容が変更された時点
非表示	・ 退職または異動などで情報システムに関係のなくなったとき
利用者権限変更	・ 基本的に、医師・師長・技師・看護師等の設定がされているが、業務上、必要な区分がなくなったとき

#### 3) 申請・登録・交付・氏名変更・非表示

(1) 利用者権限の交付は、業務の責任者が運用責任者に利用者の申請書を提出し、システム委員会の承認を得る。また、利用者の異動に伴って事務部総務課または利用者管理者から非表示申請が出た場合、運用責任者はシステム委員会および監査責任者に報告する。

(2) 利用者の登録設定・非表示手続きは、事務部総務課または業務の責任者が次の項目を申請書に記入して運用責任者へ提出する。

- ① 利用者ID
- ② 所属
- ③ 所属科（※医師の場合指定）
- ④ 職種
- ⑤ 利用者氏名（漢字及びカナ氏名）
- ⑥ 性別
- ⑦ 役職
- ⑧ 麻薬管理者免許の番号

(3) 運用責任者は、申請書に基づき交付を行う。ただし、非表示申請は、事務部総務課または利用者管理者の異動連絡で運用管理者がこれを行い、委員会に事後報告する。

(4) 婚姻等により利用者氏名の変更がある場合、医師法施行規則（昭和二十三年十月二十七日厚生省令第四十七号）および医師法施行令（昭和二十八年十二月八日政令第三百八十二号）により保険医の場合は医籍、その他の職員の場合は戸籍に則つ

て、事務部総務課の連絡で運用管理者は利用者氏名の変更を行い、委員会に事後報告する。尚、「保険医・保険薬剤師氏名変更届」の「変更事由」欄に「旧姓使用を希望する」旨の記載を行い、旧姓のままの保険医登録票を使用している場合は例外とする。

(5) 人事異動・退職その他の事由により、当該システム使用に関係なくなった時、速やかに運用管理者が非表示処理をする。

## 5) 利用者ログの監査

### (1) 不正アクセスの防止

監査責任者は、不正アクセスを防止するため、以下の点を監視する。

- ① アクセス権の無い者によるデータアクセス
- ② パスワードの失権状況

(2) 点検の結果、異常がある場合は、その対象のパスワードを使用不可とし、不正使用の防止に努める。

## 2. 資産管理

### 1) システムバックアップ／復元手順

機器障害や災害などに備えて、システムのバックアップをとる事を義務付ける。

#### (1) バックアップの種類

- ① DBジャーナルのバックアップ
- ② データベース
- ③ システム本体 (OS)

#### (2) バックアップのタイミング

- ① 新規のアプリケーションが発生した場合
- ② 業務のアプリケーションに変更があった場合
- ③ 日次処理時

### 2) システムバックアップ媒体の管理手順

#### (1) システム資源の管理対象

運用管理者は、システム資源を保存する媒体は、パンク状態に陥るとシステムダウンと同等の重大な影響を及ぼしかねない障害に結びつくため日常の利用頻度の確認をしなければならない。

- ① DB格納の管理
- ② ディスク使用率の管理

## 3. データ管理手順

### 1) データの保管方法と場所

電子カルテを中心とした情報システムの医療情報を含むデータ及び機密情報は、施錠管

理できるサーバ室内のバックアップ装置に保管し、機密保護を努める。

## 2) データ授受管理手順

(1) 電子カルテを中心とした情報システムの医療情報を含むデータ及び機密情報については原則院外へ持ち出してはならない。やむを得ずデータ授受を行う場合は申請書に次の項目を記入し運用責任者へ提出する。

- ①目的
- ②情報資産名称
- ③持ち出し先
- ④返却・消去又は破棄方法
- ⑤返却・消去又は破棄予定日
- ⑥複製物の数

## 3) 破棄データ

(1) 電子記憶媒体の場合

媒体の破棄は、読取り不能の状態にした後、指定の廃棄場所に破棄する。

ハードディスク…ハードディスクデータ完全抹消ソフトを用いデータを破棄するか、物理的に破壊をして読取り不能にする。

CD・DVDメディア・USBメモリ等…物理的に破壊をして読取り不能にする。

(2) 紙帳票の場合

業務運用上発生する廃棄帳票は、シュレッダーにかけ、廃棄置場に破棄する。

## 4. ドキュメント管理

1) 取扱対象

取扱ドキュメントとは、システムプログラム・ユーザプログラム・電子カルテを中心とした情報システムの医療情報を含むデータ及び機密情報が記述されている全てのドキュメントである。

(1) 媒体の場合

磁気媒体に記憶されたプログラムドキュメントは、施錠管理される場所あるいは施錠管理のできる所定の保管ロッカーに保管する。

(2) 帳票の場合

紙に記述されたドキュメントは、施錠管理される場所あるいは施錠管理のできる所定の保管ロッカーに保管する。この際、ドキュメント管理台帳を作成し、ドキュメント管理を行う。

## 5. 入退室管理

医療法人以和貴会西崎病院 病院情報システム運用管理規程

- 1) 院内では、病院が定めた職員証を第三者が見える所に着用すること。
- 2) サーバ室への訪問者の入室は原則として禁止する。
- 3) 夜間あるいは時間外の訪問者は、時間外受付を通して事務当直者が確認をとること。

と。

4) サーバ室へ入退できるものは以下の者に限定する。

- (1) 病院職員（但し運用責任者をはじめとして権限付与のある者。）
- (2) 医療法人以和貴会法人管理部の職員
- (3) コンピュータ保守要員
- (4) 運用支援要員
- (5) システム開発者
- (6) 病院が契約あるいは依頼した保守業者
- (7) 病院が認めた訪問者

※ (3) ～ (7) に関して運用責任者の了解を必要とする。

#### 6. 情報システム障害対策

- 1) 情報システムの障害対応は、運用責任者がシステム全体の障害対応の詳細について全職員に周知する。

#### 7. ネットワーク管理

##### 1) インターネットネットワーク・患者診療情報提供ネットワークの構築

対外的な情報通信を行うためインターネット・プロトコル技術を利用し世界中にあるネットワークと相互接続されたコンピュータネットワークを院内に構築すること。利用の際には、以下の事項を守り利用すること。

- (1) 個人情報を含む情報をメールで送受信してはならない。
- (2) メールを院外に自動的に転送してはならない。
- (3) Webメールやネットディスクなどインターネットを經由して院外のサーバに個人情報を送受信してはならない。
- (4) 院内のパソコンを院外からアクセスできる状態にしてはならない。
- (5) セキュアネットワークアウトソーシングサービスを利用し、不正アクセス防止、不正通信防止、ウィルス・スパイウェア対策、情報漏洩対策を講じること。
- (6) 電子メールの送受信は、電子メール受信サーバおよび電子メール送信サーバを直接アクセスしてはならない。電子メールの送受信は、一時的にセキュアネットワークアウトソーシングサービスが提供するアプライアンスサーバに電子メールの受送信を行い、外部にはアプライアンスサーバを介して受送信をすること。
- (7) ファイル転送プロトコルを使用したファイル転送をしてはならない。

##### 2) 医療業務用ネットワークの構築

院内および医療法人以和貴会内の情報システム利用に限定された医療業務用ネットワークを院内に構築すること

- (1) 医療情報等の個人データを取り扱う機器・端末は、イントラネットに接続しなければならない。
- (2) 医療情報等の個人データは、許可なく情報システムの外に出さないこと。

(3) 医療情報等の個人データは、院外に持ち出しするノートパソコン、可搬記憶媒体に保存しないこと。

### 3) 個人所有端末のネットワーク接続・外部ネットワーク接続

職員個人が所有する端末のネットワーク接続および外部からネットワークを接続する端末の取り扱いについて以下のとおりとする。

(1) コンピュータウィルス感染の防止等データ保護のため接続する端末のオペレーションシステムは、運用責任者が許可したものに限定する。

(2) 医療情報等の個人データを保存しないこと。

(3) 所定の「個人所有端末利用・外部接続利用申請書」で、許可申請を行い運用責任者が指定した医療情報等の個人データおよび業務データが端末側にデータを残さないアプリケーションおよび接続方式にて利用を行うこと。外部接続の際には、データの漏洩、改竄及び破壊等を防止するため送信時の暗号化、受信時の復号化する VPN 通信以上のデータの安全かつ適正なセキュリティの確認が取れた通信回線を用いて以下の接続方式にて行い、すべて利用者識別番号（ユーザ ID）と暗証番号（パスワード）を用いて接続認証を行うこと。

① リモートデスクトップ方式

② 携帯用ゲートウェイ方式

③ 仮想デスクトップ方式

④ 電子署名検証方式

### 5) リモート保守回線管理

運用責任者は、情報システムの保守・運用作業を行うためリモート保守の回線を整備すること。

(1) リモート保守を行うパソコンには、医療情報等の個人データを保存しないこと。

(2) リモート保守を行う回線の接続は、作業を行うとき以外行わないこと。

(3) リモート保守をできるものは以下の者に限定する。

① 運用責任者

② 医療法人以和貴会法人管理部の職員

③ 病院が契約あるいは依頼したシステム開発会社・コンピュータ保守業者

※ ①②に関して所定の「院内ネットワークリモート接続利用申請書」を提出し許可の得た回線・端末のみで接続を可能とする。

※ ③に関して運用責任者の了解を必要とする。

(4) リモート保守状況をログ情報によって定期的にチェックし、システム委員会に報告する。

## 8. 無線 LAN に関する対策

### 1) セキュリティ対策

無線 LAN の脅威である「通信内容の傍受」、「無線 LAN の不正利用」、「アクセスポ

イントのなりすまし」等の対策を講じなければならない。

- (1) 利用者以外に無線LANの利用を特定されないようにすること  
→ANY 接続拒否による SSID 隠蔽有効設定
- (2) 不正アクセスの対策を施すこと  
→SSID によるアクセス制限
- (3) 不正な情報の取得を防止すること  
→WPA-PSK 方式の暗号化

## 2) 医用機器への考慮

無線LAN機器設置および医療機器等設置による動作の影響について留意しなければならない。当院では以下の発表資料から無線LAN設置影響による医療機器等への影響は1cm以内近づけた場合を除き影響がないと考える総務省「各種電波利用機器の電波が植込み型医療機器への及ぼす影響を防止するための指針」総務省「電波の医用機器等への影響に関する報告書」(平成16年3月)

※ 無線LAN規格 IEEE802.11/IEEE802.11b/ IEEE802.11g/ IEEE802.11a を調査対象とした調査研究報告

## 9. コンピュータウイルス感染対策

- 1) コンピュータウイルス感染の防止等データ保護のために端末にウイルス対策ソフトを常駐させるなど必要な措置を講じなければならない。
- 2) 可搬記憶媒体は、コンピュータウイルス対策、暗号化、パスワード認証の機能を兼ね備えた病院指定の媒体を利用すること。病院指定以外の可搬記憶媒体を利用する場合は、コンピュータウイルス対策、暗号化、パスワード認証の機能を兼ね備えた媒体を、所定の「外付けデバイス利用申請書」で、許可申請を行い運用責任者が指定した接続方法・利用方法にて利用を行うこと。
- 3) 病院指定の媒体の管理は、業務の管理者が行わなければならない。

## 10. 個人情報の取り扱い

個人情報の取り扱いについては、医療法人以和貴会西崎病院個人情報保護規程に則り処理を行うこと。

## 第5章 管理者マニュアル

### 1. はじめに

- 1) 本マニュアルは、西崎病院情報システム(以下「情報システム」という。)を安全に管理・運用するため、当病院の情報システム管理者が注意すべき事項を定めたものである。
- 2) 情報システムの管理者は、本マニュアルを遵守して、診療情報等の漏洩、改ざん、破壊などが発生しないように、安全に情報システムを管理運用しなければならない。

### 2. 管理者およびシステム委員会

1) 本マニュアルで規定する管理者および職務内容は、以下のとおりとする。

(1) システム委員会（以下「委員会」という。）の委員長：システム委員会を統括する。

(2) 運用責任者

① 各部署からの登録申請あるいは事務部総務課または業務の責任者からの異動情報を受けて情報システムへのアクセス権限の登録および変更許可をシステム委員会に報告する。

③ ハードウェアおよびソフトウェアの資源管理、特にハッキング等によるシステム障害の防止のための情報収集と各種メディアの感染防止に関する調査・検証を行う各部門の所属責任者で情報システムのセキュリティを管理するため、利用者に対して指示を行う。

2) 各構成委員が一利用者として情報システムを利用する場合には、本マニュアルおよび「利用者マニュアル」を遵守し、診療情報の漏洩、改ざん、破壊などが発生しないよう、安全に情報システムを利用し、また他の職員にも啓蒙しなければならない。

3. 義務

各構成委員は、本ガイドラインに則して情報システムの管理、運用しなければならない。また、情報システム上の情報について守秘義務を負わなければならない。

4. 利用者への指導および管理

各構成委員は、情報システムの利用者に対して、「利用者マニュアル」を遵守するように指導、管理し、その徹底を図らなければならない。

5. システムの利用

情報システムを利用する可能性があるすべての職員を登録し、利用者の異動、退職時には、速やかに利用者権限の設定、変更の依頼を行う。

6. 業務の管理者の管理項目

情報システムの利用環境面でのセキュリティについて業務の管理者は、以下の項目について管理する。

1.入退出管理

(1) 病院が定めた職員証の着用管理

病院が定めた職員証の有無により、権限のない者が情報システムを利用していないか確認する。

2. ノートブック型端末の管理

(1) ノートブック型端末の配置してある部署の業務の管理者は、常に配置台数と使用状況について管理する。

3. 情報システム端末機器管理

(1) 情報システム端末機器の設置してある場所は施錠管理すること。

4. リモート保守回線管理

- (1) 情報システムの保守・運用作業を行うためリモート保守回線の利用状況を管理する。

## 7. 運用責任者の管理項目

情報システムの運用管理面でのセキュリティは、以下の項目について管理する。

### 1) 設備についての管理

- (1) 重要なデータがどの装置に格納されているのか明確に定める。
- (2) 定期的に棚卸し、機器を厳重に管理する。

### 2) コンピュータウイルス感染対策管理

(1) 第4章第9項のウイルス対策ソフトのパターンファイルが常に最新となるよう更新作業を行うこと。

### 3) ドキュメント管理

- (1) 患者のプライバシーおよび病院運営に危害が及ぶ情報が記述されている重要なドキュメントは厳重に管理する。
- (2) 重要なドキュメントや帳票のコピーや持ち出しについて管理を行われなければならない。

## 8. 運用責任者と監査責任者

情報システムの利用時のセキュリティ (運用責任者および監査責任者)

### 1) 監査責任者の責任

#### (1) 端末の利用状況

- ① 医療情報システムの端末利用状況を管理しなければならない。
- ② 端末利用状況をログ情報によって定期的にチェックし、システム委員会に報告する。
- (2) 監査責任者は、アクセスログの管理あるいは利用者からの報告を受けてセキュリティの侵害またはそのおそれがある場合には速やかに調査の上その状況をシステム委員会に報告しなければならない。

(3) 特別な権限の利用は、制限されなければならない。

(4) 利用者のアクセス制限は、定期的に見直されなければならない。

### 2) 運用責任者の責任

(1) 情報システムのサービスへのアクセスには、運用責任者が正式に利用者登録および登録解除の手続きがされるように管理しなければならない。

(2) 利用者のパスワードは、暗号されたパスワードによって安全に管理されなければならない。

### 3) 利用者IDとパスワード管理

(1) 利用者は、初期登録時において運用責任者より配布されたパスワードを一時利用し、自らパスワードの変更操作を行われなければならない。

(2) 自分のパスワードは、決して他人または他のグループに口外しない。

(3) パスワードを紙などに記述して記録しない。

- (4) パスワードはファンクションキーなどに記録しない。
- (5) パスワードには、推測可能な用語を設定してはならない。
- (6) パスワードは英数字、大文字・小文字記号が混在するランダムな13桁以上とする。
- (7) パスワードは使いまわしをしてはいけない。

(パスワードの禁則)

- ① 年月日、曜日、その他の日付に関すること
- ② 姓名、名字、イニシャル、ニックネームなど
- ③ 医療機関名、部署名、それらに関するもの
- ④ 電話番号やそれに類似するもの
- ⑤ ユーザ識別子、ユーザネーム、グループID、他のシステム識別子

9. システム委員会の管理項目

法的に利用される電子カルテ情報に出力する装置の管理（運用責任者および管理責任者）は以下の項目について

管理する

- 1) 法的に利用される電子カルテ情報を出力するシステムは、常に情報が出力されるように管理する。
- 2) 少なくとも法的な要求される期間は、電子カルテ情報の出力が保証されるように維持、管理する。

10. 事件または異常事象の報告

(1) 運用責任者は、情報システムの異常が報告された場合あるいは確認された場合は、速やかにシステム管理責任者、監査責任者および厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室へ報告し、異常事象への必要な対処処置を取らなければならない。

医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先  
医政局・医療情報担当参事官室  
TEL: 03-6812-7837  
MAIL: igishitsu@mhlw.go.jp

医療法人以和貴会のネットワーク接続実施拠点へ影響が想定される異常事象が確認された場合は、速やかに運用責任者は、ネットワーク接続拠点のシステム管理責任者にその内容を連絡し、ネットワーク接続実施拠点への影響を及ぼさないように必要な対処処置を取らなければならない。

(2) 運用責任者は、必要に応じ、事件または異常事象の発生の状況・原因・対応処置に関するレポートを作成し委員会に報告しなければならない。

医療法人以和貴会のネットワーク接続実施拠点へ影響が想定された事件または異常事象の発生状況・原因・対応処置に関するレポートを必要に応じて作成し、ネットワーク接続拠点のシステム管理責任者に報告しなければならない。

#### 1 1. 教育・訓練

新たに情報システムを利用することになった利用者に対し、使用方法についてカリキュラムを編成し、操作方法の習熟に努めなければならない。

#### 1 2. マニュアル整備

運用責任者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に使用可能な状態に置く。

## 第6章 利用者マニュアル

### 1. はじめに

本マニュアルは、西崎病院情報システム（以下「情報システム」という。）を安全に管理、運用するため、システム委員会（以下「委員会」という。）が定めた「電子保存に関する管理規定」（以下「管理規定」という。）を基に、当病院の情報システム利用者

が注意すべき事項を定めたものである。従って、情報システムの利用者は、本マニュアルならびに「管理規定」および「管理者マニュアル」を遵守して、診療情報の漏洩、改ざん、破壊などが発生しないように、安全に情報システムを利用しなければならない。利用者権限は、情報システムを利用する上で、利用資格の識別およびプログラムやデータファイル等への不正アクセスを制御し、データ変更等において利用者の真正性を高めることを目的とし、利用者情報区分によりアクセス権を設定するものである。

## 2. 情報システムの利用

情報システムは、事務部総務課または業務の責任者が申請書を運用責任者に提出した情報を元に、利用者権限の付与・登録された者のみ利用できるものとする。

## 3. 義務と懲罰

- (1) 情報システムの利用者は、本ガイドラインに則して情報システムを利用しなければならない。
- (2) 患者のプライバシーを侵害しないことを目的として情報システム上の情報については守秘義務を負わなければならない。
- (3) 与えられたアクセス権限を越えた操作を行わないこと。
- (4) 参照した情報を、目的以外に利用しないこと。  
違反した場合は、懲罰を課されるものとする。

## 4. 情報システムの利用時のセキュリティ

### 1) 利用時の画面管理および就業時間外の情報システムの利用内容報告

- (1) 端末利用中に席を外す場合には、他の者にそのまま自分の権限で端末を利用されないよう、必ず処理をログオフする。ログオフ処理をせずに席を外した場合、その間行われた不正行為について、ログオフ処理せずに席を外した利用者の責任とする。
- (2) 利用者は、端末の利用を終了する場合には業務終了処理を行い、ログオフ状態にななければならない。
- (3) 利用者は、勤務時間外に情報システムを利用した場合、利用内容の報告を業務の管理者に行わなければならない。
- (4) 利用内容を報告しない場合は、ただちに運用責任者または事務当直者に連絡し指示を受ける。

### 2) 病院が定めた職員証の着用

- (1) 情報システムを利用できる端末が設置してある場所では、必ず病院が定めた職員証を着用しなければならない。
- (2) 身近に非着用がいた場合、ただちに運用責任者に連絡し指示を受ける。

## 5. 情報システム運用管理面でのセキュリティ

### 1) 設備について

利用者は、運用責任者が許可した装置以外で情報システムを利用してはならない。ま

た、運用責任者が許可した装置からアラートメッセージが出力された場合には、速やかに運用責任者に届けなければならない。

## 2) ドキュメント管理

- (1) 重要度の高いドキュメントや帳票のコピーや持ち出しは、業務の責任者の許可を得なければならない。
- (2) 診療記録のハードコピーなど重要度の高いドキュメントや帳票が不要になった場合には、速やかにシュレッダーで破砕する。
- (3) 重要度の高いドキュメントや帳票は、鍵付きのキャビネットまたは施錠した部屋(保管庫も含む)に保管する。

## 6. 電子カルテシステムの利用時のパスワードセキュリティ

1) パスワードセキュリティ情報システムの利用者は、パスワードセキュリティの侵害またはその恐れがある場合には、速やかに運用責任者に報告しなければならない。

### 2) パスワードの利用の責任

利用者は、パスワードの選定および使用に際しては、本ガイドラインに従わなければならない。パスワードを失念した場合あるいは漏洩した可能性がある場合には、速やかに運用責任者は監督責任者に届けなければならない。

## 3) 利用者IDとパスワード管理

- (1) 利用者は、初期登録時において運用責任者より配布されたパスワードを一時利用し、自らパスワードの変更操作を行われなければならない。
- (2) 自分のパスワードは、決して他人または他のグループに口外しない。
- (3) パスワードを紙などに記述して記録しない。
- (4) パスワードはファンクションキーなどに記録しない。
- (5) パスワードには、推測可能な用語を設定してはならない。
- (6) パスワードは英数字、大文字・小文字記号が混在するランダムな13桁以上とする。
- (7) パスワードは使いまわしをしてはいけない。(パスワードの禁則)

① 年月日、曜日、その他の日付に関すること

② 姓名、名字、イニシャル、ニックネームなど

③ 医療機関名、部署名、それらに関するもの

④ 電話番号やそれに類似するもの

⑤ ユーザ識別子、ユーザネーム、グループID、他のシステム識別子

⑥ パスワードの失念した場合の再発行は以下の手順による。

⑦ 運用責任者あるいは監査責任者に連絡する

⑧ 運用責任者に連絡をし、運用管理者はパスワードの変更をする

⑨ パスワードの確認を行う

## 7. 法的に利用される電子カルテ情報の管理

- (1) 法的に利用されるデータと署名データについては、法的に求められる期間保管して

おく。

- (2) 利用されるデータと署名データを、可搬記憶媒体で保管する場合には、施錠したキャビネットまたは施錠した部屋で管理しなければならない。また、用紙で保管する場合も同様の取扱いによって管理する。

#### 8. 事件または異常事象の報告

情報システムに何らかの異常が検出あるいは疑われた場合、直ちに当該職員が所属する業務の管理者及び運用責任者に異常事象を報告する。

##### (1) コンピュータウイルス感染時

情報システム端末がコンピュータウイルスに感染したことを認めたときは、直ちに当該情報システムの利用を中止するとともに、当該職員が所属する業務の管理者及び運用責任者に報告し、その指示に従わなければならない。

#### 9. 教育・訓練

新たに情報システムを利用することになったものは、情報システムの利用する前に、教育訓練を受けシステムを使用しなければならない。

## 第7章 医用画像運用・保守管理

### 1. 画像情報の確定操作と作成責任者の記録

画像診断に関わる検査において、検査実施者をオーダーリングシステムにおいても同一者とし、検査実施者は検像システムもしくは画像診断装置（以下モダリティ）にて画

像確定操作を行い、画像サーバに送信する。

## 2. 画像管理責任者

PACS 画像管理システムにて管理者権限を付与された者を指し PACS システムに於いて読影権限の付与、画像情報の修正、削除、画像表示モニターの管理、ID、パスワードの付与などを行う事が出来る。尚、システム管理者（システム管理部職員）も管理者権限を付与する。

## 3. 検像

・検像システムが接続されているモダリティは検像システムにて修正、確定操作を行う。検像システムが接続されていないモダリティに於いては各モダリティ上で検像作業を行い、画像サーバに送信する。その際、確定操作者（検査実施者）は以下の画像情報、画像付帯情報を原則確認しなければならない。

患者情報 患者 I D

患者氏名

年齢

性別

依頼情報 依頼科

依頼医師

検査目的

依頼時病名

画像情報

モダリティ名部位

画像数

画像シリーズ数

画像表示順序

撮影線量\*（X線一般撮影のみS値としてチェックする）

画像表示 濃度 コントラスト表

示方向

マーク

## 4. 時刻同期

検査を実施した結果、得られる診断の根拠となるべき画像情報は、保存行為が確定操作に当たる行為になる為、信頼出来る時刻源を用いた作成日時が記録に含まれている必要がある。検査撮影装置や PACS で時刻同期が取られている事が必要であり、時刻同期を担保するものとする。

## 5. 可搬媒体、フィルムでの画像出力、取り込みについて

5.1 持ち込まれた可搬媒体の取り扱い持ち込まれた可搬媒体は、本来患者の所有物である為、原則患者に返却するものとする。又、破棄する場合は、厚生労働省ガイドライン 6.7 に従

い、シュレッダーにて破断するものとする。 5.2 画像情報の取り込みと作成責任者外部の医療機関から持ち込まれた可搬媒体、フィルムの画像情報を当院サーバに取り込む際、取り込み作業を行う者を作成責任者とする。又、取り込み依頼は当該医師がオーダーリングにて行うものとし、これを放射線情報システムにて当該作成責任者が実施操作を行う事により責任の所在を担保するものとする。 5.3 画像付帯情報の修正について持ち込まれた可搬媒体を当院サーバに取り込む際、画像付帯情報修正箇所は患者IDとする。

- ・画像出力

CD、DVD などその他の可搬媒体及びフィルムで画像出力を行う場合には、オーダーリングシステムにより、依頼情

報を入力し実施履歴を管理するものとする。又、受け渡し担当者も実施履歴で管理する。

- ・画像取り込み

CD、DVD などその他の可搬媒体で画像取り込みを行う場合は、画像出力手順同様にオーダーリングシステムにて依頼情報、実施履歴を管理する。

- ・可搬媒体の個人情報保護

可搬媒体中の個人情報保護に於いては医療法人以和貴会西崎病院 個人情報保護規則に則り取り扱うものとする。

## 6. 画像情報の保存期間と画像圧縮

診療完結の日から10年間は可逆圧縮にて保存を行う。

診療完結の日から10年間を経過した画像情報は非可逆圧縮にて保存若しくは削除を行う。但し、これにより当該患者が不利益を被る事が予想される場合には、これを適用しない。