○国保京丹波町病院医療情報システム運用管理規程

平成 22 年 4 月 1 日
告示第 16 号

(目的)

第 1 条　この規程は、国保京丹波町病院(以下「本院」という。)における、医療情報システム(以下「システム」という。)の安全かつ合理的な運用を図り、併せて、法令に基づき保存が義務づけられている診療録(診療諸記録を含む。以下「保存義務のある情報」という。)の電子媒体による運用の適正な管理を図るために、必要な事項を定めるものとする。

(法令等の遵守)

第 2 条　システムの利用にあたっては、京丹波町個人情報保護条例(平成 17 年京丹波町条例第 10 号)を遵守するほか、この規程の定めるところによる。

(定義)

第 3 条　本規程の対象とするシステムは、電子カルテシステム及び電子カルテシステムと接続する各部門システム機器及び医事会計システムのことをいう。

2　システムは、次の各号に掲げる基本原則に則り運用する。

(1)　保存義務のある情報の電子媒体による保存については、情報の真正性、見読性、保存性を確保する。

(2)　システムの利用にあたっては、守秘義務を遵守し、患者個人の情報を保護する。

(3)　システムへのコンピュータ・ウィルスの進入及び外部からの不正アクセスに対しては、必要な対策を直ちに講じる。

(システムの管理体制)

第 4 条　システムの管理者(以下「システム管理者」という。)を置き、病院長あるいは病院長が指名した者を充てる。

2　病院長は、システムを円滑に運用するため、システムに関する運用を担当する責任者(以下「運用責任者」という。)を置く。

3　システムに関する取扱い及び管理に関し必要な事項を審議するため、国保京丹波町病院医療情報システム管理運営委員会(以下「管理運営委員会」という。)を置く。

4　管理運営委員会に関する事項は別に定める。

(システム管理者)

第 5 条　システム管理者は、システムの管理・運営を統括し、次の各号に掲げる任務を行う。

(1)　システムに用いる機器及びソフトウェアを導入又は更新する場合は、当該機器及びソフトウェアの機能がこの規程に適合することを確認すること。

(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こと。

(3)　保存義務のある情報として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置くこと。

(4)　機器やソフトウェアが更新された場合においても、情報が継続的に利用できるように維持すること。

(5)　システム利用者の登録を管理し、そのアクセス権限を規定するとともに、不正な利用を防止すること。

(運用責任者)
第 6 条　運用責任者は、次の各号に掲げる任務を行う。
(1)　システムを安全で合理的に運用し、運用上に問題が生じた場合は、速やかにシステム管理者に報告する。
(2)　利用マニュアル及び仕様書等を整備し、必要に応じて速やかに利用できるよう各部門に周知する。
(3)　システムの有効活用を図り、機器の配置及び利用について決定する。
(4)　利用者に対して、システムの安全な運用に必要な知識及び技能を研修する。
(5)　システムと外部システムとのデータの連携に関して、システム管理者の承認を得る。

(利用者の定義と責務)
第 7 条　システムを利用できる者は、次のいずれかに掲げる者で、システム管理者が利用を許可した者とする。
(1)　本院の職員で診療、事務等の業務に従事する者
(2)　本院の業務の委託を受けた者
(3)　その他病院長が必要と認めた者
2　システムの利用にあたっては、別に定める様式に従い、システム管理者に対して利用申請を行い、利用者認証に関する情報(以下「ID 及びパスワード」という。)を取得し、利用許可を得るものとする。
3　利用者は、次の事項を遵守しなければならない。
(1)　自身の ID 及びパスワードを自らの責任において管理し、これを他者に利用させてはならない。
(2)　システムの利用に際して、ID 及びパスワードによって自身を認識させること。
(3)　参照した情報を目的外に利用しないこと。
(4)　患者のプライバシーを侵害しないこと。
(5)　システムの異常を発見した場合は、速やかに運用責任者に報告し、その指示に従うこと。
(6)　不正利用を発見した場合は、速やかに運用責任者に報告し、その指示に従うこと。

(主要機器の管理)
第 8 条　システム管理者は、システムに係る主要機器を独立した電算機室に設置する。
2　電算機室の出入り口は常時施錠し、運用責任者がその入退室を管理する。
3　運用責任者は、設置機器を定期的に点検する。

(システムの監査)
第 9 条　システムの運用が安全かつ合理的に行われているかを監査する必要がある場合、システム管理者が監査責任者を指名し、監査を依頼することができる。
2　監査責任者は、監査結果をシステム管理者に報告し、問題解決の改善策を提案するように努める。
3　監査の結果、問題があった場合には、管理運営委員会の審議を経て別途管理者が定める。

(雑則)
第 10 条　この規程に定めるもののほか、システムの運用管理に関し必要な事項は、管理運営委員会の審議を経て、システム管理者が別に定める。
附　則
この告示は、平成 22 年 4 月 1 日から施行する。

国保京丹波町病院
医療情報システム
運用管理内規（第２版）

目次

(別紙)

・マスタ追加・変更申請書（運用内規第３章－２－（４）－③）
・利用者登録申請書（第５章－２－（４）－②）
・可搬記憶媒体使用申請書兼診療データ二次利用申請書（第９章－５－（２）－②）

第１章　医療情報システムに関する基本目標

１　理念

(1)　医療情報システムの管理者及び利用者は、保存義務のある情報の電子媒体による保存が、自己責任の原則に基づいて行われることをよく理解しておかなければならない。

(2)　電子保存された保存義務のある情報の真正性、見読性、保存性を確保し、かつ、情報が患者の診療や病院の管理運営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。

(3)　医療情報システムの管理者及び利用者は、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。

【自己責任の原則】

自己責任とは、当病院が運用する医療情報システムについて、どういう方法によって電子保存のための条件を満たしているか第三者にわかるように示す『説明責任』、運用方法が決められたとおり、実行できるように運用管理を行う『管理責任』、決められた運用方法が後になって、電子保存のための条件を満たしていなかった、又は適切に運用できていなかったことによる第三者に対して損失を与えた場合の責任を当病院が負う『結果責任』を果たすことを意味する。

【真正性･見読性･保存性の原則】

『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。など、“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、訴訟等に際して、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。

第２章　目的

この内規は、当病院において、法令に保護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。)並びに医事会計記録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「医療情報システム」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に資することを目的とする。

また、ここに規定する原則とそれに基づく各種運用マニュアル等は、すべてネットワークを介して行われる業務を前提とし、今後想定する院外の専用線等を介して持ち込まれる医療関連情報も綴集･付加されるものとする。

１　電子カルテ運用開始

○電子カルテシステム使用開始日：平成２８年２月１日（月）

※稼働日以前のデータについては、前電子カルテシステム「ｅ－ｃｌｉｎｉｃ診療支援システム」より、平成２８年２月１日現在の更新凍結状態の診療録２号紙の全データ（ＰＤＦ形式）を保存した。

※稼動当初の過去の診療録については、前電子カルテシステム「ｅ－ｃｌｉｎｉｃ診療支援システム」の閲覧により補完する。

２　診療情報管理システム使用開始

○診療情報管理システム使用開始日：平成３０年１１月２０日（火）

※主として、診療録管理体制加算算定のため、診療情報管理システム（Ｍｅｄｉ－Ｂａｎｋ　Ｌｉｇｈｔ）の運用を開始した。

第３章　管理体制

１　医療情報システムの管理体制

この章では、国保京丹波町病院医療情報システム運用管理規程（平成２２年告示第１６号）第４条に規定する医療情報システムの管理体制を定める。

２　医療情報に係るシステムの管理者

(1)　医療情報に係るシステムの管理者の情報管理に関する責務

①　当病院に医療情報に係るシステムの管理者(以下「システム管理者」という。)を置き、病院長をもって充てる。また、副管理者として副院長及び事務局長を充てる。

②　システム管理者は、電子保存に用いる器機及びソフトウェアを導入するに当って、システムの機能を確認し、これらの機能が「法令に保存義務が規定されている診療記録及び診療諸記録の電子媒体による保存に関するガイドライン」に示される各項目に適合するよう留意すること。

③　システム管理者は、「医療情報システム安全管理基準」と「セキュリティ方針書」を作成し、さらに効率的に運用するために「情報管理をする組織」として医療情報システム管理運営委員会を設置する。

④　システム管理者は、情報の共有化を図るとともに、共有化によって起こる各種情報の漏洩防止のためにその「セキュリティ権限付与」を設定し常に管理しなければならない。

⑤　システム管理者は、医療情報システムを利用するために必要な「運用内規」を設けなければならない。

⑥　システム管理者は、医療情報システムを円滑に運営し、医療情報システム全体の管理状況を把握しなければならない。

⑦　システム管理者は、医療情報システム管理運営委員会の責任者等を選任するとともに、同委員会から協議内容について随時報告を受けるものとする。

３　運用責任者

運用責任者は、看護部長及び各部門から選出した若干名で構成する。

4　医療情報システム管理運営委員会

(1)　構成委員

①　医療情報システム管理運営委員会の委員長は、運用責任者の長である看護部長とする。

②　事務局は、事務室の運用責任者をもって充てる。

③　構成委員は、システム管理者が選任した前２号のほか、各部門の責任者（以下、各部門責任者）をもって構成する。

(2)　委員会の開催

①　　医療情報システム管理運営委員会は、必要に応じて委員長が招集し開催する。

(3)　情報セキュリティ管理

①　医療情報システムに関する取扱い及び管理に関し必要な事項を審議し、システム管理者のもとに医療情報システムを管理するものとする。

②　画面ハードコピーをとった資料など、不要となった診療情報等を安全な方法で、速やかに廃棄・消去することを各部門に指導しなければならない。

(4)　情報マスタ管理

①　医療情報システムに関する取扱い及び管理に関し必要な事項を審議し、システム管理者のもとに医療情報システムを管理するものとする。

②　システム導入業者及びシステム保守管理業者と協調してマスタ管理を行う。

③　医療情報システム利用者（以下、利用者）が必要なマスタ変更等を希望する場合は、マスタ追加・変更申請書（様式１）により所属する各部門責任者を通じて運用責任者へ申請するものとする。

④　委員長は、速やかに申請の可否を判断し、システム管理者に報告するものとする。

(5)　医療情報システムダウン検討

①　医療情報システムが機能しなくなった時でも診療に大きな混乱を来さないための方策を検討し各部門の詳細な対応を定める。

(6)　外部ネットワークや電子媒体の利用制限

①　インターネットを通じた外部ネットワークは利用してはならない。

②　診療情報の受け取りのためにやむをえず CD を読み取る場合は、事前に外部ネットワークと繋がりのない端末でウィルスチェックを行うこと。通常業務のために USB メモリ等は利用してはならない。

(7)　医療情報システム教育

①　医療情報システムの使用について効率的な使用ができるように、利用者に対して、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、教育研修を行うものとし、運用責任者がその実務を担当する。

(8)　システム企画協議

①　医療情報システムの適正な管理・運用を図るため、中長期に係る医療情報システムの改善や随時発生する小規模なシステム改善等を計画的に実行できるよう全体調整を行う。

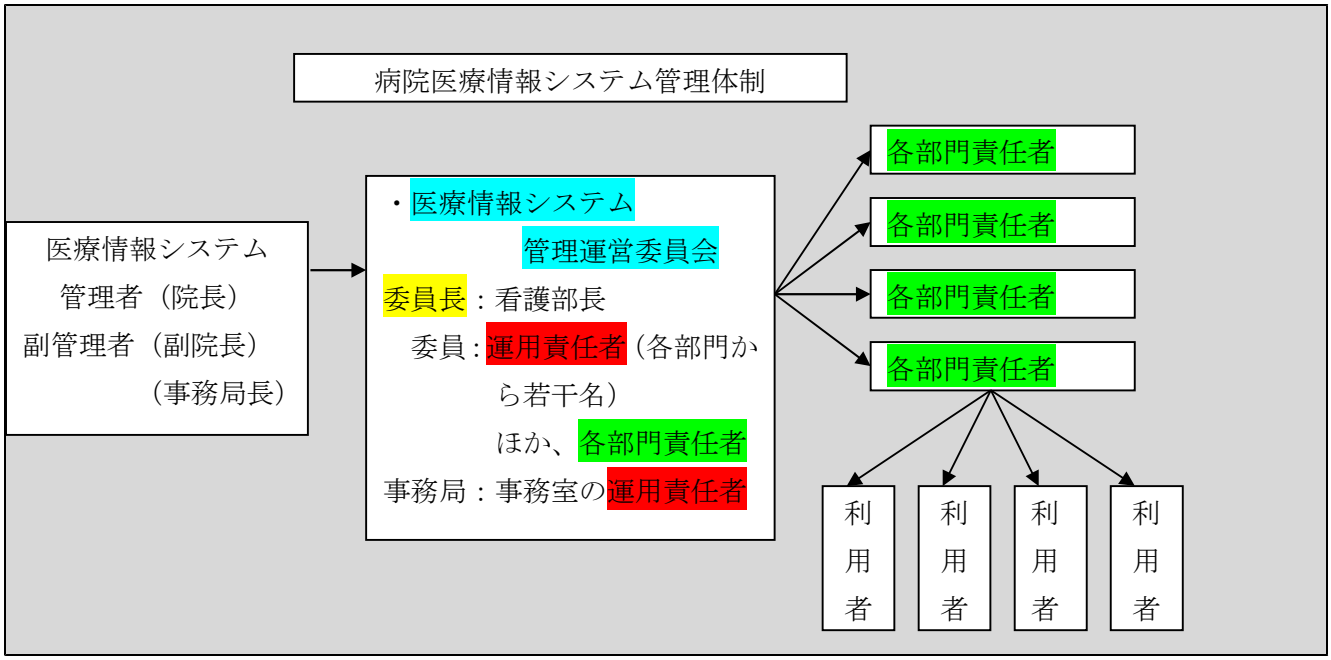
(9)　監査の実施

①　医療情報システムの利用者の端末利用状況を管理するため、端末利用状況をログ情報等によって毎年４回定期的にチェックし、これを広報する。なお、問題点の指摘等がある場合には、直ちに必要な措置を講じなければならない。

②　監査内容については、システム管理者がこれを定める。

③　システム管理者から要請があった場合、定期監査以外に臨時の監査を行うものとする。

【ログ】
　ログとは、電子カルテシステムを中心とした医療情報システムの処理内容や利用状況を、時間の流れに沿って記録したもの、あるいは記録すること。



第４章　電子保存する情報の範囲

１　保存範囲

(1)　当病院において、保存義務のある情報を電子保存する際に対象とする情報の範囲については、「第３章　管理体制　４　医療情報システム管理運営委員会」に規定する医療情報システム管理運営委員会の審議を経て、システム管理者がこれを定めるものとする。

２　保存情報の保護

(1)　医療情報システムの運用並びにそれに関する責任を定めることにより、診療情報等の不適切な取扱いに起因する患者の権利･利益の侵害の防止及び基本的人権の保護と同時に、利用者の情報の共同利用に関する保護を図る。

(2)　当病院の医療情報システムのデータは、別に定める「第７章　医療情報システムのセキュリティ方針書（以下「セキュリティ方針書」という。）」、「第８章　管理者マニュアル（以下「管理者マニュアル」という。）」及び「第９章　利用者マニュアル（以下「利用者マニュアル」という。）」により保護されるものとし、次に定める医療情報システムのデータの保護については、以下のとおりとする。

①　「セキュリティ方針書」（第７章参照）

- 情報の管理や保護のための技術的な対策事項
- システムの利用者や管理者への教育の実施等を定めた「セキュリティガイドライン」を定める。

②　「管理者マニュアル」（第８章参照）

- 医療情報システムの管理者が注意すべき事項を定める。

③　「利用者マニュアル」（第９章参照）

・　医療情報システムの利用者が注意すべき事項を定める。

(3)　電子カルテを中心とした医療情報システムの診療情報を含むデータ及び情報は、機密性、一貫性、可用性の欠如に起因する危害から保護しなければならない。

【機密性】

利用者に対して、その利用者が権限行使できる責任範囲に限り、その権限の条件に従ってデータ及び情報が書き換えられ、あるいは見読できること。

【一貫性】

データ及び情報が正確で完全であり、かつその真正性、保存性が維持されること。

【可用性】

データ、情報、計算システムが、適時に必要な様式に従い、アクセスでき、利用できること。

(4)　電子媒体による保存を認める文書等(法律の適用)

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 年法律第 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 年法律第 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　救急救命士法(平成 3 年法律第 36 号)第 46 条に規定されている救急救命処置録

⑧　保健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等

⑨　保健薬局及び保険薬剤師療養担当規則(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

⑪　診療放射線技師法(昭和 26 年法律第 226 号)第 8 条に規定されている照射録

(5)　利用者は医療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、規程等の存在及びその範囲について適切な知識を得ることができ、管理者はこれらについて周知を図る。

(6)　医療情報システムの保護対策は、他の者の権利及び利益を尊重して提供され、利用する。

(7)　診療情報等の保護のための法律、規則、対策、手続き、規則、技術、管理、組織、運営、教育、法律を含めた範囲で、関連する考え方を考慮に入れて院内の対策等を図る。

(8)　医療情報システムの保護施策の状況は、運用形態、利用形態及び技術の進歩と共に変化するため、診療情報等の保護のための対策、手続き、規則は定期的に再評価する。

第５章　利用者

1　医療情報システム利用者

(1)　利用者の責務

① 利用者自身の認証番号やパスワードを管理し、これを他者に利用させないこと。

② 医療情報システムの情報の参照や入力(以下「アクセス」という。)に際して、認証番号やパスワード等によって、システムに利用者自身を認証させること。

③ 医療情報システムの情報入力に際して、確定操作(入力情報が正しいことを確認する 操作)を行って、入力情報に対する責任を明示すること。

④ 与えられたアクセス権限を越える操作は行わないこと。

⑤ 参照した情報を目的外に利用しないこと。

⑥ 患者のプライバシーを侵害しないこと。

⑦ システムの異常や不正アクセスを発見した場合は、速やかに各部門責任者を通じて運用責任者に連絡し、その指示に従うこと。

2 利用者管理

(1) 利用者管理の目的

利用者権限は、医療情報システムを利用する上で、利用資格の識別及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、または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とする。

(2) 利用者権限の管理

新規	・当病院で採用(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(中止)	・退職又は異動等で医療情報システムに関係の無くなった時
利用者権限変更	・基本的に、医師、看護師、検査技師等の設定がされているが、 業務上、必要な区分が変更になる時

※ 後利用等でデータを作成する際、利用者の関連付けができなくなる為に、登録された利用者 ID は削除しない。

(3) 利用者権限の分類・権限範囲区分

利用者権限は、利用者の職種による分類・権限範囲区分を原則とし、医療情報システム管理運営委員会において別途定める。

(4) 申請・登録・交付・非表示

① 利用者権限の交付は、各部門責任者が医療情報システム管理運営委員会に利用者の申請を提出し、承認を得る必要がある。また、利用者の異動に伴って各部門責任者から非表示申請が出た場合は、事後報告として医療情報システム管理運営委員会に非表示の依頼を出すものとする。ただし、当病院職員に対する利用者権限の交付等については、その者の人事異動に伴い、システム管理者の責任において設定を行う際は申請を必要としない。

② 利用者の登録設定・非表示手続きは、各部門責任者が利用者登録申請書（様式２）に次の項目を記入し、医療情報システム管理運営委員会へ提出する。

ア 申請者の部門、氏名

イ 利用者所属、職種、氏名

ウ 適用開始日

エ 権限付与に関する理由等

③　医療情報システム管理運営委員会は、利用者登録申請書に基づき利用者 ID、利用者区分を記入する。ただし、非表示申請は、各部門責任者の異動連絡で運用責任者に依頼し、事後報告とする。

④　医療情報システム管理運営委員会で承認されれば、利用者登録申請書に基づき交付を行う。

⑤　医療情報システム管理運営委員会は、利用者登録申請書を保管する。

(5)　利用者 ID のパスワードの登録あるいは運用管理については、パスワード管理をする者にあっては「管理者マニュアル」、システムを利用するものにあっては、「利用者マニュアル」に詳述する。

(6)　利用者ログの監査

①　不正アクセスの防止

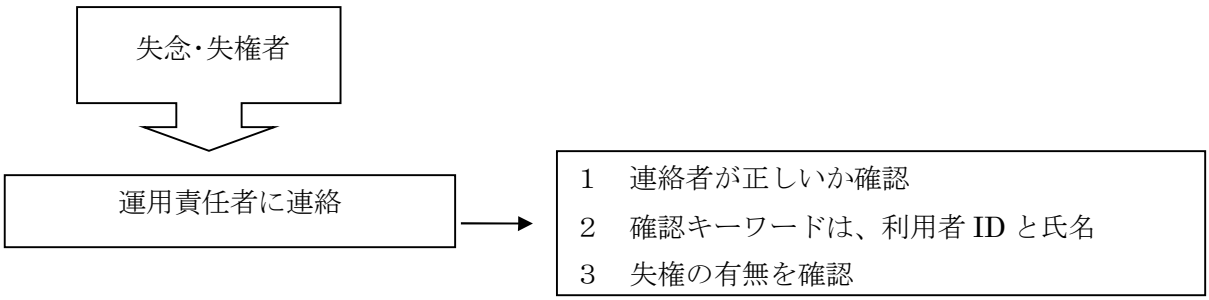
運用責任者は、不正アクセスを防止する為、以下の点を監視する。

・アクセス権の無い者によるデータアクセス

・パスワードの失権状況

②　点検の結果、異常が発見された場合は、その対象の ID･パスワードを使用不可とし、不正使用の防止に努める。

(7)　失念･失権者の復旧手順



3　医療情報システムの機能要件

①　システム内の情報にアクセスしようとする者の識別と認証

②　情報の機密度に応じた利用者のアクセス権限の設定と不正なアクセスを排除する機能

③　利用者入力した情報について確定操作を行うことができる機能

④　利用者が確定操作を行った情報を正確に保存する機能

⑤　利用者が確定操作を行った情報の記録及びその更新に際し、その日時並びに実施者をこれらの情報に関連付けて記録する機能

⑥　管理上又は診療上の必要がある場合、記録されている情報を速やかに出力する機能

⑦　複数の機器や媒体に記録されている情報の所在を一元的に管理できる機能

⑧　情報の利用範囲、更新履歴、機密度等に応じた管理区分を設定できる機能

⑨　利用者が情報にアクセスした記録を保存し、これを追加調査できる機能

⑩　記録された情報のバックアップを作成する機能

第６章　医療情報システム安全管理基準

1　機器の管理

(1)　電子保存された医療情報システムの記録媒体を含む主要器機は、独立した施錠管理が可能な電算機室（以下、「サーバ室」）に設置する。ただし、サーバ室への設置が困難と判断される場合に限り、

当病院職員が 24 時間常駐することを条件として、他の部屋への設置を可能とする。

(2) サーバ室の出入り口は常時施錠し、IC カード等による入退出管理機能を備えると共に、事務室の運用責任者がその入退出記録を管理する。なお、システム機器の搬入出等により、一定時間入退出を繰り返す場合には、当病院職員が必ず作業に立ち会うものとする。

(3) 万が一の災害等発生を考慮して、サーバ室には無水消化装置、漏電防止装置、無停電電源装置等を備える。

(4) 設置するシステム機器は定期的に点検を行う。

2 記録媒体の管理

(1) 品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写し、媒体品質の劣化に伴う記録喪失等の発生を防ぐ。

(2) 記録媒体は、利用者権限で施錠管理された場所において厳重保管し、機密保護に努める。

(3) 破棄データの取扱い

① 記録媒体は、読取り不能の状態にした後に破棄する。

② 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する。

3 ソフトウェアの管理

(1) 運用責任者は、医療情報システムで使用されるソフトウェアを、使用の前に審査を行い、情報の安全性に支障が無いことを確認する。

(2) 運用責任者は、ネットワークや可変型媒体によって情報を受け取る機器について、必要に応じてこれを限定する。

(3) 運用責任者は、定期的にソフトウェアのウィルスチェックを行い、感染の防止に努める。

4 資源管理

(1) システムバックアップ

機器障害や災害などに備えて、システムのバックアップの取得を義務付ける。

復旧が必要な緊急時には、システムサポート会社へ即座に連絡し復旧作業を行う。

① バックアップの形式

ア 正サーバのバックアップとして副サーバを設ける。

イ カルテのバックアップとして参照系サーバを設ける。

ウ 磁気媒体へのバックアップを行う。

② バックアップ対象は、患者におけるカルテ情報データ全てとする。

③ バックアップのタイミング

ア 上記①アについて、常時自動にて、正サーバ／副サーバで同期を取得する。

イ 上記①イについて、毎日自動にて、参照系サーバへの同期を取得する。

ウ 上記①ウについて、毎日自動にて、磁気媒体へのバックアップを取得する。

(2) システムバックアップ媒体の管理手順

① 上記(1)①アイにおける各サーバは、サーバ室にて管理を行い、日々、異常ランプの点灯等を確認する。

② 上記(1)①ウにおける磁気媒体には世代管理を行い、３世代での媒体管理を行う。

③ 上記(1)①ウにおける磁気媒体は個人情報保護に基づき厳密に管理する。

(3) システム資源の容量チェック手順

① システム資源の管理対象

医療情報システム資源を保存する媒体(格納領域)は、容量不足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、システム管理者は、次の項目について日常の利用頻度の確認をしなければならない。

ア データベース格納率の管理

イ 格納先ディスク使用率の管理

5 ドキュメント管理

(1) 取扱い対象

取扱いドキュメントとは、システムプログラム･ユーザーズプログラム･電子カルテを中心とした医療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。なお、申請手続きの無いドキュメントは管理対象外とする。

(2) ドキュメントの保管･管理

① 媒体の場合

磁気媒体に記録されたプログラムドキュメントは、サーバ室の保管金庫に格納し保管する。

※ 磁気媒体は、毎年定期的に利用確認を行い、媒体劣化等の恐れがある場合には、必要に応じて複写を行う。なお、媒体の管理については、2 節で述べた管理手順に従う。

② 帳票の場合

紙に記述されたドキュメントは、サーバ室の保管金庫にファイリングして保管する。

※ ドキュメント類を格納する保管金庫は、常時鍵を閉めて管理する。

6 ネットワーク管理

(1) 医療情報システム管理運営委員会は定期的にシステムの利用履歴やネットワーク負荷等を検査し、通信環境の効率的な運用を維持するとともに、不正に利用された形跡がないか確認する。

(2) 各部門責任者はネットワークの不正な利用を発見した場合には、直ちに運用責任者に報告するとともに、運用責任者と連携してその原因を追求し、再発防止対策を実施する。

7 事故対策

(1) システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるような媒体に保存し管理する。

(2) 医療情報システムのいずれかに障害が発生した場合は、「医療情報システムダウン対策マニュアル」により対応する。

第７章 医療情報システムのセキュリティ方針書

1 方針

当病院において運用する医療情報システムが取扱う情報は不当に暴露されたり、不当に内容が改ざん

されたり、不当に処理が妨害されたりしないように管理及び保護されなければならない。
医療情報システムで処理、保管されているデータに関するいかなる情報も、このシステムに関係のない者には公表しないことを原則とする。

２　目的

本章「第７章　医療情報システムのセキュリティ方針書」（以下「セキュリティ方針書」という。）は、上記１の方針に基づき、情報の管理や保護のための技術的な対策及びシステムの利用者や管理者への教育の実施等を定めた「セキュリティガイドライン」を定めることを目的とする。

３　修正

医療情報システム管理運営委員会は、「セキュリティ方針書」に定められた事項について修正の必要が生じた場合には、速やかに見直しを行うものとする。

４　適用範囲

本セキュリティ方針は、医療情報システムを構成する全ての部分(コンピュータシステムに関連する装置、システムの運用に携わる人、システムの利用者等を言う。以下同じ。)に適用する。
特に、プライバシー情報(診療情報等を含む。)を扱う全ての部分に対しては、運用時の必須要件として本セキュリティ方針を適用する。

５　配布

本セキュリティ方針書は、医療情報システムに関係する全ての者に配布する。

６　医療情報システム管理運営委員会

(1)　セキュリティ方針を実施するため、その実施方法について、その評価や問題点などを検討し、情報セキュリティの保護、管理を行うとともに、病院内で実施される情報セキュリティ対策に矛盾が生じないよう調整を行う。
(2)　業務内容
　①　病院のデータ保護に関する「セキュリティ方針書」の適切な運用とそれに関する責任についての検討
　②　病院の情報財産に対する脅威についての監視と予防対策の検討
　③　セキュリティ対策を実践するための病院長への提言
(3)　業務の実務については、医療情報システム管理運営委員会の責任の下に運用責任者が行う。

７　リスク管理

セキュリティ管理は、セキュリティ対策と保護対象となる情報の価値とのバランスを維持するために、次の点に留意して方針を決定する。
①　医療情報システムのセキュリティ上の想定脅威(発生が懸念される不正暴露、改ざん、処理妨害等)
②　想定脅威に対して、その発生が及ぼす損失とそのセキュリティ対策費用及び利便性を考慮した有効な対策とその速やかな実施

８　プライバシー情報

行政機関の保有するプライバシー情報は「行政機関の保有する電子計算機処理に係わる個人情報の保護に関する法律」(昭和６３年１２月施行)お呼び「京丹波町個人情報保護条例（平成 17 年 10 月 11 日条例第 10 号)」によって法的に保護が義務付けられている。民間の機関に対しては本法律の適用はなされないが、他人の財産を管理し、しかも、一度暴露等の事故が発生すると、取り戻すことができないという情報固有の特性並びに各契約書に基づき、委託先民間企業も含めた医療情報システムに関与するすべての利用者は、その保護に最優先で取り組まなければならないものとする。

９　セキュリティ管理

委員長は、医療情報システムのセキュリティ確保のために各部門から「各部門責任者」を任命するものとする。

１０　責任の分散

セキュリティ管理の責任を分散し、特定の個人に権限と責任が集中して、矛盾を引き起こさないように配慮する。

１１　違反者に対する処置

本セキュリティ方針を含む組織、機関の定めた情報セキュリティに違反した者には、罰則を科する。

１２　診療にかかわる情報のアクセス

診療にかかわる情報にアクセスできる者は、医師及び関連する医療スタッフとし、患者による直接アクセスは、行えないこととする。ただし、医師の判断により診療に必要であると認めた情報を当該患者に開示する場合は、担当医師の責任において行うものとする。

また、患者の要請に基づくカルテの開示を行う場合は、「京丹波町情報公開条例（平成 17 年 10 月 11 日条例第 8 号)」によるものとする。

なお、診療の準備、症例研究、カンファレンス等の目的で診療にかかわる情報にアクセスする場合も同様に、医師の責任において行うものとする。

１３　電子カルテへのアクセス

(1)　通常時の電子カルテへのアクセスは、外来･入院を問わず、受診を希望する旨の根拠となる情報が患者又は患者の代理人の意思により表明され、かつ、患者の登録手続きが済まされていなければ行うことができない。受診者が本人であることが判明しない場合には、患者の診療券の磁気テープ部分もしくはバーコード部分を電子カルテ端末に認識させることにより、確認しなければならない。

(2)　緊急時の電子カルテへのアクセス

①　患者氏名が不詳の場合は、新たに診察券(患者 ID)を作成する。

②　前述の診察券は、新規の ID で作成されるため、患者の重複登録にならないよう作成にあたっては、万全の配慮をしなければならない。

③　患者名が確認できた場合で、従来 ID が存在していたときは、その ID と新規 ID の融合方法を関係部門と調整するための方法を勘案しなければならない。

１４　物理的なセキュリティ管理

自然災害や装置の故障、盗難、破壊等から医療情報システムを保護するために以下の対策を実施する。

① コンピュータ装置本体、ネットワーク管理装置等、電子カルテシステムの処理に重大な影響を与える装置は、盗難、破壊及び関係者外の利用から保護するための物理的な対策を実施する。

② 全装置の一覧表を維持管理し、不正な持ち出し等が発生しないようにする。

③ システム診断用のハード及びソフトの使用は利用目的を限定し、その使用を管理する。

④ 回線は全ての部分で物理的に保護されることとし、定期的に検査する。

⑤ 電源設備の故障による停電等の場合でも、無停電電源供給装置(UPS)等の別系統電源供給によって電力の供給を可能とする。

⑥ 重大な故障又は災害時の業務継続計画(「医療情報システムダウン対策マニュアル」)は、別途定める。

１５ 情報セキュリティ管理

(1) 利用者の識別と認証

① 個々の情報に対し、権限を持っている利用者に対して、その権限の範囲内でのみ利用させるようにするため、利用者一覧を作成し、医療情報システム管理運営委員会にて管理する。

② 利用者は、利用者 ID によって識別し、本人の確認は、パスワードによって行う。

(2) ファイル管理

① ファイル(データベースを含む。)やプログラムを管理しているシステム(以下、「管理システム」という。)あるいは業務上特別な条件下で必要なツールさらに、後利用データベースにおいて患者のプライバシーに影響を与えるデータなどは、運用責任者のみ利用できる。

② システム運用関連及びファイル(データベース含む。)管理関連のプログラムやデータの変更は、運用責任者が事前に変更手続きを行った後に、行うことができる。

③ 管理システムは、運用中は常時、管理者が管理できる状態にしておく。

(3) ネットワークセキュリティ管理

① ネットワークの利用及びネットワークの構成の登録･変更には、事前の手続きを規定し、その規定に基づき実施するようにする。

② 内部ネットワーク(業務で使用するサーバ、無線 LAN 及び端末が接続された病院医療情報システム専用ネットワーク)から、部門システム等を介して外部と通信する場合(リモートメンテナンスに限る。)には、院外のリモートメンテナンス端末の管理方法も把握して許可を与えなければならない。

③ 院内に敷設された外部ネットワークは、内部ネットワークを接続しないものとする。

④ 特に許可された者以外は、院外回線を通じて内部ネットワークを利用できない。

⑤ プライバシーに関係するような重要なデータをネットワーク上で使用する場合は、ネットワーク環境がセキュリティの確保上完全ではないことを考慮した上で使用しなければならない。

(4) 分散管理

① システムを構成する部門サーバ間のセキュリティレベルを統一する。

② 部門サーバ間で一貫したセキュリティ属性の解釈が行えるように管理する。

(5) 電子メール管理

① プライバシーに関係するような重要なデータを、電子メールで送信する場合は、データを暗号化する等、その送信方法について考慮されなければならない。

(6) 監査

① 運用責任者は、情報セキュリティの管理のため監査情報を収集し、それらを監査し、その結果を

システム管理者に報告する。

② 責任者は、常に第三者的立場を堅持して、公正にシステムの不正あるいは改ざんあるいは混同の存在について指摘しなければならない。

③ 監査情報には、利用者(利用者 ID)、利用場所、日時、アクセスした資源名、利用事象のタイプ、アクセスの可否結果を記録しておかねばならない。

④ 監査情報が収められているファイルは、保護されなければならない。

⑤ 運用責任者は、監査情報を少なくとも月 1 回、チェックしなければならない。

⑥ 違反に関する監査記録は、少なくとも 60 日間は保存しておかねばならない。

⑦ 監査ツールの使用は、監査者のみに限る。

(7) データ保存とコンピュータウィルス

① 利用者が持ち込むデータや、システム運用に直接関連するプログラム等重要なプログラムを扱う場合には、利用前にウィルスチェックを実施する。

② ウィルスワクチンプログラムサーバでの一括管理とし、ウィルスワクチンメーカーから新しいプログラムが提供された場合には、各端末に配信するものとする。

③ 利用者は、使用中にウィルス感染の疑いが生じた場合は、運用責任者に連絡するとともに、その指示に従って端末隔離等の処理を行わなければならない。

④ 運用責任者は、障害の状況を分析しウィルスが確認された場合は、その旨を全利用者に通知して注意を喚起し、同時に医療情報システム管理運営委員会に報告しなければならない。

⑤ メディアの管理は、業務の責任者が負うものとする。

(8) 法的に使用される情報の管理

① 法的に使用される電子カルテ情報は、その真正性を確保するように講じられていること。

② 法的に使用される電子カルテ情報の真正性は、操作を行う者の利用者 ID とパスワードで認識させ、操作を行う者が入力した確定情報は、確定入力を動機付けできる画面で構成し、その修正は原本を保存しながら修正データが見読できるように設計されていること。

③ 法的に使用される電子カルテ情報は、法的に求められる期間中保存でき、機器等の新調によるデータの互換性は保持できるものであること。

④ 法的に使用される電子カルテ情報を、保存及び出力するシステムは、法的に求められる期間内は、常に稼動できる状態にしておくこと。

⑤ 法的に使用される電子カルテ情報の所在を明確にし、法的保存期間の情報の開示を求められた場合、速やかに開示できるようにすること。

⑥ 紙面での保存が法的に必要な情報は、その法的根拠が保たれる状態で保存しなければならない。

１６ 運用管理

(1) 運用管理

① システムは、以下の条件に従って適切に管理されなければならない。

ア システムが災害にあった場合の対処方法と復旧方法について手順を明確にし、必要に応じて運用責任者で見直しを実施すること。

イ システムのバックアップを定期的に実施するとともに、バックアップ媒体は、安全な場所に保管されていること。

ウ 機密性の高いバックアップデータは、厳重に保管されていること。

エ 可搬媒体(テープ、ディスク、カセット及びプリントしたレポート等)に関する管理手順を明確

にし、利用者に遵守させること。

オ　システム資源の容量を定期的に確認し、容量不足が予想される場合には速やかに対処すること。

(2)　システム管理

①　利用者の本人確認は、システムの利用を開始する時点で実施する。

②　不正なシステム利用は、許可しない旨の通知を行う。

(3)　システムの運用を適切に管理するために、「管理者マニュアル（第８章)」及び「利用者マニュアル（第９章)」を定めるものとする。

(4)　各部門別において、管理者が必要と認める場合はシステム運用実施細則を定める。

１７　スタッフセキュリティ

(1)　外部委託管理

①　医療情報システムを利用することのできる職員を雇用する委託業者は、当病院で作業する職員に対して十分な利用者教育を行わなければならない。

②　医療情報システムの利用者は、守秘義務と同時に、医療情報システムの構造を熟知して、院外からのアクセスに注意を払わなければならない。

③　部門システムに対して院外からのアクセス手段を有する委託業者は、その構造(仕組み)について事前に運用責任者の許可を得なければならない。

④　部門システムは、部門内でログ管理をし、定期的に、定められた内容で運用責任者に報告、もしくは運用責任者が必要に応じて管理端末から随時ログを確認できるようにしなければならない。

⑤　委託契約の締結に際しては、契約上に職員の情報セキュリティに関する項目を盛り込まなければならない。

(2)　教育･訓練

①　医療情報システムの利用者は、医療情報システムの利用を許可される前にセキュリティ方針及びセキュリティ対策、運用の教育を受けなければならない。

②　セキュリティに理解の乏しい利用者は、セキュリティ方針及びセキュリティ対策の研修を受けなければならない。

③　教育内容には、以下の項目が盛り込まなければならない。

ア　療情報システムの利用者に対する教育

(ア) セキュリティ侵害や情報の漏洩が何によって起きるかを含めた、プライバシー、機密性、完全性、可用性、情報公開及び情報セキュリティの概念

(イ) プライバシー、機密性及びセキュリティに影響を与える情報技術

(ウ) 利用者のセキュリティ管理における個人の責任及び立場による責任範囲の違い

(エ) 診療情報の重要性と、その利用者及び使用用途

(オ) 利用者情報の重要性

(カ) 情報セキュリティに対する想定脅威の種類

(キ) データの保護の方式

(ク) セキュリティ違反の重大さと罰則

(ケ) セキュリティに対する定期的な評価と改良

④　管理者に対する教育

初めて管理者になった者に対する教育は、利用者に対する教育に加えて以下の項目を履修しな

ければならない。

(ア) 情報セキュリティ教育のプログラムを確立するための管理責任

(イ) 「セキュリティ方針書」とその実践を実現、監視、評価するための戦略

(ウ) 全ての利用者に対する情報の取扱い方法･内容

(エ) 情報セキュリティに影響を与える新技術や、セキュリティ計画に影響を与える規制･規則について熟知する責任

(オ) 不適切な情報の漏洩によって発生する法律上の要件や罰則

(カ) セキュリティ侵害時の一貫した対応と訓練

⑤ 医療情報システムを利用するすべてのスタッフは、教育･訓練を受けなければならない。

第８章　管理者マニュアル

1　はじめに

(1) 本章は、医療情報システムを安全に管理、運用するため、システム管理者が定めた国保京丹波町病院医療情報システム運用管理内規(以下「運用内規」という。)及び「第７章　医療情報システムのセキュリティ方針書（以下「セキュリティ方針書」という。)」を基に、医療情報システム管理運営委員会（この章では「管理者」）が注意すべき事項を定めたものである。

(2) 医療情報システム管理運営委員会は、本章ならびに「運用内規」及び「セキュリティ方針書」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、安全に医療情報システムを管理運用しなければならない。

2　医療情報システム管理運営委員会及び各構成委員の職務内容

(1) 本章で規定する医療情報システム管理運営委員会及び各構成委員の職務内容は、以下のとおりとする。

① 医療情報システム管理運営委員会

ア　医療情報システムに関するすべてを統括する。

イ　医療情報システムを利用する可能性のあるすべての職員を把握し、必要に応じて利用者の異動･職種･勤務形態等の登録情報を各部門責任者に通知する。

② 各部門責任者： 各部門の登録申請あるいは異動情報を受けて医療情報システムへのアクセス権限の登録及び変更許可を医療情報システム管理運営委員会に報告する。

③ 運用責任者 : 医療情報システム管理運営委員会の責任の下に、ハードウェア及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。

(2) 各担当者は、権限分散のため兼務しないことを原則とする。

(3) 各構成委員が一利用者として医療情報システムを利用する場合には、「セキュリティ方針書」及び「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、安全に医療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　義務と罰則

各構成委員は、本ガイドラインに則って医療情報システムを管理、運用しなければならない。また、医療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。違反した場合には、罰則を科されるものとする。

4　利用者への指導及び管理

各構成委員は、医療情報システムの利用者に対して、「セキュリティ方針書」及び「利用者マニュアル」を遵守するよう指導、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

(1) 医療情報システム管理運営委員会は、内部ネットワーク及び外部ネットワークを利用する可能性のあるすべての職員を登録し、利用者の異動、退職時には、システム管理者に速やかに利用者権限の設定、変更の依頼を行う。

(2) 医療情報システム管理運営委員会は、各部門責任者から新規利用の申請を受けて、規定に基づき医療情報システムに利用者権限を設定する。

6　ネットワークの利用及び構成の管理

(1) 利用者の管理

① 内部ネットワーク及び外部ネットワークの利用者の申請･登録･変更については、事前に別途手続きを規定し、その手続きに則って実施するようにする。

② 院外からの転送情報は、外部ネットワークのサーバに保存する。

③ 内部ネットワークから外部ネットワークに対してアクセスすることはできない。

④ 定期的に利用者の利用レベルの妥当性のチェックを行う。

⑤ 利用者は、各部門責任者を通じて医療情報システム管理運営委員会へ報告され、利用者権限が付与された後、登録されるものとする。ただし、失念による処理についてはこの限りでない。

(2) ネットワーク構成の管理

① ネットワーク構成の登録･変更については、事前に別途手続きを規定し、その手続きに則って実施するようにする。

② 医療情報システム管理運営委員会は定期的にネットワーク構成をチェックし、必要と判断した場合には、「医療情報システムダウン対策マニュアル」の障害時連絡網に従って対策本部責任者に確認を取り、構成部分を追加･変更･破棄する。

7　院外接続管理

(1) 共通事項

① 内部ネットワークへの院外からの直接のアクセスを禁止する。

② 内部ネットワークに対して、院外からアクセスできる通路を設けることを禁止する。

③ 部門システム等のリモートメンテナンスを含め、院外と接続する場合には、事前に医療情報システム担当と協議し、その構造について許可を得るとともに、管理者の適切な指示のもとに設置しなければならない。

8　利用環境面におけるセキュリティについての管理者の業務

(1) 入退室管理

① 休日･夜間には通常使用されない設置場所の端末については、休日･夜間における医療情報システム利用情報を運用責任者がログ管理するものとする。

② ログは6ヶ月間保存する。

(2) 名札の着用管理

名札の有無により、権限のない者が医療情報システムを利用していないかどうか確認する。

(3) ノートブック型端末の管理

① ノートブック型端末の設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。

② ノートブック型端末は、原則として業務の管理者の管理区域を越えて使用することができない。

9 運用管理面におけるセキュリティについてのシステム資源管理

(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 インフォメーションあるいは情報開示用端末以外は、人の通行の多い場所に設置しない。

③ 定期的にチェックし、機器を厳重に管理する。

(2) 可搬記憶媒体の管理

① 可搬記録媒体(専用ドライブやカードリーダ等の装置を含む。)は、運用責任者が予め許可したもの以外の使用を禁止する。

② 可搬記録媒体の使用にあたって、利用者にウィルス感染を防止するなどの自己管理について十分に指導する。

③ 医療情報システムで利用するCD及びUSBメモリ等のデータの格納媒体で患者のプライバシー及び病院運営上重要なものは、施錠したキャビネット又は施錠した部屋(保管庫も含む。)で管理しなければならない。

(3) ノートブック型端末の管理

ノートブック型端末は運搬が容易なため、可搬記録媒体と同様に管理を行う。

(4) ドキュメント管理

① 患者のプライバシー及び、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、暗号化する等の処置を行う。

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なければならない。

１０ 医療情報システムの利用時のセキュリティ

(1) 運用責任者の責任

① 端末の利用状況

ア 医療情報システムの利用者の端末利用状況を管理しなければならない。

イ 端末利用状況をログ情報によって定期的にチェックし、医療情報システム管理運営委員会に報告しなければならない。

② 運用責任者は、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、又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管理者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。

(2) 各部門責任者の責任

① 医療情報システムのサービスへのアクセスは、各部門責任者が正式な利用者登録及び登録解除(非表示)手続きがなされるよう管理しなければならない。
② 利用者のパスワードは、暗号化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 利用者は、パスワード受理時もしくは直近の変更時から 180 日間の間にパスワードの変更をしなければならない。
④ システム管理者は、利用者の登録状況及び医療情報システムの利用状況を管理し、異動等で利用者外になった者は、速やかに、また、180 日以上利用のない利用者の権限を失権(非表示)させなければならない。また、1 年以上利用のない場合「利用者マスタ登録」を抹消(非表示)しなければならない。
⑤ 漏洩した可能性がある旨の届出があった場合、速やかに当該利用者のパスワードを通常の再発行手続きで再発行するとともに、当該利用者パスワードによる利用履歴のチェック等の調査を医療情報システム管理運営委員会に依頼しなければならない。
⑥ 各部門責任者は、利用者の再発行履歴を医療情報システム管理運営委員会から報告を受けなければならない。
⑦ 医療情報システムのサービスとデータへのアクセス範囲は、業務要件に基づいて管理されるとともに、その利用者の権限付与は業務の管理者が申請し、医療情報システム管理運営委員会が決定し、その管理は、各部門責任者が行う。

(3) 利用者 ID とパスワード管理
① 通常システムにログインする際には、パスワードを利用する。
② 自分のパスワードは、決して他人又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 パスワードをファンクションキーなどに登録しない。
⑤ 自分の利用者 ID とパスワードを他の者に教えることにより、システムの利用権限を他人に貸与しない。
⑥ パスワードは、数字を最低 4 文字以上使わなければならない。
⑦ パスワードには、以下のような推測可能な用語を設定してはならない。(パスワードの禁則)
①年月日、曜日、その他日付に関すること
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、他のシステムの識別子
⑧ 利用者のパスワードは、登録してから 180 日が経過する日まで新しいパスワードに変更する。
⑨ 再登録したパスワードで使用中のものは、継続して使用することができない。
⑩ 利用者パスワードは、一方的に暗号化し認証情報を保護する。

１１ 法的に利用される電子カルテ情報を出力する装置の管理

(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) 少なくとも法的に要求される期間は、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。

１２ コンピュータウィルス対策

医療情報システム管理運営委員会は、ウィルスに感染した旨の届けがあった場合、現状及び感染ルー

トを調査し、速やかに、これへの対処及び予防策を検討、実施し、システム管理者に報告しなければならない。

１３　事件又は異常事象の報告

(1)　医療情報システム管理運営委員会は、医療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、速やかに異常事象への対処措置を取り、システム管理者に報告しなければならない。

(2)　医療情報システム管理運営委員会は、事件又は異常事象の発生の状況･原因･対応措置に関するレポートを作成し、システム管理者に報告しなければならない。

１４　教育･訓練

(1)　医療情報システム管理運営委員会は、新たに医療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、各部門と協調して操作方法の習熟に努めなければならない。

(2)　医療情報システムの利用者に対し、毎年１回、セキュリティ研修を実施し、受講させなければならない。

第９章　利用者マニュアル

１　はじめに

本マニュアルは、医療情報システムを安全に管理、運用するため、システム管理者が定めた国保京丹波町病院医療情報システム運用管理内規(以下「運用内規」という。)及び「第７章　医療情報システムのセキュリティ方針書（以下「セキュリティ方針書」という。)」を基に、当病院の医療情報システムの利用者が注意すべき事項を定めたものである。

従って、医療情報システムの利用者は、本マニュアル並びに「運用内規」及び「セキュリティ方針書」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、安全に医療情報システムを利用しなければならない。

利用者権限は、医療情報システムを利用する上で、利用資格の識別及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　医療情報システムの利用

医療情報システムは、職員名簿の中で、医療情報システム管理運営委員会が承認し、運用責任者が利用者情報とアクセス権限を登録した者のみ利用できるものとする。

３　義務と罰則

医療情報システムの利用者は、本ガイドラインに従って医療情報システムを利用しなければならない。また、医療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。違反した場合には、別途定めるところにより、罰則を科されるものとする。

4　医療情報システムの利用時のセキュリティ

(1)　利用時の画面管理及び就業時間外の医療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、必ずログオフする。ログオフせずに席を外した場合、その間に行われた不正行為については、ログオフ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、初期画面をログオフに移行しなければならない。

③　部屋から全員が退室する場合、最終退室者は各端末の電源を切断し、部屋を施錠しなければならない。

④　利用内容の報告をしない場合には、罰則を科されるものとする。

(2)　名札の着用

①　医療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、必ず名札を誰もが見える所に着用しなければならない。

②　身近に非着用者がいた場合、ただちに各部門責任者に連絡し指示を受ける。

5　医療情報システム運用管理画面でのセキュリティ

(1)　設備の利用

利用者は、業務の管理者が許可した装置以外で医療情報システムを利用してはならない。

(2)　可搬記憶媒体の管理

①　可搬記憶媒体(専用ドライブやカードリーダ等の装置を含む。)は、運用責任者が予め許可したもの以外の使用を禁止する。

②　利用者は、業務上必要な理由(検査機器からのデータ取り込み、他院への診療情報提供など)を除き、可搬記憶媒体を使用して医療情報システムからデータ(臨床研究用画像など)を取得する必要がある場合には、可搬記憶媒体使用申請書兼診療データ二次利用申請書（様式３）により、予めシステム管理者の許可を受けなければならない。また、本記憶媒体を病院外に持ち出しは禁止する。

③　可搬記憶媒体により取得したデータを当病院における診療以外の目的(臨床研究等)で使用する場合には、データの中の個人情報特定部分削除しなければならない。また、可搬記憶媒体の使用後は、データを消去して速やかに返却(CD 等メディアの場合には再利用できないよう裁断等処分)しなければならない。

④　医療情報システムで利用する CD 及び USB メモリ等のデータの格納媒体で患者のプライバシー及び病院運営上重要なものは、施錠したキャビネット又は施錠した部屋(保管庫も含む。)で管理をしなければならない。

(3)　ノートブック型端末の管理

①　ノートブック型端末は運搬が容易なため、可搬記憶媒体と同様の取扱いによって管理を行う。

②　利用者個人の専用端末は、内部ネットワークでは使用できない。

6　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、業務の管理者の許可を得なければらない。

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に保管する。

7 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

医療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又はその恐れがある場合には、規定された手順に基づき、各部門責任者に報告しなければならない。

(2) パスワードの利用者の責任

① 利用者は、パスワードの選定及び使用に際しては、本マニュアルに従わなければならない。

② パスワードの変更を要請した後もパスワードの変更を行わない利用者は、システム管理者によってその利用権限を停止される。

③ 利用権限が停止された利用者は、失念時再登録と同様の登録方法をとる。

④ 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、電話で速やかに運用責任者に届け出なければならない。

⑤ 利用者からパスワードの失念の届を受けた各部門責任者は、運用責任者に連絡をしてパスワードの利用を有効(もしくは再発行)とする。

(3) 利用者 ID とパスワード管理

① 通常システムにログインする際に、パスワードを利用する。

② パスワードを紙などに記述して記録しない。

③ パスワードをファンクションキーなどに登録しない。

④ 自分の利用者 ID と第 1 パスワードを他の者に教えることにより、システムの利用権限を他人に貸与しない。

⑤ パスワードは、数字を最低 4 文字以上使わなければならない。

⑥ パスワードは、以下のような推測可能な用語を設定してはならない。(パスワードの禁則)

ア 年月日、曜日、その他日付に関すること

イ 姓名、名字、イニシャル、ニックネームなど

ウ 医療機関名、部署名、それらに関するもの

エ 電話番号やそれに類似するもの

オ ユーザ識別子、ユーザネーム、グループ ID、他のシステムの識別子

⑦ 利用者のパスワードは、登録してから 180 日が経過する日までに新しいパスワードに変更する。

⑧ 再登録したパスワードで使用中のものは、継続して使用することができない。

⑨ 利用者パスワードは、一方的に暗号化し認証情報を保護する。

(4) パスワードの利用に関する一般的注意事項

① 自分のパスワードは、決して他人又は他のグループに教えない。

② パスワードを紙などに記述して記録しない。

③ パスワードをファンクションキーなどに登録しない。

④ 自動化されたログオンプロセスにパスワードを含めない。

⑤ 自分の利用者 ID とパスワードを他の者に教えることにより、システムの利用権限を他人に貸与しない。

8　法的に利用される電子カルテ情報の管理

(1)　データ入力後、遅滞なく証明装置により署名する。

(2)　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。

(3)　法的に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、鍵付の保管庫に入れるなどして管理すること。また、用紙で保管する場合は、患者毎にファイルして保管庫に保管する。

9　コンピュータウィルス対策

(1)　外部から持ち込んだ CD やフロッピーディスク等の記憶媒体は、フォーマットするかウィルス検査後に使用する。

(2)　市販ソフトウェアは、必ず使用許諾に従って使用する。

(3)　フリーソフトウェアは、運用責任者によって入手経路を確認し、ウィルス検査及び医療情報システムへの影響有無を検査し、検査に合格したもののみを使用する。

(4)　オリジナルプログラムは、ライトプロテクトを施し安全な場所に保管する。

(5)　外部から持ち込んだハードウェア及びは、ウィルス検査を行うか初期化してから使用する。

(6)　ハードウェアや USB メモリ等記憶媒体を共用する場合は、使用者及び利用状況の管理を確実に行う。

(7)　利用者は、端末の再起動もしくはウィルス対策システムの機能によってウィルスワクチンソフトの更新を行う。

(8)　ウィルスに感染した可能性がある場合(ウィルスワクチンソフトから通知があった場合等)には、個人で駆除せず、各部門責任者を通じて直ちに、運用責任者に通知して指示を仰ぐ。

(9)　運用責任者は、解析結果を医療情報システム管理運営委員会とシステム管理者に報告する。

１０　事件又は異常事象の報告

医療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は、直ちに運用責任者に報告するとともに、遅滞なく異常事象に関する報告書を作成して、運用責任者に提出しなければならない。

１１　教育･訓練

(1)　新たに医療情報システムを利用することになった者は、医療情報システムを利用する前に、運用責任者の開催する教育スケジュールで教育研修を受けなければならない。

(2)　医療情報システムの利用者は、毎年１回、セキュリティ研修を受講しなければならない。

第１０章　医療情報システムダウン対策マニュアル

1　はじめに

診療録の電子媒体による保存については、真正性、見読性、保存性の三原則を条件に、病院長の責任(説明責任、管理責任、結果責任)において実施する。その際留意事項として「運用内規」を定めることとしており、「医療情報システム安全管理基準」として、クライアント･サーバ及びネットワークシステムダウン対策を定めることが要求されている。

診療情報の全てが電子カルテに搭載されるため、医療情報システムのダウンには障害の発生部

位により大小の違いはあるもの、予期せざる病院運用麻痺の発生という想定脅威を常に念頭において対応する必要が生じる。このため、医療情報システムのダウンに備えて、システムダウン対策のマニュアル化を行う必要がある。

2　目的

病院に導入されている病院医療情報システムは、病院内高速ネットワーク LAN を経路としたクライアント･サーバシステムであり、電気機器を用いたシステムである以上、システムダウンの発生を想定する必要がある。本マニュアルの作成はシステムダウン時に受診者がスムーズに受診を完了でき、診察情報が滞りなく記載され、伝達されることを目的とする。

3　システム障害の対策対象

システムダウンはメンテナンス、運用責任者の対応等により一定時間後に復旧する。3 時間を越えるシステムダウンは実際上極めて特殊な状況と考えられる。

システムダウン時間内には外来診療、部門診療、救急及び手術部門診療、病棟診療が対策上の対象業務となるが、上記時間内のシステムダウンを考えたとき、救急及び手術部門診療は口頭指示をベースにした運用と事後入力で対応可能である。病棟診療は参照カルテシステム(プライマリー･カルテシステム)より、指示情報を確認できるため、予定された指示は日常診療と同様に運用可能であり、緊急時の指示は口頭支持並びに紙運用と事後入力で対応可能である。

従って、問題とすべき主たる対象は、緊急性を要し、短時間での対応を要求される外来診療とそれに伴う部門診療と考えられる。

4　システムダウン障害区分

(1)　障害区分

システムダウンはその障害部位により、以下の 5 通りに分類する。

①病院医療情報システムサーバ(エントリー･カルテサーバ)ダウン

②部門システムダウン

③参照カルテシステム(プライマリー･カルテシステム)ダウン

④ネットワークシステムダウン

⑤端末ダウン(電気供給の瞬断、停電など)

(2)　トラブルレベルの規定

医療情報システムダウンが最も診療業務に及ぼす影響の強いトラブルであり、基本的には医療情報システムダウンの復旧見込み時間によりレベルを設定する。

レベル	内容	主な対応
0	主サーバがダウンし、従サーバに短時間(10 分以内)で切り換わり、復旧する見込みの場合	一時待機し、復旧後にオンラインアプリケーションを再起動
1	主サーバ、従サーバともダウンし、短時間で復旧する見込みがない場合で、参照カルテシステムが稼動している場合	参照カルテシステムより過去カルテを参照し、紙伝票運用に切り替えて診察を行う
2	ネットワークシステムがダウンしている場合(復旧にかなりの時間を要する)	参照カルテシステムより過去カルテを印刷し、紙カルテ及び紙伝票運用に切

		り替えて診察を行う

※　部門システムダウンについては、診療に及ぼす影響の程度が低い、あるいは範囲が狭いため、紙運用を要求される場合もあるが、診療全体に及ぼす影響は少ないため全てレベル 0 を基本とし、復旧見込み等の状況を判断してレベル 1 を適用する。また、端末ダウン(瞬断、停電など)については、システムダウンとは異なるため、後述する。

※　レベル判断は運用責任者にて行ない、システムダウン時に各関連部署に連絡をする。

5　システムダウン時の基本姿勢

(1)　システムダウンは病院機能の突然の運用麻痺をもたらす非常事態であり、本来の持ち場に必要最小限の人員を残し、とりわけ短時間の早急な対応を要する外来診療を集中的に対応することを原則とする。

(2)　本来提供すべきサービスが、当病院で発生したトラブルのため遅延あるいは提供できない状態にあることを十分に理解し、患者に対して、『ご迷惑をおかけしていますが、全職員が誠意をもって対応していますのでご理解をいただきたい』という心構えで接する。

(3)　レベル 2 のシステムダウンが発生した場合は、病院長を本部長とする対策本部を設置し、本部長、医療情報システム管理運営委員会の協議のもとにマニュアルに沿った指示を決定･発令し、統率のとれた対応を行なう。

(4)　迅速な対応と患者への声掛けが混乱を避ける方法であり、対策本部設置と指示系統の確立、速やかな連絡を徹底する。

(5)　外来への動員体制

①　対策本部の指示を受けた動員可能な病棟看護師は、外来への稼動を行い、外来看護師とともに患者対応(状況説明、患者整理)を行なうものとする。

②　対策本部の指示を受けた動員可能な管理局の職員は、外来への稼動を行い、患者対応や対患者用物品(机、椅子)など準備し、患者誘導を行なう。

6　システム障害時の対応

(1)　医療情報システムサーバ及びネットワークシステムの障害

①　通常、主なサーバがダウン状態に陥っても、従サーバの稼動により通常の診察が継続できるため、従サーバの稼働中に主サーバを復旧することが可能であり、なんら影響を受けない。ただし、主･従サーバともにダウンした場合は、電子カルテへの記載を中断して、運用責任者からの連絡を待つ。運用責任者の確認と判断によってレベル 0 と判断された場合は、10 分以内に再稼動可能となるため、再度、運用責任者からの復旧の連絡を待ち、復旧後に電子カルテシステムを再起動する。また、レベル 1 以上の連絡があった場合は、紙カルテ運用に切り替え、診療業務を再開する。

②　システムダウンの情報が入れば、医療情報システム使用者は、その時点からシステムが復旧するまでの間、システムダウンのレベルにかかわらず端末の使用は中止する。カルテ保存やシステム終了などの処置も一切加えないで待機する。(原因究明のために必要となる)

③　レベル 0 の場合、診療業務については、電子カルテシステムの復旧待ちの体制であり、基本的に外来患者への説明のみで対応をする。

④　レベル 1 の場合、診療業務については、参照カルテシステムにより過去カルテを参照にし、紙カルテ運用にて診療業務を再開し、復旧後、紙カルテにて診察した患者データを事後入力する。

⑤　レベル 2 の場合、各サーバ(診療支援システム、部門システム、医事システム)自体はシステムダウンをしていないが、それを結ぶネットワークに障害があるため各システムの使用はできない状態に陥る障害である。従って、診療業務については、参照カルテシステムにより過去カルテを印刷(サーバ室内で印刷)し、出力した過去カルテを参照して診療業務を再開し、復旧後、紙カルテにて診察した患者データを事後入力する。なお、レベル 2 の場合は、院内に対策本部が設置されるので、対策本部の指示やマニュアルに沿って初動対応を行なうものとする。

⑥　画像系ネットワークダウンの場合は、装置に直接、患者 ID 等必要な情報を入力、撮影を行ない直ちにフィルム化し診療に使用する。その際、画像は撮影を行なった各機器に保存し、復旧後、画像サーバに送信し保存する。

⑦　医事担当課は、システムダウンに備えて紙運用に必要な物品を各部署に配布し、いつでも運用できるよう準備しておく。

準備すべき物品　：　紙カルテ(患者情報･受診歴･診察内容･過去処方)
カルテ記載用紙、事後入力のための記録紙
検査依頼指示伝票(検体検査、生理検査、放射線検査)
処置伝票
処方せん･麻薬処方せん
手書き用検体ラベル　等

⑧ 薬剤部は、システムダウンの通知後 10 分を経過しても復旧のみられない場合は、予約一覧を参照して当日受付患者の受診診療科の前回処方を出力し、各外来に配布する準備を開始する。

⑨ レベル 1 以上の段階で受付に到着した患者については、紙による受付を総合受付で行ない、診察室、担当医、受付時間を明示する受付票を手渡し、診察受付へ誘導する。ブロック受付では、各診察室の予約一覧が準備されているので、手書きで当該患者の受付を行なう。また、総合受付が非常に混雑することが予想されるので、総合受付近くに案内表示をし、机を 2･3 台用意して仮受付所を設置する。

⑩　運用責任者よりシステム復旧の連絡を受けた後に、紙カルテ運用にて行なった診療業務分のデータは当日中に入力を完了する。ダウン時に入力され電子カルテシステム上指示が伝達されていない事項については、調査の上、指示入力依頼があるのでこの点も事後入力する。

⑪ システムダウン時に使用した紙(カルテ 2 号紙、伝票等)については、当該紙が原本となるため、カルテ庫にて厳重に保管する。

(2)　端末ダウン(瞬断、停電など)

①　端末レベルで全端末が同時に使用不可能になる状態としては瞬断や停電が考えられる。停電が発生すると全ての端末において一旦電源が切れる状態になる。しかし、サーバ側は無停電対応となっており、電源が切れることなく稼動しているため、自家発電が起動(1 分以内)して端末への給電が開始された際には、端末の電源を投入し、サーバとの再接続を自動的に開始される。

②　個別端末レベルで使用不可能になる状態としては、ハードウェア障害や画面のフリーズが考えられる。この状態の時は、運用責任者に速やかに連絡をし、端末交換等を含めた復旧作業後に診療業務を再開する。

※　白色コンセントは商用電源のみの系統であり、停電時に自家発電に切り換わらない。一般的には端末やプリンタの電源を白色非常用（常時）と赤色コンセントに接続して設置してあるが、移設や他医療機器利用のために接続コンセントを変更する場合には注意が必要となる。
緑コンセントは非常時（常時）で一番の優先である。

(3)　外部ネットワーク由来の障害対応

外部ネットワークは、電子カルテシステムとは接続のないシステムであり、その障害が診療自体になんら影響を与えないので、本マニュアルでは取扱わないものとする。

第１１章　その他

１　委任

この内規の施行に関し必要な事項は、管理者が別に定める。

附　則

この内規は、平成２８年２月１日から施行する。

この内規は、平成３０年１１月１日から施行する。