済生会松山病院

情　報　シ　ス　テ　ム

運　用　管　理　規　程

第３版　　平成２３年１月

もくじ

第１章　目的

この規程は、済生会松山病院（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、ソフトウェアおよ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、その取扱いおよ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なわれる業務を前提とし、今後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・付加されるものである。

第２章　　管理組織

１　情報システム管理者

１）　情報システム管理者の情報管理に関する責務

⑴　当病院に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。

⑵　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。

⑶　システム管理者は、「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」を設けなければならない。

⑷　システム管理者は、医療職種間で情報を共有する環境を提供するために、その基本をなす「情報システムに関する理念」を作成し、全職員に周知しなければならない。

⑸　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。

⑹　システム管理者は、情報システムを利用するために必要な「運用規程」を設けなければならない。

⑺　システム管理者は、情報システムを円滑に運営し、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。

⑻　システム管理者は、情報システムが常に業務の効率化と円滑化ができるように情報収集し、合理的運営を指針するために適切に、済生会松山病院情報システム委員会（以下「情報システム委員会」という。）に諮問しなければならない。

⑼　システム管理者は、情報システム委員会の責任者等を選任あるいは承認し、同委員会から答申あるいは協議内容について報告を受けなければならない。

２　済生会松山病院情報システム委員会

１）　情報セキュリティ管理

⑴　情報システムに関する取扱いおよ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情報システムを管理するものとする。

⑵　ハードコピーをと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、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。

２）　情報マスタ管理

⑴　ネットワークを介して使用するすべての用語を共有化するためにその関係するマスタを統合管理する。

⑵　システム開発ＳＥと協調してマスタ管理を行う。

３）　情報システムダウン検討

⑴　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。

４）　インターネット

⑴　外部および内部ネットワークを利用して各種情報を病院利用者あるいは院内職員に提供する内容について検討し、編集する。

⑵　外部ネットワークの院内利用者についてその利用者権限を管理し、特に臨床研究情報を個人の端末に保有する職員については、その端末のセキュリティ管理について指導する。

⑶　外部ネットワークのサーバを管理し、ホームページの編集を行う。

５）　情報システム教育

⑴　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、教育研修を行うものとし、医療システム係がその実務を担当する。

6） システム企画協議

⑴ 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。

7） 医療システム係

⑴ 情報システム委員会の実務については、情報システム委員会の責任のもとに医療システム係が行う。

3 監査委員会

1） 監査委員会の責務

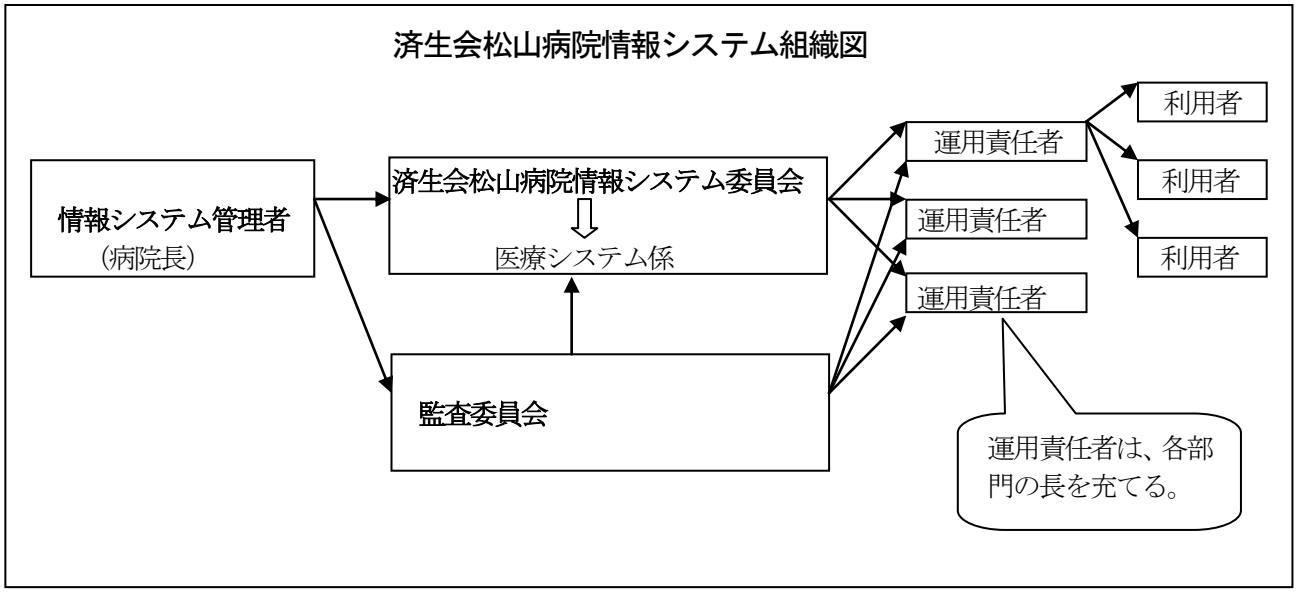
⑴ 情報システムの利用者の端末利用状況を管理しなければならない。

⑵ 端末利用状況を医療システム係がログ情報によって毎年４回チェックし、情報システム委員会に報告し、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３章　　情報システムに関する理念

１　理念

１）　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）　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通り、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１章に規定する情報システム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）　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・利益の侵害の防止およ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）　当病院の情報システムのデータは、別に定める「セキュリティ方針書」、「運用責任者マニュアル」及び「利用者マニュアル」により保護されるものとする。

ここに規定する情報システムのデータ保護の規程等の内容は、以下のとおりとする。

①　「セキュリティ方針書」

ア　情報の管理や保護のための技術的な対策

イ　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」として規定

②　「運用責任者マニュアル」

情報システムの運用責任者が注意すべき事項を規定

③　「利用者マニュアル」

情報システムの利用者が注意すべき事項を規定

３）　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危害から保護されなければならない。

【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）

一 医師法(昭和23年法律第201号)第24条の診療録
二 歯科医師法(昭和23年法律第202号)第23条の診療録
三 保健師助産師看護師法(昭和23年法律第203号)第42条の助産録
四 医療法（昭和23年法律第205号）第51条の2第1項及び第2項の規定による事業報 告書等及び監事の監査報告書の備置き
五 歯科技工士法(昭和30年法律第168号)第19条の指示書
六 薬剤師法(昭和35年法律第146号)第28条の調剤録
七 外国医師又は外国歯科医師が行う臨床修練に係る医師法第17条及び歯科医師法第17 条の特例等に関する法律（昭和62年法律第29号）第11条の診療録
八 救急救命士法(平成3年法律第36号)第46条の救急救命処置録
九 医療法施行規則（昭和23年厚生省令第50号）第30条の23第1項及び第2項の帳簿
十 保険医療機関及び保険医療養担当規則(昭和32年厚生省令第15号)第9条の診療録等

（作成については、同規則第22条）
十一 保険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条の調剤録
（作成については、同規則第5条）
十二 臨床検査技師等に関する法律施行規則（昭和33年厚生省令第24号）第12条の3の書類
（作成については、同規則第12条第14号及び第15号）
十三 医療法（昭和23年法律第205号）第21条第1項の記録（同項第9号に規定する診療に関する諸記録のうち医療法施行規則第20条第10号に規定する処方せんに限る。）、
第22条の記録（同条第2号に規定する診療に関する諸記録のうち医療法施行規則第21条の5第2号に規定する処方せんに限る。）、及び同法第22条の2の記録
（同条第3号に規定する診療に関する諸記録のうち医療法施行規則第22条の3第2号に処方せんに限る。）※
十四 薬剤師法(昭和35年法律第146号)第27条の処方せん※
十五 保険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条の処方せん ※
十六 医療法(昭和23年法律第205号)第21条第1項の記録（医療法施行規則第20条第10号に規定する処方せんを除く。）、同法第22条の記録（医療法施行規則第21条の5第2号に規定する処方せんを除く。）、及び同法第22条の2の記録（医療法施行規則第22条の3第2号に規定する処方せんを除く。）
十七 歯科衛生士法施行規則(平成元年厚生省令第46号)第18条の歯科衛生士の業務記録
十八 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

5） 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、規定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） 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。
7） 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、規則の調和を図るべきである。
8） 情報システムの保護施策の要求は、運用形態、利用形態及び技術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　情報システム利用者

１）　利用者の責務

⑴　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。

⑵　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。

⑶　情報システムの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。

⑷　与えられたアクセス権限を越えた操作を行わないこと。

⑸　参照した情報を、目的外に利用しないこと。

⑹　患者のプライバシーを侵害しないこと。

⑺　システムの異常を発見した場合、速やかに医療システム係に連絡し、その指示に従うこと。

⑻　不正アクセスを発見した場合、速やかに医療システム係に連絡し、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、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	・退職又は異動などで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・看護課長・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）　交付・変更・非表示

⑴　利用者権限の交付は、総務人事係より行う。変更・非表示・利用者権限変更時も総務人事係が行う。

４）　利用者ＩＤのパスワードの運用管理については「利用者マニュアル」に詳述する。

５）　利用者ログの監査

⑴　不正アクセスの防止

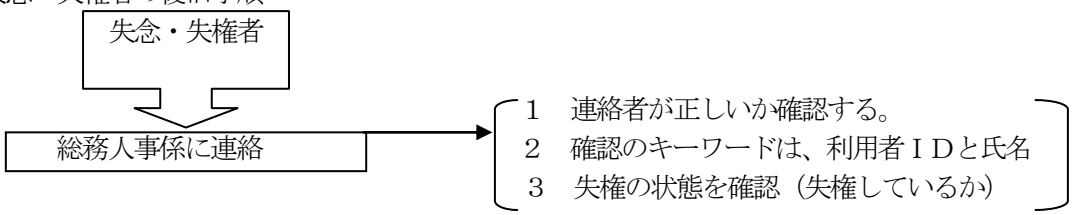
医療システム係は、不正アクセスを防止する為、以下の点を監視する。

ア　アクセス権の無い者によるデータアクセス

イ　パスワードの失権状況

⑵　点検の結果、異常がある場合は、その対象パスワードを使用不可とし、不正使用の防止に努める。

６）　失念・失権者の復旧手順



3　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）　利用者が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　　安全管理

1　機器の管理

1）電子保存された情報システムの記録媒体を含む主要器機は独立した電算室に設置する。
2）電算室はサーバー室内に設置し、入退出を管理する。
3）電算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する。
2）　記録媒体は、利用者権限で施錠監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
⑴　媒体の破棄は、読取り不能の状態にした後、破棄する。
⑵　業務運用上発生する廃棄帳票は、シュレッダーにかけ破棄する

3　ソフトウェアの管理

1）　医療システム係は、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）　医療システム係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）　医療システム係は、定期的にソフトウェアのウイ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／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。

⑴ 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）
⑵ バックアップ対象は、運用に係るすべてのサーバとする。
⑶ 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 オンライン終了時、又はコンピュータ利用が低い時間帯。

２） システムバックアップ媒体の管理手順
⑴ バックアップする媒体には、ボリューム管理を行う。
⑵ 媒体には、世代管理を行い少なくとも３世代の媒体管理を行うこと。
⑶ 媒体の保存管理は、２節で示すデータ管理手順に順ずる。

３） システム資源の容量チェック手順
⑴ システム資源の管理対象
情報システム委員会は、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格納率の管理
② 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
⑴ 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、電算室の媒体保管ロッカーに格納し保管する。この際、ドキュメント管理台帳を作成し、ドキュメントの保存管理を行う。
※ 磁気媒体は、毎年定期的に複写を行う。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。
⑵ 帳票の場合
紙に記述されたドキュメントは、電算室のデータ保管ロッカーにファイリングして保管する。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。
※ 保管ロッカーは、常時鍵を閉めて管理する。

6 ネットワーク管理

１） 情報システム委員会は定期的に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を確認する。

２） 運用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、直ちにその原因を追求し対策を実施する

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）　情報システムのいずれかに障害が発生した場合は、「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　　情報システムのセキュリティ方針書

情報セキュリティ方針

１　方針

済生会松山病院情報システム（ 以下「情報システム」という。）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および保護されなければならない。

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

本セキュリティ方針書は、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

情報システム委員会は、本セキュリティ方針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、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いう。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、情報システムに関係する全ての者に配布する。

６　情報システム委員会

１）情報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

⑴　病院のデータ保護に関する情報セキュリティ方針の適切な運用とそれに関する責任についての検討

⑵　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

⑶　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、情報システム委員会の責任のもとに医療システム係が行う。

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、下記の点に留意して方針が決定される。

1）　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 」（１９８８年１２月施行）によって法的に保護が義務づけられている。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を考え、委託民間企業も含めた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

病院長は、情報システムのセキュリティ確保のために各部門から運用責任者を指名し、情報システム委員会の承認を得る。

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

本セキュリテイ方針を含む組織、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こととする。ただし、患者の要請に基づく全カルテの開示を行う場合は、別に定める「個人情報の保護に関する院内規則」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こととする。

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志により表明され、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。

なお、受診者が本人であることが判明しない場合には、患者の診察カードにより、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

⑴　患者氏名が不詳の場合は、新たに診察カード（患者ＩＤ）を作成する。

⑵　この診察券は、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。
⑶　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や破壊、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およ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（「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
⑴　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、利用者権限チェック表を作成し、運用責任者にて管理する。
⑵　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
⑴　ファイル（データベース含む 。）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、特別に権限を付与された利用者のみ利用できる。
⑵　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、特別な権限を付与された者のみが事前に変更手続きを行った後に、行うことができる。
⑶　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
⑴　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。
⑵　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など）はできないものとする。
⑶　無線ＬＡＮを利用する場合、不正アクセスの対策を施すこと。また利用者以外に特定されないようにし、電波干渉等の対策を施すこと。
⑷　院内の外部ネットワークは、内部ネットワークと接続しないものとする。
⑸　院外回線を通じて内部ネットワークを利用できないようにする。
⑹　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
⑴　部門サーバ間のセキュリティレベルを統一する。
⑵　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

⑴ プライバシーに関係するような重要データを、電子メールで送信する場合は、その送信方法について考慮されなければならない。
⑵ メール発信者、メール内容、メール受信者についての許可範囲は、「利用者マニュアル」に明確に定めるものとする。

6） 監査
⑴ 監査責任者は、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、その結果を医療システム係に報告する。
⑵ 監査責任者は、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。
⑶ 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く。
⑷ 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。
⑸ 監査責任者は、監査情報を少なくとも月１回、チェックする。
⑹ 違反に関する監査記録は、少なくとも６０日間は保存しておく。
⑺ 監査ツールの使用は、監査者のみに限る。

7） データ保全とコンピュータウィルス
⑴ 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。
⑵ ウィルスワクチンプログラムは、サーバでの一括管理とする。
⑶ 利用者は、使用中にウィルス感染の疑いが生じた場合は、医療システム係に連絡する。
⑷ 医療システム係は、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、同時に情報システム委員会に報告しなければならない。
⑸ メディアの管理は、業務の責任者が管理する。

8） 法的に使用される情報の管理
⑴ 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。
⑵ 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て、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。
⑶ 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。
⑷ 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。
⑸ 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。
⑹ 代行入力については、医師の責任のもと看護師又は医師事務作業補助者が行うものとし、必ず代行入力機能を利用し、医師の承認を受けるものとする。代行入力業務内容については、情報システム委員会にて承認を得た業務内容とする。
⑺ 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
⑴ 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。
① 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、必要に応じて医療システム係で見直しを実施すること。
② 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ること。

③　機密性の高いバックアップデータは、厳重に保管されること。
④　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。
⑤　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

⑴　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。
⑵　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、「運用責任者マニュアル」及び「利用者マニュアル」を定めるものとする。

4）　各部門別において、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

⑴　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企業は、職員に十分な利用者教育を行わなければならない。
⑵　情報システムの利用者は、守秘義務と同時に、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。
⑶　部門システムは、部門内でログ管理をし、定期的に、定められた内容で医療システム係に報告しなければならない。
⑷　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。
⑸　清掃等の医療情報システムにアクセスしない作業の場合においても作業後にチェックを行うこと。

2）　教育・訓練

⑴　情報システムの利用者は、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。
⑵　セキュリティに理解の乏しい利用者は、1年に一度、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。
⑶　教育内容には、以下の項目が盛り込まれなければならない。

①　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、その利用者および使用用途
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

②　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　情報セキュリティ方針とその実践を実現、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

⑷　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　運用責任者マニュアル

１　はじめに

１）　本マニュアルは、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済生会松山病院運用管理規程（以下「運用管理規程」という 。）及び「セキュリティ方針書」を基に、当病院の情報システムの管理者が注意すべき事項を定めたものである。

２）　情報システムの運用責任者は、本マニュアルならびに「運用管理規程」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、安全に情報システムを管理運用しなければならない。

２　運用責任者及び情報システム委員会

１）　本マニュアルで規定する運用責任者及びその職務内容は、以下のとおりとする。

⑴　情報システム委員会：情報システムに関するすべてを統括する。

⑵　運用責任者：各部門ごとの情報システムについて運用管理にあたる。

⑶　医療システム係：情報システム委員会の責任のもとに、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。

また、院内の内部ネットワークの利用を管理する。

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、「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情報システムを管理、運用しなければならい。

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。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、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

総務人事係は、内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、退職時には情報システム委員会によって承認された利用者権限に基づき、設定、変更を行う。

６　ネットワークの利用及び構成の管理

１）　利用者の管理

⑴　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。

⑵　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。

⑶　利用者は、ＩＤ・パスワードを交付されてから利用できるものとする。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

⑴ ネットワーク構成の登録・変更については、事前に手続きを規定し、その手続きに則って実施するようにする。

⑵ 情報システム委員会は、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、「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

⑴ 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。

⑵ 内部ネットワークに対して、院外からアクセスできる経路を設けることを禁止する。

8 利用環境面におけるセキュリティについての運用責任者の業務

1） 入退出管理

⑴ 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。

⑵ 管理簿は６カ月保存する。

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

⑴ ノートブック型端末の配置してある部署の業務の責任者は、常に配置台数と使用状況について管理する。

⑵ ノートブック型端末は、原則として業務の責任者の管理区域を越えて使用することはできない。

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

⑴ 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。

⑵ 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。

⑶ 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

⑴ 可搬記憶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。

⑵ ウィルス管理は、内部ネットワークに接続されている情報システムの端末機については自動チェックがかかる。ウイルスの感染アラームの表示された媒体は、業務の管理者が電算室に持参する。

⑶ 情報システム上で使用する可搬記憶媒体は、定期的にチェック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、可搬記憶媒体と同様に管理を行う。

4） ドキュメント管理

⑴ 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考慮する。

⑵ 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　情報システムの利用時のセキュリティ

１）　監査責任者の責任

⑴　端末の利用状況

①　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。

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、情報システム委員会に報告し、これを広報する。

⑵　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、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委員長に報告しなければならない。

⑶　特別な権限の利用は、制限されなければならない。

２）　運用責任者の責任

⑴　情報システムのサービスへのアクセスには、運用責任者が管理しなければならない。

⑵　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。

⑶　利用者パスワードの有効期間は６０日間とし、利用者は、有効期間内に速やかにパスワードの変更をしなければならない。

⑷　システム管理者は、利用者の登録状況及び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。

⑸　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（期限前のパスワード更新）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、情報システム委員会に依頼しなければならない。

⑹　運用責任者は、利用者の再発行履歴を情報システム委員会から報告を受けなければならない。

⑺　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。

3）　利用者ＩＤとパスワード管理

⑴　利用者は、初期登録時において配布された中のパスワードを一時利用し、有効期限までに自らのパスワードを設定する。（有効期限：翌日午前０時）

⑵　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。

⑶　パスワードを紙などに記述して記録しない。

⑷　パスワードをファンクションキーなどに登録しない。

⑸　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。

⑹　パスワードは、以下の条件で付与する。

①　パスワードに使用するキャラクタは、アルファベット（大文字・小文字）、数字をそれぞれ最低限１文字以上用い８文字以上３２文字以下で使用する。

②　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。

⑺　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

⑻　利用者のパスワードは、登録してから有効期限の６０日が経過する日までに新しいパスワードに変更する。

⑼　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。

⑽　パスワードの通常変更は、以下の手順による。

①　パスワード変更ボタンによる操作で変更を可能にする。

②　有効期限が経過する日の２週間前よりアラーム表示を行い、変更可能とする。

ただし、変更処理を行われなくても処理を続行できるよう『ＯＫ』ボタンを用意する。

③　パスワード変更は、パスワード変更ツールにて処理を行うが、新パスワード反映は翌日以降となるため、当日中は現パスワードで運用するものとする。

⑾　パスワードの失念再発行は以下の手順による。

①　総務人事係に電話連絡をする。

②　総務人事係は、失念者のパスワードを確認し、失念者に連絡する。

⑿　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　コンピュータウイルス対策

情報システム委員会は、ウイ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）　情報システム委員会は、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）　情報システム委員会は、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）　情報システム委員会は、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、各局と協調して操作方法の習熟に努めなければならない。

２）　情報システムの利用者に対し、毎年１回、セキュリティセミナーを実施し、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、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済生会松山病院運用管理規程（以下「運用管理規程」という 。）及び「セキュリティ方針書」を基に、当病院の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、情報システムの利用者は、本マニュアル並びに「運用管理規程」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　情報システムの利用

情報システムは、職種・業務内容により情報システム委員会によって承認された利用者権限に基づき、利用者権限の付与を決定し、登録された者のみ利用できるものとする。

３　義務と罰則

情報システムの利用者は、本ガイドラインに従って情報システムを利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。

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　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情報システムの利用内容報告

⑴　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。ログオフ処理を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、ログオフ処理せずに席を外した利用者の責任とする。

⑵　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。

⑶　部屋から全員がいなくなる場合、最終退室者は端末の電源を切らなければならない。また、部屋の施錠をしなければならない。

⑷　利用者は、就業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。

⑸　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

⑴　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。

⑵　身近に非着用者がいた場合、ただちに運用責任者に連絡し指示をうける。

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、業務の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。

２）　可搬記憶媒体の管理

⑴ 利用者は、業務上必要な理由により、情報システムで可搬記憶媒体を利用する場合には、業務の責任者の許可を受けなければならない。
⑵ 情報システムで利用する磁気テープ（MT）及びフロッピーディスク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

⑴ 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。
⑵ 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。

4） ドキュメント管理

⑴ 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ならない。
⑵ 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。
⑶ 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。

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

2） パスワードの利用者の責任

⑴ 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。
⑵ 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。
⑶ 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。
⑷ 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
⑸ 利用者からパスワードの失念の届を受けた運用責任者は、総務人事係に連絡をしてパスワードの利用を有効とする。

3） 利用者ＩＤとパスワード管理

⑴ 利用者は、初期登録時において配布された中のパスワードを一時利用し、有効期限までに自らのパスワードを設定する。 （有効期限：翌日午前０時）
⑵ パスワードを紙などに記述して記録しない。
⑶ パスワードをファンクションキーなどに登録しない。
⑷ 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。
⑸ パスワードは、以下の条件で付与する。
① パスワードに使用するキャラクタは、アルファベット（大文字・小文字 ）、数字のそれぞれを最低限１文字以上用い８文字以上３２文字以下で使用する。
② 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。
⑹ パスワードは、以下のような推測可能な用語を設定しない。（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
⑺ 利用者のパスワードは、登録してから有効期限の６０日が経過する日までに新しいパスワードに変更する。

⑻ 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。
⑼ パスワードの通常変更は、以下の手順による。
① 通常は、パスワード変更ボタンによる操作で変更を可能にする。
② 有効期限が経過する日の２週間前より変更可能とする。ただし、有効期限内であれば変更処理を行わなくても処理を続行できるよう『ＯＫ』ボタンを用意する。
⑽ パスワードの失念再発行は以下の手順による。
① 総務人事係に電話連絡をする。
② 総務人事係は、失念者のパスワードを確認し、失念者に連絡する。
⑾ 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
⑴ 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。
⑵ パスワードを紙などに記述して記録しない。
⑶ パスワードをファンクションキーなどに登録しない。
⑷ 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。
⑸ 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。

７ 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。

８ コンピュータウィルス対策

１） 通信回線等を経由しての情報漏出、外部からの不正侵入等の被害を未然に防ぐため、同一コンピュータでの院内・院外配線の切替は行わない。
２） 院外接続のコンピュータ及び外部から取り寄せたデータを院内コンピュータで利用する場合には、ウィルスチェックのソフトを導入し、安全性を確認した上で利用する。
３） 内部ネットワークに繋がる端末機器は、ウィルスワクチンソフトウェアを常駐させる。
４） 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、運用管理者を通じて直ちに、医療システム科に通知して指示を仰ぐ。
５） 医療システム係は、解析結果を情報システム委員会とシステム管理者に報告する。

９ 事件又は異常事象の報告

１） 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、直ちに医療システム科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、医療システム係に提出しなければならない。

１０ 教育・訓練

１） 新たに情報システムを利用することになった者は、情報システムを利用する前に、医療システム係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） 情報システムの利用者は、毎年１回、セキュリティセミナーを受講しなければならない。

第１０章　　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「運用管理規程」を定めることとしており、「情報システム安全管理基準」として、クライアント･サーバー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、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、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

済生会松山病院情報システムは、病院内高速ネットワークＬＡＮを経路としたクライアント・サーバーシステムであり、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、医療システム係の対応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。病棟診療は紙カルテ運用より、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る。緊急時の指示は口頭指示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である。

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通りに分類される。

① 済生会松山病院情報システムサーバー（エントリー・カルテサーバー）ダウン
② 部門システムダウン
③ ネットワークシステムダウン
④ 端末ダウン（瞬断、停電など）

２）　トラブルレベルの規定

レベル設定・・・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、基本的には情報システムダウンの復旧見込み時間によりレベル設定する。

レベル	内　　容	主　な　対　応
0	主サーバーがダウンし、従サーバーへ切り換り短時間（１０分以内）で復旧する見込みの場合	一時待機し、復旧後、オンラインアプリケーション再起動
1	主サーバー・従サーバーともダウンし、短時間で復旧する見込みがない場合	紙カルテ運用に切り替え診察を行う
2	ネットワークシステムダウンの場合（復旧にかなりの時間を要する 。）	紙カルテ運用に切り替え診察を行う

＊　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とする。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。

レベル判断は医療システム係にて行ない、システムダウン時に各関係部署に連絡をする。

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、当方が引き起こ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、情報システム委員会、事務長及び医事課長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
⑴　対策本部の指示を受けた動員可能な病棟看護師は、外来への移動を行い、外来看護師とともに患者対応（状況説明、患者整理など）を行なうものとする。
⑵　対策本部の指示を受けた動員可能な事務所の職員は、外来への移動を行い、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）　情報システムサーバー及びネットワークシステムの障害
⑴　通常、主サーバーがダウン状態に陥っても、従サーバーの稼動により通常の診察が継続できるため、従サーバーの稼動中に主サーバー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・従サーバー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、医療システム係からの連絡を待つ。医療システム係の確認と判断により、レベル０と判断された場合は、１０分以内に再稼動可能なので、再度、医療システム係からの復旧の連絡を待ち、復旧後、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。
⑵　システムダウンの情報が入ったら、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。カルテを閉じるとか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）

⑶　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。

⑷　レベル１の場合、診療業務については、プライマリー・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ーを事後入力とする。

⑸　レベル２の場合、各サーバー（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、紙カルテにて診察した患者データーを事後入力する。

　レベル２の場合は、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。

⑹　画像系ネットワークダウンの場合は、装置に直接、患者ＩＤを打ち込み、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、画像サーバーに送信し保存する。

⑺　医療システム係は、システムダウンに備え、紙運用に必要な物品を各部署に配付し、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
再診予約記載用紙
コピー用カーボン紙
手書きの検体ラベル等

⑻　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、ダウン時予約一覧を参照し、当日受付患者の受診診療科の前回処方を打出し、各外来に配付する準備を開始する。

⑼　レベル１以上の段階で受付に到着した患者については、紙による受付を受付窓口にて行ない、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、受付窓口が非常に混雑することが予想されるので、受付窓口近くに案内表示をし、机を２・３台用意し、仮受付所を設置する。

⑽　医療システム係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ー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。

⑾　システムダウン時に使用した紙カルテについては、当該紙カルテが原本となるため、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）

⑴　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。停電が発生すると自家発電が起動するまで（約１分）には、電源が切れるので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、サーバー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、端末への給電開始と同時に、それまでに使用していた端末は再接続を自動的に開始する。

⑵　個別端末レベルで使用不可能になる状態としては、短絡や画面のフリーズが考えられる。この状態の時は、医療システム科に速やかに連絡をし、復旧後、診療業務を再開する。

３）　外部ネットワーク由来の障害対応

⑴ 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、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。