新潟市民病院医療情報セキュリティ基本方針

Ver 1.01

平成27年7月1日

新潟市民病院医療情報セキュリティ基本方針

１　目的

新潟市民病院が取り扱う医療情報及びこれに関連する情報（以下「医療情報」という。）には，市民・患者の個人情報をはじめ病院運営上重要な情報など，外部に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

これらの守るべき情報や情報を取り扱う情報ネットワーク及び情報システム等を，災害，事故，故意及び過失等の様々な脅威から防御することは，市民・患者の財産やプライバシー等を守るためにも，また，病院事業の安定的な運営のためにも必要不可欠であり，ひいては新潟市民病院に対する市民・患者からの信頼の維持向上に寄与するものである。

新潟市民病院医療情報セキュリティ基本方針は，新潟市民病院の医療情報セキュリティ対策の基本的な方針として，適用の対象や位置づけ等を定め，新潟市民病院が所掌する医療情報資産の機密性，完全性及び可用性を維持し，総合的，体系的かつ継続的に情報セキュリティ対策を図ることを目的とする。

２　用語の定義

⑴　情報ネットワーク

コンピュータを相互に接続するための通信網，接続機器のハードウエア及びソフトウエア並びに電磁的記録媒体で構成され，処理を行う仕組みを情報ネットワークという。

⑵　情報システム

ハードウエア及びソフトウエアで構成されるコンピュータ，情報ネットワーク並びに電磁的記録媒体で構成され，処理を行う仕組みを情報システムという。

⑶　情報資産　　次の各号を情報資産という。

ア　情報ネットワークと情報システムの開発・運用に係る全ての情報及び情報ネットワークと情報システムで取り扱う全ての情報

イ　アの情報が記録された紙等の有体物及び電磁的記録媒体

ウ　情報ネットワーク及び情報システム

⑷　情報セキュリティ

情報資産の機密性，完全性，可用性を維持すること。

ア　機密性

アクセスを許可された者だけが情報にアクセスできることを確実にすること。

イ　完全性

情報及び処理方法が，正確であること及び完全である状態を保護すること。

ウ　可用性

許可された利用者が，必要なときに，情報及び関連する資産にアクセスできることを確実にすること。

３　新潟市民病院医療情報セキュリティ基本方針の位置づけと規定の体系

新潟市民病院医療情報セキュリティポリシーは，新潟市民病院が所掌する医療情報資産に関する情報セキュリティ対策について，総合的かつ体系的に取りまとめたものであり，新潟市民病院医療情報セキュリティ基本方針と新潟市民病院医療情報セキュリティ対策基準によって構成する。

また，新潟市民病院医療情報セキュリティポリシーに基づき，情報セキュリティ実施手順を策定することとする。

新潟市民病院医療情報セキュリティポリシーの構成

文書名		内容
新潟市民病院医療情報セキュリティポリシー	新潟市民病院医療情報セキュリティ基本方針	新潟市民病院が所掌する医療情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものであり，情報セキュリティ対策の頂点に位置するものである。
	新潟市民病院医療情報セキュリティ対策基準	新潟市民病院医療情報セキュリティ基本方針に基づき，情報セキュリティ対策を統一的に講ずるために，職員等が遵守すべき行為及び判断等の基準を規定するものである。
情報セキュリティ実施手順		新潟市民病院医療情報セキュリティポリシーに基づき，情報セキュリティ対策を具体的に実施するために，職員等が遵守すべき情報セキュリティ対策の実施手順を，情報資産ごとに具体的に規定するものである。

4　適用範囲

新潟市民病院医療情報セキュリティポリシーの適用範囲は，以下の各号に示すものとする。

⑴　適用組織

新潟市民病院の各部，センター及び事務局の各課とする。

⑵　適用情報資産

適用組織が所掌する医療情報資産とする。

⑶　適用対象者

適用される情報資産に接する適用組織の職員（非常勤職員及び臨時職員等を含む。以下「職員等」という）とする。

5　職員等の義務

⑴　遵守義務

職員等は，情報セキュリティの重要性について共通の認識を持つとともに，新潟市民病院が所掌する医療情報資産を取り扱う際には，不正アクセス行為の禁止等に関する法律や著作権法等の情報セキュリティに関連する法令並びに新潟市民病院医療情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

⑵　懲戒処分等

本ポリシーに違反した職員等は，その重大性及び発生した事案の状況等に応じて，地方公務員法等による懲戒処分の対象となる場合がある。

６　情報セキュリティ管理体制

新潟市民病院の所掌する医療情報資産について，適切に情報セキュリティ対策を推進・管理するための体制を確立する。

７　情報資産の分類

新潟市民病院の所掌する医療情報資産をその内容によって分類し，その重要度に応じた情報セキュリティ対策を講ずる。

８　情報資産への脅威

情報セキュリティ対策を講ずるうえで，特に認識すべき脅威は以下のとおりである。

⑴　本ポリシーに規定する適用対象者以外の第三者による，故意の不正アクセス又は不正操作によるデータやプログラムの持出，盗聴，改ざん，消去並びに機器及び記録媒体の盗難等

⑵　職員等及び新潟市民病院が医療情報システム開発，警備及び清掃等の目的で業務を委託した者（以下「外部委託業者」という。）による，誤操作又は故意の不正アクセス又は不正操作によるデータやプログラムの持出，盗聴，改ざん，消去並びに機器及び記録媒体の盗難等

⑶　地震，落雷，火災，水害等の災害，事故及び故障等

９　情報セキュリティ対策

新潟市民病院の所掌する医療情報資産を先に掲げた脅威から保護するため，以下の情報セキュリティ対策を講ずるものとする。

⑴　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り，医療情報資産への損傷・妨害等を防ぐため，入退室や機器管理上の物理的な対策を講ずる。

⑵　人的セキュリティ対策

医療情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに，全ての職員等に情報セキュリティポリシーの内容を周知徹底するため，教育及び啓発が行われるよう必要な対策を講ずる。

⑶　技術的セキュリティ対策

医療情報資産を不正なアクセス等から適切に保護するため，医療情報資産へのアクセス制御，コンピュータウイルス対策等の技術的な対策を講ずる。

⑷　運用セキュリティ対策

情報セキュリティポリシーの実効性を確保し，情報システム等の稼動状況の監視や情報セキュリティポリシーの遵守状況の確認のため，アクセスログ監査の実施，運用面における必要な対策を講ずる。また，緊急事態が発生した場合に迅速な対応を可能とするため，危機管理対策を講ずる。

１０ 情報セキュリティ対策に関する規定の公開・非公開

新潟市民病院医療情報セキュリティ基本方針は公開するが，新潟市民病院医療情報セキュリティ対策基準及び情報セキュリティ実施手順の公開は，犯罪の予防その他の公共の安全及び秩序の維持に支障を及ぼすおそれがあるため，これ等は公開しない。

１１ 情報セキュリティ対策実施状況の検証

新潟市民病院医療情報セキュリティポリシーが適切に遵守されていることを確認するために，定期的に情報セキュリティ対策の実施状況について検証を行う。

１２ 情報セキュリティ対策の評価，見直し

情報セキュリティ対策実施状況の検証結果，情報システムの変更，新たな脅威等情報セキュリティを取り巻く状況の変化に対応し，新潟市民病院医療情報セキュリティポリシー及び情報セキュリティ実施手順の評価と見直しを適宜行う。

附　則

（施行期日）

１　この新潟市民病院医療情報セキュリティ基本方針は，平成２７年７月１日から施行する。