所沢市市民医療センターセキュリティ基本方針

1　目的

所沢市市民医療センター（以下「医療センター」という。）が保有する医療情報システム及びこれに関連する情報（以下「医療情報」という。）には、利用者様の個人情報のみならず病院運営上重要な情報など、外部への漏えい等が発生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ます。

したがって、医療情報を様々な脅威から防御することは、利用者様の財産・プライバシー等をまもるために、また、病院事業の安定的な運営のためにも必要不可欠です。ひいては、このことが、医療センターに対する利用者様からの信頼の維持向上に寄与するものです。

そのため、医療センターの医療情報を様々な脅威から防御する際の基本的な方針として、所沢市市民医療センター情報セキュリティ基本方針（以下「基本方針」という。）を策定し、医療センターが保有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運用するとともに、これらを効果的に取り扱うことで、利用者様からの継続的な信頼を得ることを目的とします。

2　用語の定義

(1)　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、その構成機器(ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいいます。

(2)　医療情報システム

電子計算機（サーバ、クライアント等）とソフトウェア、ネットワーク及び記録媒体で構成され、一連の事務処理を行う仕組みをいいます。

(3)　情報資産

ネットワーク及び医療情報システムの開発と運用及び保守に係る全ての情報並びにネットワーク及び医療情報システムで取り扱う全ての情報をいいます。なお、情報資産には紙等の有体物に出力された情報を含みます。

(4)　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいいます。

(5)　情報セキュリティポリシー

基本方針及び別に定める医療情報セキュリティ対策基準をいいます。

(6)　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいいます。

(7)　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいいます。

(8)　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいいます。

(9)　外部委託業者

業務委託契約等により、医療センターの事務事業の執行を受託した事業者をいいます。

3　所沢市市民医療センター情報セキュリティ基本方針の位置づけと体系

所沢市市民医療センター情報セキュリティポリシーは、医療センター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、総合的体系的に取りまとめたものであり、所沢市市民医療センター情報セキュリティ基本方針と所沢市市民医療センター対策基準によって構成します。

また、所沢市市民医療センター情報セキュリティポリシーに基づき、所沢市市民医療センター情報セキュリティ実施手順を策定します。

所沢市市民医療センター医療情報セキュリティポリシーの構成

文書名		内　容
所沢市市民医療センター情報セキュリティポリシー	所沢市市民医療センター情報セキュリティ基本方針	基本方針は、医療センターが保有する情報資産を様々な脅威から防御する際の基本的な方針であり、医療センターの情報セキュリティ対策の頂点に位置するものです。
	所沢市市民医療センター情報セキュリティ対策基準	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統一的な基準として、情報セキュリティ対策基準を策定するものです。
所沢市市民医療センター情		所沢市市民医療センター情報セキュリティポリ

報セキュリティ実施手順	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策定するものです。

4　対象範囲

この基本方針の対象範囲は、医療センターが保有する情報資産、情報資産に関する事務に関わる全ての職員（嘱託職員、非常勤特別職員、非常勤職員及び臨時的任用職員等を含む。以下「職員等」という。）及び外部委託業者とします。

5　情報セキュリティ管理体制

医療センターの医療情報資産について、情報セキュリティ対策を積極的に推進・管理するための体制を確立します。

6　情報資産の分類

医療センターの医療情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行います。

7　情報資産への脅威

情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりです。

(1)　部外者の侵入による機器又は情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊・盗聴・改ざん・消去等

(2)　職員等又は外部委託事業者による機器又は情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏えい等

(3)　コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

(4)　大規模・広範囲にわたる疫病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

8　情報セキュリティ対策

上記７で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じます。

(1)　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・妨害等から保護するために物理的な対策を講じます。

(2)　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者に基本方針等の内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講じます。

(3)　技術におけるセキュリティ対策

医療情報資産を外部からの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、ネットワーク管理等の技術面の対策を講じます。

(4)　運用におけるセキュリティ対策

システム開発等の外部委託、ネットワークの監視、情報セキュリティ対策の遵守状況の確認等、運用面の対策を講じます。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じます。

9　情報セキュリティ対策に関する規定の公開・非公開

所沢市市民医療センター医療情報セキュリティ基本方針は公開しますが、所沢市市民医療センター医療情報セキュリティ対策基準及び所沢市市民医療センター医療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恐れのある医療情報資産であることから非公開とします。

10　職員等及び外部委託業者の責務

職員等及び外部委託事業者は、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業務の遂行に当たって法令及び対策基準等を遵守しなければならないものとします。

11　情報セキュリティ対策に違反した職員等及び外部委託業者への対応

　情報セキュリティ対策に違反した職員等及び外部委託事業者についてはその重大性、状況等に応じて厳正に対応します。

12　情報セキュリティ対策の実施状況の検証

　所沢市市民医療センター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、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います。

13　情報セキュリティ対策の評価及び見直しの実施

　情報セキュリティ対策実施状況の検証結果により、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情報の変化に対応し、医療情報セキュリティポリシーおよび実施手順の評価と見直しを適宜実施します。

附　則

この方針は、平成２６年４月１日から施行する。