医療法人 社団 玄同会 小畠病院

情報セキュリティポリシー

（基本規定）

【 序文 】

医療法人社団玄同会 小畠病院（以下「当院」と言う）が取り扱う情報には、患者の個人情報、職員に関する情報をはじめ病院運営上重要な情報等（以下、「情報資産」と言う。）があり、取り扱いについては高い安全性が求められています。

当院では患者の利益を最優先に考え、情報資産や情報資産を取り扱う情報ネットワークおよび情報システム等に関わる全ての事項について適切な安全対策を施し、また、職員に対しては教育を行い意識の向上を図ります。

当院の情報セキュリティ対策の基本方針として情報セキュリティポリシーを策定し、情報資産の機密性・完全性・可用性を維持し、総合的・体系的・継続的に情報セキュリティ対策を図ります。

この情報セキュリティポリシーを全ての職員が遵守し、患者へ安全で安心できる医療サービスを提供してまいります。

情報セキュリティポリシーは、基本方針を定めた「基本規定」、セキュリティ対策の基準を定めた「対策基準」、情報セキュリティに関する緊急時の行動手順を定めた「緊急時対応」および具体的な情報管理システム別の運用手順を定めた「運用管理規定」により構成されています。

1. 総則

(1) 目的

当院における情報セキュリティ対策の基本となる事項を定め、当院の情報資産の機密性・完全性・可用性を維持し、情報資産を適切に保護し安全に運用することを目的とする。

(2) 情報セキュリティポリシー

① 当院の情報セキュリティ対策は、情報セキュリティポリシーに基づき実施する。
② この規定を、当院の情報セキュリティ対策の基本方針とする。
③ 情報セキュリティの管理規定を定め、情報セキュリティ確保のために必要な対策を講じる。

(3) 用語の定義

情報セキュリティポリシーにおいての用語の定義は、以下のとおりとする。

① 情報 ： 有形、無形を問わず、当院が取り扱う患者の個人情報、職員に関する情報をはじめ病院運営上重要な情報など全ての情報（当院以外の医療機関、企業、団体又は個人から取得、借用又は預かり受けている情報資産を含む。）をいう。
② 情報資産 ： 情報およびそれらを取り扱う全ての人的、物理的な資産をいう。媒体（紙媒体、電子媒体等）、情報の伝達手段（情報システム、口頭、電気通信等）を含む。
③ 情報システム ： 情報を取り扱う機器装置等のハードウェア、ソフトウェア、プログラム等により構成される電子システム及びその収納施設等をいう。また、情報システムによる情報伝送経路を情報ネットワークという。
④ 職員 ： 常勤および非常勤を問わず当院の業務に従事する全ての者をいう。

⑤ 外部要員 ： 当院の情報資産を取り扱うことを認められた者で、次に掲げる者をいう。
ア 人材派遣契約により当院に派遣され、当院の情報資産を取り扱う者
イ 委託契約又は請負契約に基づき、当院の情報資産を取り扱う者
ウ その他当院の情報資産の取り扱いを許可された者

⑥ 脅威 ： 故意による不正アクセスや過失による情報の漏えい、情報機器の故障等による事故および災害等による情報の流出、滅失または利用不能など、機密性・完全性・可用性を損なわれる事態をいう。

⑦ 安全性 ： 次に掲げる機密性、完全性および可用性の総称をいう。
ア. 機密性 ： ある情報へのアクセスを認められた人だけが、その情報にアクセスできる状態を確保すること
イ. 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
ウ. 可用性 ： 情報へのアクセスを認められた人が、必要時に中断することなく、情報にアクセスできる状態を確保すること

⑧ 個人情報 ： 当院の「個人情報の保護に関する院内規則」に規定する個人情報をいう。

⑨ 情報セキュリティ対策 ： 機密性、完全性および可用性を維持し、脅威から情報を保護するための対策をいう。

(4)適用範囲、適用対象者

適用範囲は、次に掲げる範囲とする。

① 当院の保有する情報資産

② 当院の保有する情報資産を取り扱うシステム、関連設備、建物およびその環境

③ 当院の保有する情報資産を取扱う全ての職員および外部要員

2. 情報セキュリティ対策の基本方針

(1)職員等の責務

情報セキュリティポリシーに基づき、法令並びに各規定を遵守し、情報セキュリティ対策を行わなければならない。

(2)情報の安全管理

① 情報については、次に掲げる措置を講ずる。
ア. 情報資産の分類に応じた機密性の確保
イ. 情報の内容等について完全性の確保
ウ. 情報資産に相応する可用性レベルの確保

② 個人情報については、個人情報保護に関する規定を整備し、情報の利益保護を徹底するための措置を講ずる。

(3)安全性の確保と体系的な対策

① 重要な情報資産については、利便性の確保よりも安全性の確保を優先する。

② 情報セキュリティ対策の実施に当たっては、物理的、人的および技術的な側面から、予防、防止、検知および回復手段を考慮したものとする。

ア. 物理的セキュリティ対策

情報システムや機密性の高い情報を取り扱う部屋などへの不正な立入り、情報資産の

完全性を確保するため、入退室や機器管理上の物理的な対策を講ずる。

イ. 人的セキュリティ対策

情報資産を取り扱う職員および外部要員の情報セキュリティに関する権限や責任等を定め、情報セキュリティポリシーおよび各規定の遵守を徹底するための教育および啓発などに必要な対策を講ずる。

外部要員が、当院の情報資産、建物および関連設備を取り扱う場合においては、情報セキュリティポリシーに遵守する旨の契約を締結するとともに、外部要員に対して適切な監督を行う。

ウ. 技術的セキュリティ対策

情報資産を不正なアクセスや機器トラブル等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策、バックアップ等の技術的な対策を講ずる。

エ. 運用上の対策

情報セキュリティポリシーを担保するため、情報資産の取扱いに関する規定を整備し、情報資産の保護を組織的に行うための措置を講ずる。

また、緊急事態への迅速な対応を図るため、危機管理対策を講ずる。

(4)継続的な情報セキュリティ対策

情報セキュリティ対策は、定期的又は随時に評価し、継続的に実施する。

(5)効率的な情報セキュリティ対策

① 情報の利用に際し、利便性についても考慮し、安全性と利便性の両立した情報セキュリティ対策を施す。

② 情報セキュリティ対策の実施に当たっては、費用対効果を勘案する。

(6)情報機器、情報ネットワークおよび情報システム等の適正な管理

① 情報機器については、導入・設置・運用等において適正な管理を行う。

② 情報ネットワークおよび情報システムについては、設計・構築・運用等において適正な管理を行う。

③ 情報資産を保管又は設置する建物および関連設備については、適正な管理を行う。

(7)情報セキュリティ事故への対応

情報セキュリティ事故が発生または発生した疑いが生じた場合の、連絡および手続きなどの対応策を定め、業務継続のための復旧措置を実施し、再発防止措置を講ずる。

(8)著作権の保護

① 当院に帰属しない著作物を利用する場合には、その著作権に配慮した取り扱いを行う。

② 当院以外で開発されたソフトウェアを導入する場合には、前項に加えて使用許諾条件を遵守し、導入・運用・ライセンス管理等その使用状況を適正に管理する。

(9)監査および点検

情報セキュリティ対策の状況等について、外部監査、内部監査又は各部署等による自主点検を適宜実施する。

3. 体制

① 情報管理委員会 ： 情報セキュリティ対策を運営するための組織として設置し、情報資産のうち人事・財務に関する情報を除く情報資産管理に関する事項を審議する。
② 情報統括責任者 ： 情報資産の統括責任者をいい、病院長に指名された者がその責を担う。
③ 個人情報管理責任者 ： 個人情報管理に関する責任者をいい、事務部長がその責を担う。
④ 診療情報管理責任者 ： 診療情報に関する責任者をいい、診療情報管理担当部長がその責を担う。
⑤ 情報システム管理責任者 ： 情報システム管理に関する責任者をいい、情報システム管理室長がその責を担う。
⑥ 広報担当責任者 ： 広報情報に関する責任者をいい、医事課長がその責を担う。
⑦ 部署で扱う情報の責任者 ： 部署における情報管理に関する責任者をいい、各部署長がその責を担う。
⑧ 人事・財務に関する情報管理の責任者 ： 人事・財務に関する情報およびそれらを専ら扱う情報システムに関する責任者をいい、事務部長がその責任者となり管理する。

5. その他

(1)法令遵守

① 業務の遂行において使用する情報資産の取り扱いに当たっては、著作権法、不正アクセス行為の禁止等に関する法律のほか、関連する法令・規則等を遵守しなければならない。
② 個人情報保護に関する法令・規則等を遵守しなければならない。

(2)守秘義務

① 業務上知り得た情報を正当な理由なく第三者に開示または漏洩してはならない。但し、すでに公開済みのものや独自にないし別ソースから入手されたものは除く。
② 当院の設定した個人情報保護に関する規定等を遵守しなければならない。

(3)懲戒

情報セキュリティポリシーに定める事項の遵守を怠った結果、当院に損害をもたらした場合は、懲戒および損害賠償の対象とする。

(4)例外措置

情報資産の取り扱いについて情報セキュリティポリシーに照らして判断できないとき、正当な理由でその遵守が困難となる事態が発生または発生するおそれがある場合には、情報管理委員会が対応を協議し病院長に諮り、病院長より指示あるものとする。

(5)運用

情報管理委員会は、当院の情報セキュリティの水準を維持および向上するため、情報セキュリティポリシーを適宜見直し、必要に応じて改正するものとする。

【附 則】

この規定は、2019 年 4 月 2 日から施行する。