

## 広島赤十字・原爆病院

### — 情報セキュリティ基本方針 —

広島赤十字・原爆病院(以下、当院という)は、一日でも早く患者さんが健康を取り戻していただくことを最優先に考えています。そのために患者さんからお預かりしている多くの個人情報を最大限に活用して、診療・治療・看護を行うことを使命としています。

当院では、個人情報保護に関する取り組みを年々強化しています。強化に当たっては、情報セキュリティに関する態勢の強化と情報セキュリティポリシーの最適化を図り、患者さんとその家族や親族、友人、および当院を取り巻く地域社会に対して個人情報の保護を通して安心と安全を提供できるように取り組んでいきます。

本基本方針は、情報セキュリティポリシー構成要素の一つであり、個人情報の保護に万全を期す上で必要な情報セキュリティの推進に関して基本的な方向を示すものです。

平成17年4月に個人情報保護に関する法律が施行された後も、国、地方自治体、企業はもとより医療機関においても個人情報の漏えい事故発生が後を絶ちません。これらの原因は、個人情報を安全に管理する技術的な問題もさることながら、その本質はそれを取り扱う者の人的な問題にあることは個人情報漏えいに関する報道発表の内容からも明らかです。

この問題を解決するに当たり当病院では、全職員を対象に個人情報の保護に関する情報セキュリティ研修を行い、個人情報を安全に取り扱えるように習慣化を図ります。さらに患者さんからお預かりした個人情報には暗号化などの対策を施して、万が一紛失や盗難に遭遇しても患者さんの権利や利益が侵害されないように万全を期します。

診療・治療において、患者さんからお預かりした個人情報を医師が必要と判断して家族や親族、および友人などに提供することもあります。当然、患者さんの権利や利益を損なわないように、患者さん本人の同意を取ることを原則とするなど、細心の注意を払って行いますのでご理解とご協力をお願いします。

以上のことを踏まえ、当病院では個人情報の保護に当たり以下の5つを基軸として取り組みます。

#### 『個人情報保護に関する5つの取り組み基軸』

1. 個人情報保護の状況を定期的に内部監査にて把握し、情報セキュリティポリシーを継続的に最適化する。
2. 全職員に対して個人情報保護研修を継続的に行い、情報セキュリティポリシーの周知と徹底を図る。
3. 個人情報に対しては、閲覧・更新・印刷・複製などの制限や暗号化などの保護対策を実施する。
4. 情報セキュリティや個人情報保護を取り巻く環境の変化、およびセキュリティ技術の進歩に絶えず追従し最適な状態を保つ。
5. 個人情報の保護と併せてプライバシーに関する権利を尊重する。

患者さんからお預かりした個人情報の保護には、情報セキュリティ対策は不可欠です。今後も段階的に情報セキュリティレベルの向上を図ります。そして、患者さんはもとより家族や親族、友人、および当院を取り巻く地域社会に対して、当院は本基本方針に基づき全職員が全力を尽くして個人情報を保護し、安心と安全の提供を実行します。

## 【情報セキュリティポリシーの体系】

### 1 情報セキュリティ体制の整備

情報セキュリティマネジメントシステムの体制として、「情報セキュリティ委員会」を設置し、情報セキュリティ統括責任者、情報セキュリティ管理者、情報セキュリティ部署管理者をおき、情報セキュリティの確保、維持、向上および必要な措置を迅速に対応できる体制を整備します。

### 2 情報セキュリティ対策基準の策定

情報セキュリティ対策の実施に当たり、判断や実行の基準となる考え方および順守事項を情報セキュリティ対策基準として策定します。

### 3 情報セキュリティ実施手順の策定

情報セキュリティ対策を実施するために、情報セキュリティ対策基準で示した判断や実行について具体的に示し、全職員等が実行する手順書を定めます。手順書には情報に対する脅威からの保護および情報の重要度に応じた具体的な情報の取り扱いについて記述します。

### 4 教育・訓練の実施

全職員に対して、定期的に情報セキュリティに関する教育・訓練を行い、情報セキュリティの重要性、適切な情報の取り扱いの周知と徹底を図ります。

### 5 情報セキュリティインシデント及び情報セキュリティアクシデントへの対応

職員は、日常において情報セキュリティインシデントの発見に尽力します。発見した場合は、インシデントレベルにより対策基準と実施手順書に基づき、情報セキュリティ委員会も含めて協議し、対応を決定します。情報セキュリティアクシデント(事件・事故)は、情報セキュリティ委員会を招集し、調査、被害者の特定、対応方針の決定、被害者への連絡、および関連機関への報告を行うとともに、再発防止策を検討・実施して安心と安全の確保に尽力します。

### 6 事業継続管理

偶発的に発生する災害・故障・過失および意図的な情報の悪用などによる事業の中断を可能な限り抑え、事業の継続を確保します。

### 7 継続的改善

情報セキュリティポリシーの順守状況を定期的に監査するとともに、対策基準書、実施手順書、および更新計画書を見直します。また、情報セキュリティや個人情報保護を取り巻く環境の変化やセキュリティ技術の進歩を絶えず追従し最適な状態を保ちます。

### 8 法令・条例・規範の順守

職員は、情報セキュリティポリシー、関連する法律、および日本赤十字社の例規等を順守します。違反する行為があれば厳しく対処するとともに再発防止を検討・実施して適切な情報管理を図ります。

以上

令和5年4月1日  
広島赤十字・原爆病院  
病院長 古川 善也