

健康保険組合等における個人情報保護 ・情報セキュリティ対策について

別紙 1 「健康保険組合等における個人情報の適切な取扱いのためのガイドライン」(平成 16 年 12 月)(目次)

<http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161227kenpo.pdf>

別紙 2 「レセプトのオンライン請求に係るセキュリティに関するガイドライン」(平成 18 年 4 月)(目次)

<http://www.mhlw.go.jp/bunya/shakaihoshho/iryouseido01/pdf/recept03b.pdf>

参考 1 「医療情報システムの安全管理に関するガイドライン第 2 版」(平成 19 年 3 月)(目次)

<http://www.mhlw.go.jp/shingi/2007/03/s0301-12.html>

参考 2 「政府機関統一基準の構成」(第 1 回検討会資料より抜粋)

<http://www.nisc.go.jp/active/general/pdf/k303-071.pdf>

※ 各ガイドラインの全文については、それぞれの URL を参照。

健康保険組合等における
個人情報の適切な取扱いのためのガイドライン

平成16年12月27日
厚生労働省

目 次

I	本ガイドラインの趣旨、目的、基本的考え方	
1.	本ガイドラインの趣旨	1
2.	本ガイドラインの構成及び基本的考え方	1
3.	本ガイドラインの対象となる「健保組合等」の範囲	1
4.	本ガイドラインの対象となる「個人情報」の範囲	2
5.	大臣の権限行使との関係等	2
6.	健保組合等が行う措置の透明性の確保と対外的明確化	2
7.	責任体制の明確化と被保険者等窓口の設置等	3
8.	遺族への個人情報の提供の取扱い	3
9.	他の法令との関係	3
10.	認定個人情報保護団体における取組	3
II	用語の定義	
1.	個人情報	4
2.	個人情報の匿名化	4
3.	個人情報データベース等	5
4.	本人の同意	5
III	健保組合等の義務等	
1.	利用目的の特定等（法第15条、第16条）	6
2.	利用目的の通知等（法第18条）	9
3.	個人情報の適正な取得、個人データ内容の正確性の確保 （法第17条、第19条）	11
4.	安全管理措置、従業者の監督及び委託先の監督（法第20条～第22条）	12
5.	個人データの第三者提供（法第23条）	17
6.	保有個人データに関する事項の公表等（法第24条）	22
7.	本人からの求めによる保有個人データの開示（法第25条）	24
8.	訂正及び利用停止（法第26条、第27条）	26
9.	開示等の求めに応じる手続及び手数料（法第29条、第30条）	28
10.	理由の説明、苦情処理（法第28条、第31条）	31
IV	ガイドラインの見直し等	
1.	必要に応じた見直し	32
2.	本ガイドラインを補完する事例集等の作成・公開	32
別表1	健保組合等が保有する個人情報の例	33
別表2	健保組合等の通常の業務で想定される主な利用目的	35

レセプトのオンライン請求に係る
セキュリティに関するガイドライン

平成18年4月

厚生労働省

目 次

I 総則	1
1 目的	1
2 適用範囲	2
3 位置付け	3
4 構成	4
5 見直し	4
II セキュリティに関するガイドライン	5
1 組織・体制	5
(1) 責任者の任命	5
(2) 責任の所在	5
(3) 連絡体制	5
2 情報の分類と管理	6
(1) 情報の管理責任	6
(2) 情報の分類	6
(3) 情報の分類に応じた管理方法	6
3 物理セキュリティ	7
(1) 医療機関及び薬局の送信機器の設置場所	7
(2) 審査支払機関の送受信機器の設置場所	7
(3) 保険者の受信機器の設置場所	8
4 人的セキュリティ	9
(1) すべての人員の基本的な責務	9
(2) 機関の長の責務	9
5 技術的セキュリティ	10
(1) レセプトデータの機密性の確保	10
(2) 伝送相手の正当性の確保	10
(3) 伝送事実の正当性の確保	10
(4) システムの機密性の確保	10
(5) 伝送経路の機密性の確保	12
(6) 伝送の完全性の確保	12
(7) 他システムと接続する場合の要求事項	12
6 運用	13
(1) 開発規程	13
(2) 管理運用規程	13
(3) 開発及び試験環境と運用環境の分離	13
7 規程遵守	14
(1) セキュリティポリシー	14
8 規程に対する違反への対応	15
9 評価・見直し	15
(1) 監査証拠の保管	15
(2) 監査の実施	15
(3) 監査結果に基づく措置	15

医療情報システムの安全管理に関するガイドライン

第2版

平成19年3月

厚生労働省

【目次】

1	はじめに.....	1
2	本指針の読み方.....	3
3	本ガイドラインの対象システム及び対象情報.....	5
4	電子情報を扱う医療機関等における責任のあり方.....	8
5	情報の相互利用性と標準化について.....	11
5.1	標準的な用語集やコードセットの利用.....	11
5.2	国際的な標準規格への準拠.....	12
6	情報システムの基本的な安全管理.....	13
6.1	方針の制定と公表.....	13
6.2	医療機関における情報セキュリティマネジメント（ISMS）の実践.....	14
6.2.1	ISMS 構築の手順.....	14
6.2.2	取扱い情報の把握.....	15
6.2.3	リスク分析.....	16
6.3	組織的安全管理対策（体制、運用管理規程）.....	19
6.4	物理的安全対策.....	21
6.5	技術的安全対策.....	22
6.6	人的安全対策.....	29
6.7	情報の破棄.....	31
6.8	情報システムの改造と保守.....	32
6.9	災害等の非常時の対応.....	34
6.10	外部と個人情報を含む医療情報を交換する場合の安全管理.....	38
7	電子保存の要求事項について.....	51
7.1	真正性の確保について.....	51
7.2	見読性の確保について.....	66
7.3	保存性の確保について.....	69
7.4	法令で定められた記名・押印を電子署名で行うことについて.....	73
8	診療録及び診療諸記録を外部に保存する際の基準.....	75

8.1	電子媒体による外部保存をネットワークを通じて行う場合	75
8.1.1	電子保存の3基準の遵守	76
8.1.2	外部保存を受託する機関の限定	80
8.1.3	個人情報の保護	84
8.1.4	責任の明確化	87
8.2	電子媒体による外部保存を可搬型媒体を用いて行う場合	90
8.2.1	電子保存の3基準の遵守	90
8.2.2	個人情報の保護	93
8.2.3	責任の明確化	96
8.3	紙媒体のままで外部保存を行う場合	98
8.3.1	利用性の確保	98
8.3.2	個人情報の保護	100
8.3.3	責任の明確化	103
8.4	外部保存全般の留意事項について	105
8.4.1	運用管理規程	105
8.4.2	外部保存契約終了時の処理について	106
8.4.3	保存義務のない診療録等の外部保存について	108
9	診療録等をスキャナ等により電子化して保存する場合について	109
9.1	共通の要件	109
9.2	診療等の都度スキャナ等で電子化して保存する場合	112
9.3	過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合	113
9.4	(補足) 運用の利便性のためにスキャナ等で電子化をおこなうが、紙等の媒体もそのまま保存をおこなう場合	115
10	運用管理について	117
	付表1 一般管理における運用管理の実施項目例	
	付表2 電子保存における運用管理の実施項目例	
	付表3 外部保存における運用管理の例	



政府機関統一基準の構成

第1部 総則

第2部 組織と体制の構築

- 組織・体制の確立(各責任者等の権限と責務の明確化等)
- 情報セキュリティ対策の教育
- 情報セキュリティ対策の自己点検
- 見直し
- 違反と例外措置
- 障害等の対応
- 情報セキュリティ対策の監査

第3部 情報についての対策

- 情報の格付け
- 情報の取扱い(利用・保存・移送・提供・消去)

第4部 情報セキュリティ要件の明確化に基づく対策

- 情報セキュリティ機能
 - 主体認証、アクセス制御、権限管理、証跡管理、情報保証、暗号・電子署名
- 脅威対策
 - セキュリティホール対策、不正プログラム対策、サービス不能攻撃対策
- 情報システムのセキュリティ要件
 - 情報システムの設計・構築・運用等

第5部 情報システムの構成要素についての対策

- 安全区域
- アプリケーション(共通、電子メール、ウェブ)
- 電子計算機(共通、端末、サーバ)
- 通信回線(共通、庁内、庁外)

第6部 個別事項についての対策

- 機器等の購入
- ソフトウェア開発
- 府省庁支給以外の情報システム(私物PC等)による情報処理の制限
- 外部委託
- 府省庁外での情報処理(情報の持ち帰り等)の制限
- その他

☆ 対策レベル: 「基本遵守事項」(必須の対策事項)と「強化遵守事項」(重要なシステムにおいて必要性を判断して取り入れる対策事項)