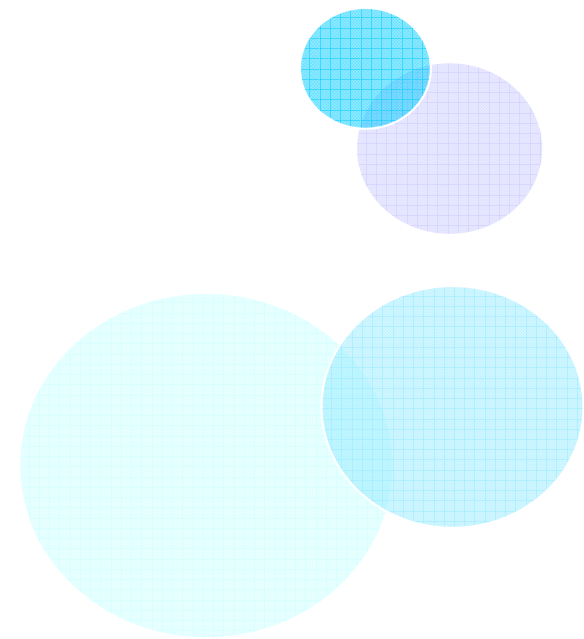


マイナンバー制度で医療現場はようになる



P I C C

株式会社 P I C C 個人情報審査センター



個人情報保護の体系

まずは個人情報保護体系を理解する・・・



OECD8原則

個人情報保護の個人情報保護の考え方の根源は、1980年にOECDが定めた“ OECD 8原則”にあります。この8原則を基本として、日本やその他各国の法律等が作られています。

- (1) 収集制限の原則
- (2) データ内容の原則
- (3) 目的明確化の原則
- (4) 利用制限の原則
- (5) 安全保護の原則
- (6) 公開の原則
- (7) 個人参加の原則
- (8) 責任の原則



個人情報保護法

個人情報保護法には基本的な内容が述べられています。具体的な内容については「政令」「基本方針」「分野別ガイドライン」等に記されています。個人情報保護法を理解し、遵守するためには、個人情報保護法のほか、政令、基本方針、分野別ガイドラインを理解しなければなりません。

ただ、法律を理解しただけでは個人情報保護体制を構築することは不可能と言わないまでも難しいと考えられます。なぜならば、遵法体制を維持し向上させるためには、何らかのマネジメントシステムが必要だからです。



経済産業省のガイドライン、厚生労働省のガイドライン

個人情報保護法をまもるために最低限必要な組織活動を記述したのが経済産業省が発行する個人情報保護に関するガイドラインです。このガイドラインに準じる形で分野別にガイドラインが整備されています。

企業や組織が個人情報保護に取り組む際はこのガイドラインの内容を参考にすることが第一歩です。



JIS Q 15001 : 1999

JIS Q 15001 は1999年に制定されたJIS規格で、プライバシーマークの認証基準でもあります。JIS Q 15001 では、まず最初に個人情報保護方針を定め、Plan (計画)、Do (実施運用)、Check (監査)、Action (事業者の代表者による見直し) というマネジメントサイクルを回すことで管理レベルをスパイラル状に向上させていく仕組みになっています。

個人情報保護に関する第三者認証

年号	法律・規格等	年号	第三者認証
1980	「OECDの8原則」 プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告		
1997	「個人情報保護ガイドライン：民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」	1997	米法人「TRUSTe」発足
1999	「JIS Q 15001：個人情報保護に関するコンプライアンス・プログラムの要求事項」制定	1998	「プライバシーマーク制度」運用開始
2005	「個人情報保護法：個人情報保護に関する法律」全面施行	2002	「ISMS」本格運用開始
		2009	「JAPHICマーク制度」運用開始

プライバシーマーク制度

日本情報経済社会推進協会
(JIPDEC)1998年～

【審査基準】

JISQ15001：2006
JIPDECガイドライン
(一部非公開)



特徴 厳しい審査
審査費用は他より割高

JAPHICマーク制度

日本個人・医療情報管理協会
(JAPHIC)2009年～

【審査基準】

経済産業省ガイドライン
個人情報保護法



特徴 易しい審査
審査費用はPマークの6～7割

JAPiCOマーク制度

日本個人情報管理協会
(JAPiCO)2011年～

【審査基準】

JISQ15001：2006
個人情報保護法
業界ガイドライン
地方条例



特徴 4つの基準で厳しい審査
審査費用はPマークの6～7割



医療機関向けの第三者認証

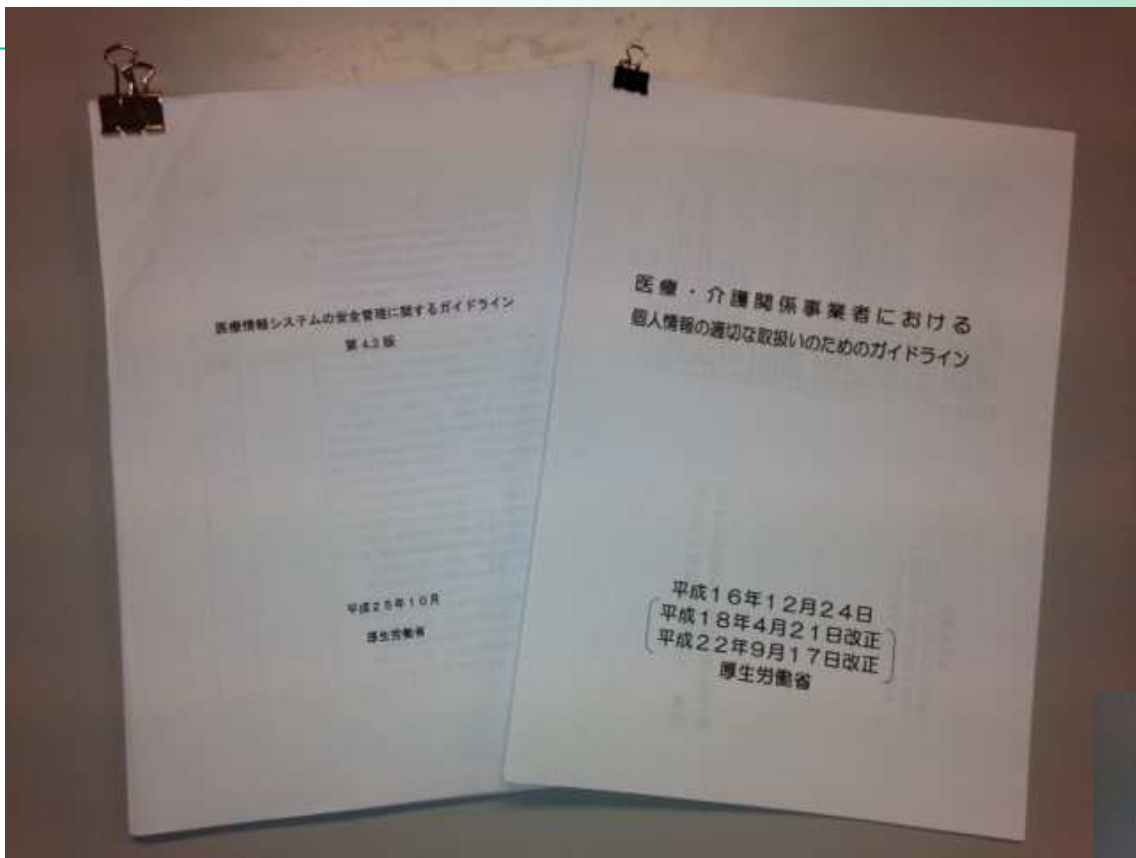
「JAPHIC MEDICAL」 (ジャフィックメディカル) 「近日発表?!」

厚生労働省の「医療・介護関係事業者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」

「医療情報システムの安全管理に関するガイドライン」をベースに近日リリース予定。

医療機関の実態に即した個人情報保護のマネジメントシステムの構築を第三者が認定いたします。

認定を取得することで**安全管理対策を行う事ができ、一般の方への大きなアピール**になります。

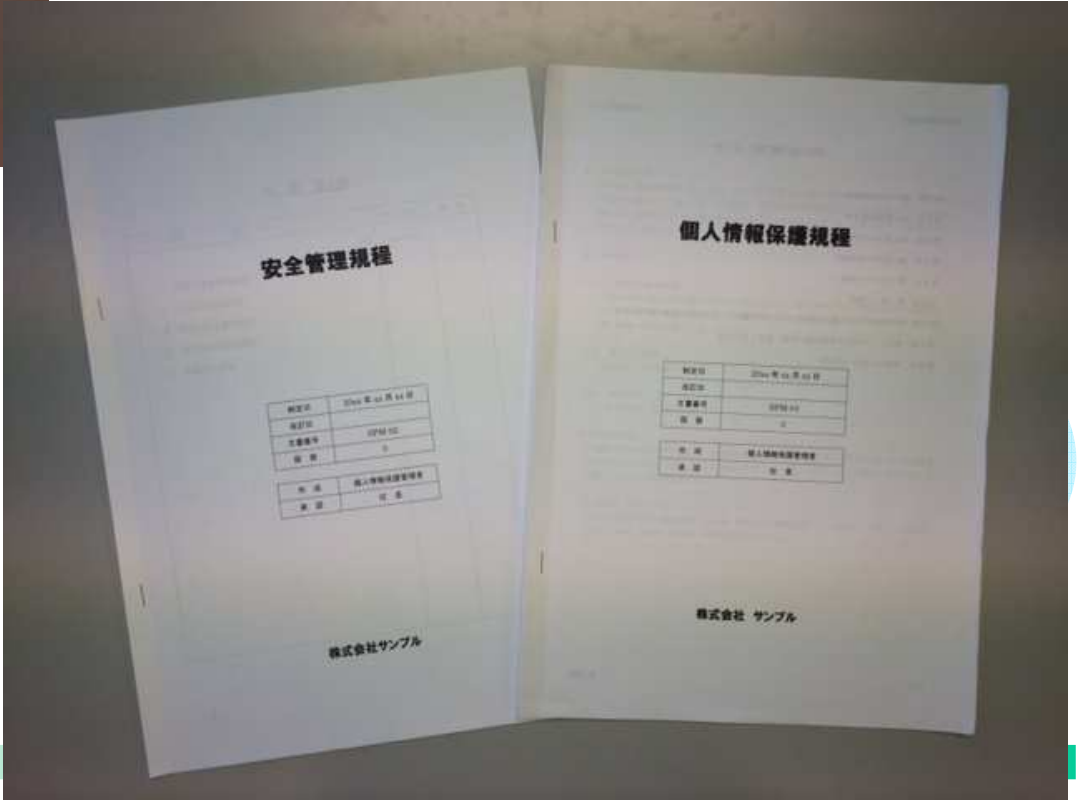
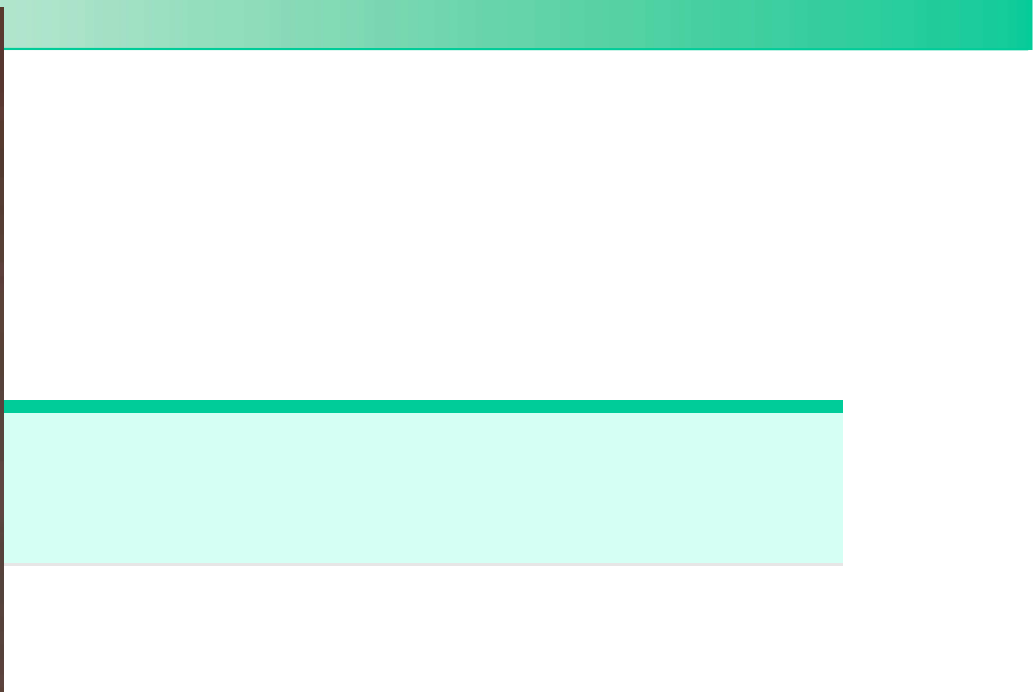


医療情報システムの安全管理に関するガイドライン
第4.2版

平成25年10月
厚生労働省

医療・介護関係事業者における
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24日
平成18年4月21日改正
平成22年9月17日改正
厚生労働省



安全管理規程

制定日	2016年11月11日
改訂日	2022年12月
文書番号	SPM-01
版 数	1
所 属	個人情報保護委員会
業 界	IT 業

株式会社サンプル

個人情報保護規程

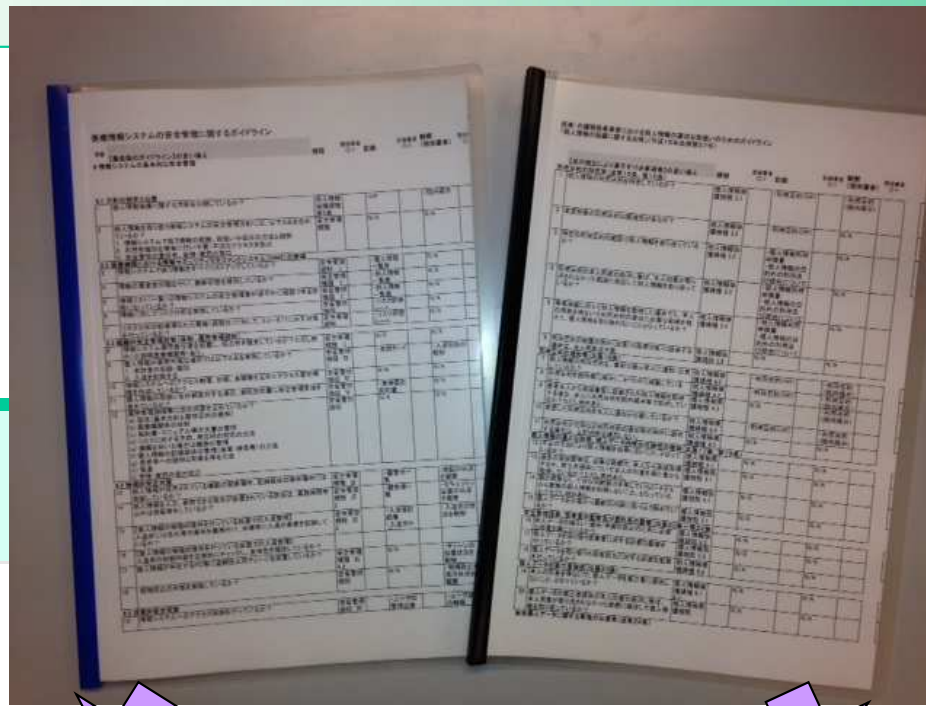
制定日	2016年11月11日
改訂日	2022年12月
文書番号	SPM-02
版 数	1
所 属	個人情報保護委員会
業 界	IT 業

株式会社 サンプル

「医療情報システムの安全管理に関するガイドライン」目次

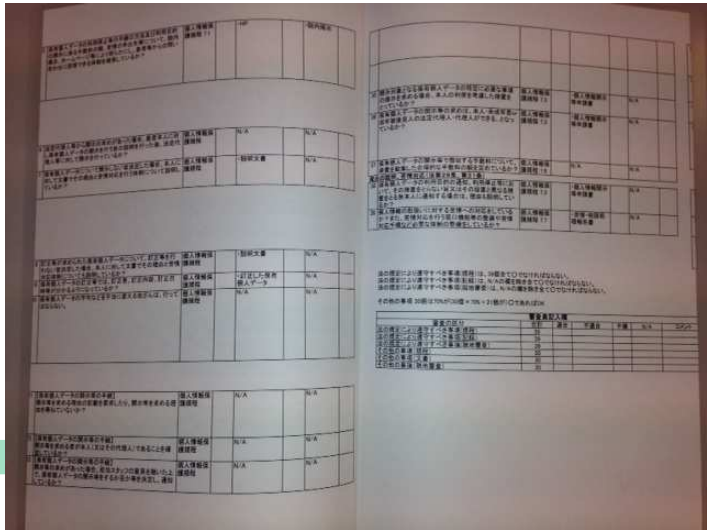
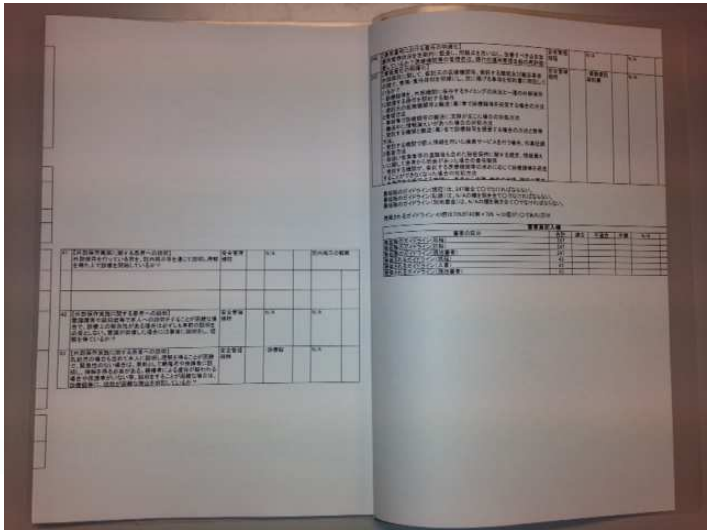
【目次】	
1 はじめに.....	1
2 本指針の読み方.....	8
3 本ガイドラインの対象システム及び対象情報.....	10
3.1 7章及び9章の対象となる文書について.....	10
3.2 8章の対象となる文書等について.....	11
3.3 調剤済み処方箋と調剤録の電子化・外部保存について.....	12
3.4 取扱いに注意を要する文書等.....	13
4 電子的な医療情報を扱う際の責任のあり方.....	14
4.1 医療機関等の管理者の情報保護責任について.....	15
4.2 委託と第三者提供における責任分界.....	16
4.2.1 委託における責任分界.....	16
4.2.2 第三者提供における責任分界.....	19
4.3 例示による責任分界点の考え方の整理.....	19
4.4 技術的対策と運用による対策における責任分界点.....	23
5 情報の相互運用性と標準化について.....	25
5.1 基本データセットや標準的な用語集、コードセットの利用.....	26
5.1.1 厚生労働省標準規格.....	26
5.1.2 基本データセット.....	27
5.1.3 用語集・コードセット.....	28
5.2 データ交換のための国際的な標準規格への準拠.....	28
5.3 標準規格の適用に関わるその他の事項.....	29
6 情報システムの基本的な安全管理.....	30
6.1 方針の制定と公表.....	30
6.2 医療機関における情報セキュリティマネジメントシステム (ISMS) の実践.....	32
6.2.1 ISMS 構築の手順.....	32
6.2.2 取扱い情報の把握.....	34
6.2.3 リスク分析.....	34
6.3 組織的安全管理対策 (体制、運用管理規程).....	37
6.4 物理的安全対策.....	39
6.5 技術的安全対策.....	40
6.6 人的安全対策.....	48
6.7 情報の破棄.....	50
6.8 情報システムの改造と保守.....	51
6.9 情報及び情報機器の持ち出しについて.....	53
6.10 災害等の非常時の対応.....	56
6.11 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.....	60
6.12 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.....	78
7 電子保存の要求事項について.....	81
7.1 真正性の確保について.....	81
7.2 見読性の確保について.....	89
7.3 保存性の確保について.....	92
8 診療録及び診療諸記録を外部に保存する際の基準.....	97
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.....	97
8.1.1 電子保存の3基準の遵守.....	97
8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準.....	98
8.1.3 個人情報の保護.....	105
8.1.4 責任の明確化.....	107
8.1.5 留意事項.....	107
8.2 電子媒体による外部保存を可搬媒体を用いて行う場合.....	107
8.3 紙媒体のままで外部保存を行う場合.....	107
8.4 外部保存全般の留意事項について.....	108
8.4.1 運用管理規程.....	108
8.4.2 外部保存契約終了時の処理について.....	108
8.4.3 保存義務のない診療録等の外部保存について.....	109
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.....	110
9.1 共通の要件.....	110
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.....	113
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.....	114
9.4 調剤済み処方箋をスキャナ等で電子化し保存する場合について.....	115
9.5 (補足) 運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合.....	115
10 運用管理について.....	117
付則1 電子媒体による外部保存を可搬媒体を用いて行う場合.....	126
付則2 紙媒体のままで外部保存を行う場合.....	133
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	
付録 (参考) 外部機関と診療情報等を連携する場合に取り決めるべき内容	

「審査基準」



「医療情報システムの安全管理に関するガイドライン」
約300の審査項目！

「医療介護関係事業者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」
約70の審査項目！



お問い合わせ



P I C C

株式会社 P I C C 個人情報審査センター

〒105-0013東京都港区浜松町1-21-5 薩田2階

[TEL:03-5777-2117](tel:03-5777-2117)

<http://www.picc.co.jp/>



☆運営協会

特定非営利活動法人 日本個人・医療情報管理協会 (JAPHIC)

(Japan Association of Personal and Healthcare Information Control)

<http://www.japhic.jp/index.php>