「特定健診・特定保健指導の実施に係る個人情報保護ガイドライン」の概要

本ガイドラインは、特定健診・特定保健指導事業の開始に先立ち、「特定健診・特定保健指導事業の実施に関する検討委員会個人情報分科会」（委員長：(財)新潟県労働衛生医学協会参与　立道　肇）において、平成 20 年２月 29 日に作成されたものです。監修は産業医科大学の堀江正知教授です。

ガイドラインは、特定健診・特定保健指導実施機関が行う個人情報保護の具体的施策を示した唯一の指針です。全衛連が平成 17 年３月に発行しました「健康診断機関における個人情報の保護に関するガイドライン　改訂版」を補完するもので、本ガイドラインの概要、個人情報保護のマネジメントシステム運用、要求事項、資料編から構成されています。

なお、本ガイドラインは、全衛連から定価 1,000 円で販売されています。

監修のことば

健康診断の結果の記録は、事業者が労働安全衛生法に基づいて保存し、健康診断を実施した医療機関が医師法や医療法に基づいて保存している。平成 17 年度からは、全面施行された個人情報保護法が、第三者に個人情報を提供する際は、原則として本人の同意が必要であることを規定したことから、（社）全国労働衛生団体連合会は「健康診断機関における個人情報の保護に関するガイドライン改訂版」を発行し、会員機関ではプライバシーマークの取得も進んだ。

ところで、平成 20 年度から施行される高齢者の医療の確保に関する法律は、保険者が事業者に対して健康診断の結果の記録を提供するよう求めた際は、その写しを提供しなければならないことを規定した。すなわち、本人の同意ではなく法律に基づいて第三者に個人の健康情報の提供を行い、保険者、社会保険支払基金、国が、これらの情報を活用する仕組みが確立されようとしている。事業者や保険者は、健康情報の保護と活用の両者を適切に行う体制を整備することが求められるが、医療制度改革や特定健診等の遂行に伴う課題も山積し、手が回らないところも多いのが現実である。

今後、特定健診等の事業では、事業者、保険者、医療機関の間で多彩な契約形態と情報連携が想定される中で、事業者や保険者が、会員機関に対して、個人の健康情報の取扱い方についての助言、指導、マネジメントも依頼してくることが予想される。その際、良質な会員機関を選別する指標として、関係法令や指針に準拠した個人情報保護管理体制の整備、個人情報保護マネジメントシステム文書の作成、法定以外の項目を含めた電子データの授受体制などが評価されると想定される。

本ガイドラインは、（社）全国労働衛生団体連合会が、特定健診等と個人情報

保護の両制度に精通した委員を選抜し、ISMS 主任審査員の森口修逸氏を専門委員に迎えて組織した「特定健診・特定保健指導事業の実施に関する検討委員会個人情報分科会」が、会員機関が特定健診等に関わる個人情報を適切に取り扱うために役立つ知識と情報をまとめたものである。現時点で、特定健診等に特化して個人情報保護のあり方を示した唯一の指針であり、関係者に広く参考となることを期待している。ただ、特定健診等はこれから始まる制度であり、いかなる内容や手続きが標準となるのかについては、これから注目していかなければならないところである。今後、会員各位からのご指導とご意見をいただきながら、改訂する努力を続けていきたいと考えている。

平成 20 年 2 月 29 日

産業医科大学教授
堀江　正知

はじめに

本ガイドラインは、平成 20 年 4 月から施行される特定健康診査・特定保健指導の実施にあたり、健診・保健指導機関が行う個人情報保護の具体的施策に関する指針を示すものです。

個人情報保護法の施行後、その運用については様々な問題が指摘されてきました。しかし、その多くは、法自体の問題というよりは、目的と手段の混同に端を発するものが多いように見受けられます。

「個人情報の利用・開示の自己決定」が確立した権利であることは、いうまでもありません。一方、医療サービスの効率と個人情報の保護が、いわばトレードオフの関係にあることも事実です。

個人情報保護の実施に当たっては、法の規定や業務の経済的合理性のみならず、医療の本来の目的についての充分な認識を根底において、本ガイドラインを活用されるよう切望する次第です。

平成 20 年 2 月 29 日

特定健診・特定保健指導事業の実施に関する検討委員会
個人情報分科会

委員長	立道　肇
委員	難波　英史
委員	小穴　信久
委員	秦　秀男
専門委員	森口　修逸

特定健診・特定保健指導の実施に係る個人情報ガイドライン

（抜粋）

目　　次

特定健診・特定保健指導の実施に係る
個人情報ガイドライン（抜粋）

１．本ガイドラインの概要

「高齢者の医療の確保に関する法律」に基く特定健康診査・特定保健指導の実施に係る契約形態は多様である。代表保険者（契約代表者）または個別医療保険者と契約取りまとめ機関との集合契約に基づいて実施されるもの、個別医療保険者と健診・保健指導機関との個別契約に基づいて実施されるもののほか、労働安全衛生法等に基づく事業者健診における共同事業として委託を受けること等もある。

このため、委託を受ける実施機関の適格性には、特定健康診査・特定保健指導データを厳正に管理できる機関であるか否かが重要である。

（社）全国労働衛生団体連合会（以下、「全衛連」という。）は平成 17 年３月に、「健康診断機関における個人情報の保護に関するガイドライン　改訂版」を発行し、個人情報保護の徹底を図ってきた。この度の特定健康診査・特定保健指導は、一般的な健康診断とは契約形態、実施方法、データの取扱い等が大きく異なることから、本ガイドラインにより前記ガイドラインを補完するものである。

２．個人情報保護のマネジメントシステム運用

1) 適用範囲

全衛連会員機関が医療保険者から委託を受けて実施する特定健康診査･特定保健指導に関する業務に適用する。

３． 要求事項

３．１　一般要求事項

個人情報保護マネジメントシステムを確立し、マネジメントシステム活動（ＰＤＣＡ）を的確に実施する。

３．２　個人情報保護方針

1) 個人情報保護の理念と代表者の責任を明確にする。
2) 個人情報保護方針を制定し公表する。

３．３　計画

３．３．１ 個人情報の特定

特定健診・特定保健指導の実施に必要な情報に限定して、保険者等からの特定健診・特定保健指導の依頼・受付・実施から、保険者に直接、もしくは代行機関・事業者等を経由して保険者に至るまでの結果報告と請求に係る、紙･電子媒体･ネットワーク等の全ての個人情報を特定する。

３．３．２ 法令、国が定める指針その他の規範

実施機関の保有する全ての個人情報に関する法令、国が定める指針その他の規範に適用し、維持する。

３．３．３ リスク等の認識･分析及び対策

1) リスク分析

特定した個人情報について、特定健診・特定保健指導の依頼・受付・実施から保険者及び受診者・利用者への結果報告・請求・保存・消去・廃棄までのライフサイクルに応じたリスク（取扱いの各局面におけるリスク）を認識し分析を定期的に実施する必要がある。また、廃棄の手順（時期、方法、記録等）についても対応する。

2) リスク対策

セキュリティ対策向上の観点から、個人情報を取扱う機器は、特定健診・特定保健指導の結果報告及び請求業務を専用に行う部屋（セキュリティ管理区画）に設置する。送受信機器は、関係者以外の者が不正に使用できないようにするため、パーティション（空間を仕切る取りはずしが可能な壁・間仕切り。）等で仕切るか、送受信機器にカバーをする等の対策を講じる。

３．３．４ 個人情報保護管理体制の整備（資源、役割、責任及び権限）

特定健診・特定保健指導に関するマネジメントシステムを確立・運用し、改善するために必要な体制を整備するとともに資源を用意し、実施機関と保険者・事業所及び代行機関のシステム責任者との連絡体制を明確にする。

３．３．５ 特定健診・特定保健指導に係る手順

特定健診・特定保健指導の受診者・利用者の健康情報を取扱う作業区域で、以下の手順を明確にする。

３．３．６ 計画書

個人情報管理責任者は教育計画書を作成し、個人情報監査責任者は監査計画書を作成し、代表者の承認を得る。

３．３．７ 緊急事態への準備

情報システムの障害・個人情報の漏洩事件の発生等の緊急事態に関しては、個々に対応手順を定め、事故または違反への対処の教育・訓練を年1回以上確実に実施する。

３．４ 実施及び運用

３．４．１ 運用手順

PDCA サイクルに基づく手順とする。

３．４．２ 取得、利用及び提供に関する原則

1) 個人情報の取得にあたっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行う。

2) 適法、かつ、公正な手段によって個人情報を取得する。

3) 特定健診・保健指導のような保健医療を含む特定の機微な個人情報の取得、利用及び提供に当たっては、下記の制限を伴う。

４）個人情報の利用に関しては、利用目的の範囲内で取扱う。

５）あらかじめ、必要な事項を本人に通知または、それに代わる同等の措置を講じたのち、第三者に提供する。

６）個人情報を特定の者との間で共同して利用する場合は、共同利用者が、既に上記１）～５）に示す事項またはそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又は、本人が容易に知り得る状態に置く。

３．４．３　適正管理

１）個人情報の正確性の確保

利用目的の達成に必要な範囲で、正確性を確実にするために、保存期間の設定、バックアップの手順の設定、入力誤り防止、取り違え防止、授受確認　の各項目に関する管理策とその手順を明確にする。

管理策の事例は、添付資料6の「5. 正確性の確保」を参照。

2)　個人情報の安全性の確保のために、組織的な安全対策の他に、物理的・技術的・人的な安全管理対策と、外部委託先の管理を行う。

３．４．４　個人情報に関する本人の権利

開示等については、次の項目に関する手順を明確にする。

1)　開示への対応方法を契約等で明確にする。
2)　本人及び代理人の場合の確認方法を確立しておく。
3)　開示等の手続きは、本人の知りうる状態にする。
4)　本人から求めがある場合は、利用目的を通知する。
5)　本人から訂正、追加、削除、利用停止等の求めがあった場合の対応方法を明確にする。

３．４．５　教育

従事者に対する個人情報保護に関する教育は、教育計画に基づいて下記に掲げる項目を明確にする。

３．５　個人情報保護マネジメントシステム文書

３．５．１　文書の範囲

個人情報保護方針、個人情報保護に関するガイドライン、内部規程、計画書及び記録等。

３．５．２　文書管理

文書の発行･改訂、配付･閲覧、保存･廃棄等の手順を明確にして管理を行う。

３．５．３　記録の管理

特定健診・特定保健指導に係る以下の記録について管理する。

３．６　苦情及び相談への対応

1)　本人からの苦情受付とその対応の迅速化が要求される。その対応の手順を定める。
2)　苦情の受付窓口及び担当者を定め、個人情報保護方針の中に明記する。

３．７　運用の確認

1)　リスク分析を実施した結果、残留リスクを対象とする。
2)　安全管理対策の中で特に必要と判断したもの。
3)　定期的（毎日、1 ヶ月毎、半年毎）または随時に監視を行うが、個人情報取扱責任者及び情報システム責任者が責任を持って対応する。
4)　チェックリスト等により実施し、その記録は残す。

３．８　内部監査

1)　監査責任者は、監査計画を作成し、監査員を選任し、監査の実施及び報告に関する全責任を負う。
2)　監査は、年 1 回以上実施し、特定健診･特定保健指導に係る個人情報取扱い

部署を対象とする。

3) 監査は監査用チェックシートを基に実施する。

4) 指摘事項に対しては、速やかに対応し是正処置及び予防処置の報告を行う。重要な不適合に関しては、原因を除去するための是正処置を計画し、代表者の承認を得たのち実施する。是正処置結果のフォローアップを行う。その結果は、是正処置報告書、予防処置報告書で記録しておく。

5) 監査結果は、代表者に報告する。

３．９　個人情報保護マネジメントシステムの見直し

内部監査終了後、代表者による個人情報保護マネジメントシステムの見直しを行う。

見直しの実施事項については次の各項を考慮し、個人情報保護委員会が行う。見直しの結果については、個人情報保護マネジメントシステムの見直し事項や見直しの結果必要となる資源の確保等を含めた報告書を作成し、個人情報管理責任者及び代表者に報告する。