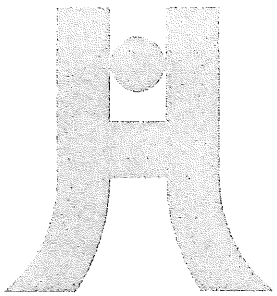
特定健診・特定保健指導の実施に係る
個人情報保護ガイドライン



社団法人 全国労働衛生団体連合会

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
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

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。

2）用語及び定義

a．個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、または個人別に付された番号、記号その他の符号、画像もしくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と組み合わせることによって当該個人を識別できるものを含む。）をいう。

b．特定健康診査

高齢者の医療の確保に関する法律（以下、「高齢者医療確保法」という。）に基づき、医療保険者が40～74歳の被保険者および被扶養者を対象に実施する、特定健康診査（糖尿病その他の政令で定める生活習慣病に関する健康診査をいう）。以下、「特定健診」という。

c．特定保健指導

高齢者医療確保法に基づき、医療保険者が特定健診の結果により健康の保持に努める必要が

あるものとして厚生労働省令で定める者に対し、保健指導に関する専門的知識及び技術を有する者としての厚生労働省令で定める者が行う保健指導をいう(以下、「保健指導」という。)。

d. 医療保険者

健康保険組合、共済組合、国民健康保険組合等、関係法令で定められている医療保険者をいう。特定健診・特定保健指導における実施主体は医療保険者である。(以下、「保険者」という。)

e. 事業所

労働者を雇用して事業活動を行い、労働基準法や労働安全衛生法等の法律が適用される事業場をいう。事業場には法人または個人企業もしくは工場、事務所等がある。

f. 事業者健診

事業者に実施義務が課せられている労働安全衛生法に基づく健康診断をいう。事業者健診の実施義務者等は、保険者から事業者健診の結果のデータ提供を求められた場合は、その写しを提供する。

g. 実施機関

特定健診・特定保健指導に係る機関番号を保有する機関をいう。機関番号は社会保険診療報酬支払基金(以下、「支払基金」という。)に届出て取得する。

h. 受診者

保険者に属する被保険者または被扶養者(40～74 歳)のうち特定健診を受診する者をいう。

i. 利用者

特定健診の結果に基き特定保健指導のサービスを受ける対象に選択された被保険者または被扶養者をいう。

j. 代行機関

医療保険者の付加を軽減するため、医療保険者に代わって、多数の健診・保健指導機関と医療保険者の間に立ち、決済や健診・保健指導データを取りまとめる機関をいう。

k. 代表者

実施機関の代表者または権限を委譲されたその代理権限者をいう。

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。

特定健診・特定保健指導に関する個人情報保護の方針と利用目的を明確にし、公表する。また、保険者・事業者の全てが、受診者・利用者である被保険者・被扶養者に対して健康情報の利用目的を周知していることを確認する。

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。

なお、特定される情報は、特定健診・特定保健指導の作業区域や、特定健診・特定保健指導の結果・請求情報が入力された紙・電子媒体・パソコンのみではなく、ここに到着する以前の特定健診・特定保健指導等の業務に係る個人情報も、特定することが望ましい。

特定した個人情報は、個人情報取扱台帳として整備する。

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。

法令等	・個人情報保護法　同法施行令 ・特定健康診査及び特定保健指導の実施に関する基準（省令 2007 年 12 月 28 日） ・高齢者医療確保法　同法施行令 ・特定健康診査の外部委託に関する基準（告示） ・特定保健指導の外部委託に関する基準（告示） ・労働安全衛生法　同法施行令 ・学校保健法　同法施行令 ・人事院規則等 ・雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（平成 16 年 7 月 1 日告示）

指針その他	・ 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(全衛連) ・ 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 ・雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について ・疫学研究に関する倫理指針 ・個人情報保護マネジメントシステム—要求事項 JIS Q 15001:2006

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。

さらに、特定健診・特定保健指導の作業区域(以下、「作業区域」という。)に到着する以前の個人情報についても、リスク分析することが望ましい。

一般的なリスクに関して、業務の流れとリスクを特定し、安全対策を打つところを、わかりやすく明示することが望まれる。

作業区域は、物理的なセキュリティ区画を設けて管理することが望ましい。セキュリティ区画の分類については、資料6を参照。

特定健診・特定保健指導については、標準化された電子情報で結果報告を行うことに留意する。

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。

特定健診・特定保健指導業務の作業区域をリスク分析で分類したセキュリティ管理区画ごとに、情報(紙媒体・電子媒体)、モノ(フイルム・検体等)、従事者、外来者、本人ごとに、脅威と脆弱性に応じて、個人情報保護の対策を行う。

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。

① 個人情報管理責任者

特定健診・特定保健指導に係る個人情報保護マネジメントシステムの確立及び運用に関する責任者としての役割を果たす。その任命は代表者とする。

② 個人情報監査責任者

客観的な立場から個人情報保護マネジメントシステムの運用状況を監査し、報告を行う。その任命は代表者とする。

③ 個人情報取扱責任者

個人情報保護マネジメントシステム推進組織の各所管部署の責任者であり、代表者から任命される。

④ 情報システム責任者

個人情報保護マネジメントシステムにおいて情報システムの管理に関する責任を有する。その指名は個人情報管理責任者とする。

⑤ 個人情報保護委員会

個人情報保護に関し、PDCA サイクルに基づき個人情報保護マネジメントシステムを推進する。委員会は、個人情報管理責任者の指示に従い、本ガイドラインの見直し、改訂案の作成、個人情報の開示・苦情等に関する審議を行い、そのうち重要事項について個人情報管理責任者を介して代表者に答申する。

委員長は代表者が任命し、委員は所属する各部門の個人情報取扱責任者及び情報システム責任者をもって構成する。委員長は個人情報管理責任者が兼務することを妨げない。

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。

① 各部門及び階層における個人情報を保護するための権限及び責任

② 個人情報を特定する手順

③ 個人情報に関するリスクの認識・分析及び対策の手順

④ 法令，国が定める指針及びその他の規範の特定、参照及び維持

⑤ 個人情報の取得、利用、提供

⑥ 個人情報の適正管理

⑦ 本人からの開示等（利用目的の通知、開示、内容の訂正、追加または削除、利用の停止または消去、第三者提供の停止）の求め

⑧ 苦情への対応

⑨ 個人情報保護に関する教育

⑩ 個人情報保護に関する内部監査

⑪ 内部規定の違反に関する罰則

⑫ 個人情報保護マネジメントシステム文書の管理

⑬ 緊急事態への準備及び対応

⑭ 個人情報保護マネジメントシステムの見直し

特定健診・特定保健指導のみの目的で取り扱う作業区域に到着する以前の特定健診・特定保健指導等の業務に係る個人情報に関する規定も、策定することが望ましい。

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。

① 直接書面で取得する場合は、明示的同意を得ることが望ましいが、少なくとも説明した記録を保管。

② 直接書面以外の方法で取得する場合は、明示的な同意を得る工夫をする。

③ 実施機関が個人情報の提供先を説明し、同意を得る。

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。

① 第三者に提供する目的

② 提供する個人情報の項目

③ 提供の手段または方法

④　当該情報の提供を受ける者または提供を受けるものの組織の種類及び属性

⑤　個人情報の取扱いに関する契約がある場合はその旨

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。

①　共同して利用すること

②　共同して利用される個人情報の項目

③　共同して利用するものの範囲

④　共同して利用するものの利用目的

⑤　共同して利用する個人情報の管理について責任を有するものの氏名または名称

⑥　取得方法

【参考1】　健診結果等及び保健指導記録等の情報の取扱い

出典：「特定健康診査・特定保健指導の円滑な実施に向けての手引」５．１委託基準
（厚生労働省保健局）

１．健診結果等の情報の取扱い

① 特定健康診査に関する電磁的記録を作成し、保険者に対して当該電磁的記録を安全かつ速やかに提出する。

② 特定健康診査の受診者本人への通知に関しては、受診者における特定健康診査の結果の経年管理に資する形式により行われるようにする。

③ 受診者の特定健康診査結果等の保存及び管理が適切になされている。

④ 高齢者の医療の確保に関する法律第 30 条に規定する秘密保持規定を遵守する。

⑤ 個人情報の保護に関する法律及びこれに基づくガイドライン等を遵守する。

⑥ 医療保険者の委託を受けて特定健康診査の結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守する。

⑦ 健診結果の分析等を行うため、保険者の委託を受けて特定健康診査の結果に係る情報を外部に提供する場合には、本来必要とされる情報の範囲に限って提供するとともに、提供に当たっては、個人情報のマスキングや個人が特定できない番号の付与等により、当該個人情報を匿名化する。

２．保健指導記録等の情報の取扱い

① 特定保健指導に関する電磁的記録を作成し、保険者に対して当該電磁的記録を安全かつ速やかに提出する。

② 保健指導に用いた詳細な質問票、アセスメント、具体的な指導の内容、フォローの状況等を保存する場合には、これらを適切に保存・管理する。

③ 個人情報の保護に関する法律及びこれに基づくガイドライン等を遵守する。

④ 医療保険者の委託を受けて特定保健指導の結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守する。

⑤ インターネットを利用した支援を行う場合には、「医療情報システムの安全管理に関するガイドライン」を遵守し、次に掲げる措置等を講じることにより、外部への情報漏洩、不正アクセス及びコンピュータ・ウィルスの浸入等の防止のための安全管理を徹底する。

- 秘匿性の確保のための適切な暗号化、通信の起点及び終点識別のための認証並びにリモートログイン制限機能により安全管理を行う。
- インターネット上で保健指導対象者が入手できる情報の性質に応じて、パスワードを複数設ける（例えば、健診データを含まないページにアクセクスする場合には英数字のパスワードとし、健診データを含むページにアクセスする場合には本人しか知りえない質問形式のパスワードとする等）。
- インターネット上で健診データを入手できるサービスを受けることについては、必ず本人の同意を得る。
- 本人の同意を得られない場合における健診データは、当該サービスを受ける者の健診データとは別の保存場所とし、外部から物理的にアクセスできないようにする。

⑥ 保健指導結果の分析等を行うため、保険者の委託を受けて特定保健指導の結果に係る情報を外部に提供する場合には、本来必要とされる情報の範囲に限って提供するとともに、個人情報のマスキングや個人が特定できない番号の付与等により、当該個人情報を匿名化する。

【参考2】　事業者健診結果の保険者への提供

出典:平成19年度関東地方協議会(平成19年11月21日　東京)　厚生労働省保健局総務課医療費適正化推進室室長補佐　東　史人氏特別講演資料

① 本人同意の要否(個人情報保護法対応)
- 法第27条の規定により、個人情報保護法に関係なく(本人同意なく)提供可能である。ただし、信義上念のため、事業者が健診実施時に、結果を保険者に提供する旨を明示(受診案内等への記載や健診会場での掲示等)することが望ましい。

② 事業者健診結果のうち、特定健診に該当しない項目についての情報提供
- 黙示による同意を得ることで、特定健診項目以外の情報提供が可能である。
- 保険者は、受領したデータのうち特定保健指導の実施等に必要なデータ以外は廃棄し、個人情報保護に十分配慮して取扱う必要がある。

③ 保険者は健診結果を標準的な電磁的記録様式での保存・提出が義務付けられているが、事業者健診の結果様式に特に定めがないことについて
- 事業者や保険者にて標準的な電磁的記録様式で結果を作成するのは負担が大きいことから、保険者・事業者間の協議調整により、事業者は標準的な電磁的記録様式で健診結果を提供できる健診機関(※)を選定する等、結果提供等が両者にとって大きな負担にならないよう連携することが望ましい。

※　支払基金ホームページに掲載されている特定健診受託可能(＝委託基準遵守)機関リストを参考に委託先を選定

④ 健診結果データの送信に関する取り決め、費用負担等について
- 保険者・事業者間の協議調整結果(必要に応じて契約)に基づくが、主に次の点を考慮した協議調整が必要である。
- 健診実施後速やかに保健指導に着手する必要があることから、医療保険者は事業者から健診が済み次第その結果を受領できる体制・流れを定めておくことが必要である。
- 医療保険者のために健診結果データを特別に作成・送付する場合は、それに要した費用を医療保険に請求することに問題はない。

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。

詳細を下記に記す。

① 物理的安全対策:添付資料6の(1)(2)を参照

特定健診・特定保健指導業務を実施する区域を、少なくとも、管理区画・アクセス制限区画・業務区画・一般区画の 4 区画以上に分けて、それぞれの区画において、情報(紙媒体・電子媒体)、モノ(フイルム・検体等)、従事者、外来者、本人(受診者・利用者)等の各々に応じて、下記の個人情報の物理的安全対策を行う。

a. 入退館(室)の管理

b. 個人情報の物理的保存区画への入退管理

c. 盗難、盗視等の防止

d. 機器・装置・情報媒体等の物理的な保護

特定健診・特定保健指導の電子データの送信または納品媒体の保存は、管理区画で、定められた管理者が行うことが望ましい。

② 技術的安全対策:添付資料6の技術的対策例(1)、(2)及び(3)を参照

健診業務を実施する区域を、少なくとも、管理区画・アクセス制限区画・業務区画・一般区画の4区画以上に分けて、それぞれの区画において、情報(紙媒体・電子媒体)、モノ(フイルム・検体等)、従事者、外来者、本人(受診者・利用者)等の各々に応じて、下記の個人情報の技術的安全対策を行う。

a. 情報システム利用者の識別及び認証

b. 情報システムのアクセス権限の管理

c. アクセスの記録(アクセスログ)

d. 不正ソフトウェア対策

e. ネットワーク上からの不正アクセス防止(ファイアウオールの導入)

f. インターネットの利用制限

特定健診・特定保健指導の電子データの送信または納品媒体への保存は、指名された管理者が行っている証拠を確実に残すとともに、当該情報システムがインターネットと接続する時間を極小化する。その結果、外部ネットワークから個人情報が参照されたり、ウィルスが混入することのないようにする。

③ 人的安全対策

下記の個人情報の人的安全対策を行う。

a. 従事者の雇用時及び外部受託者に対する守秘・非開示契約

従事者には、職員・嘱託職員・非常勤職員・派遣者・パートタイマー・アルバイト等を含み、個人情報保護に関し、秘密保持契約を締結する。その内容には、業務上知りえた個人情報を、退職後も漏らしてはならないことを明記する。

b. 従事者に対する教育

従事者には、雇入れ時・業務の着任時・配置変更時・昇格時・退職時のそれぞれに応じた教育を行い、必要な監督については 3.4.3.3 項に従う。

c. 外部委託者が施設内で行った作業内容・作業結果等の確認

外部委託のうち、実施機関に来て個人情報を取扱う者には、委託先の会社での秘

密保持契約を提出させて確認する。

外部委託で、受託先で個人情報を取り扱う場合は、4)項に従う。

d. 従事者の監督

事件・事故を起こした当事者及び事件・事故を知り得た者は、事件・事故の大小にかかわらず、発生した事件・事故についての報告を行う。この報告を怠った者は、「就業規則」により、処分を受ける。

代表者は、「就業規則」に則り罰則の適用を行う。罰則の適用は、実施機関の役員及び従事者であり、派遣会社社員・非常勤職員については、担当者が属する組織との契約関係の中で対応する。

e. 適正管理に関する緊急時の対応

個人情報に係わる過失による事件・事故が認められた場合、個人情報管理責任者は、個人情報保護委員会で事実経過、原因究明、再発防止対策等について審査し、代表者に報告する。

④ 外部委託先の管理

a. 委託先の選定

委託先を選定するに当たり、評価基準を明確にする。

b. 委託契約

次に示す事項を契約によって規定し，十分な個人情報の保護水準を担保する。

◇ 委託者及び受託者の責任の明確化

◇ 個人情報の安全管理に関する事項

◇ 再委託に関する事項

◇ 個人情報の取扱い状況に関する委託者への報告の内容及び頻度

◇ 契約内容が遵守されていることを委託者が確認できる事項

◇ 契約内容が遵守されなかった場合の措置

◇ 事件・事故が発生した場合の報告・連絡に関する事項

◇ 契約終了後の守秘義務に関する事項

c. 委託先に対する監督

委託先に対し、契約事項の遵守状況について、定期または必要に応じて監査を実施する。

◇ 監査項目は主として、個人情報に関する契約内容の遵守状況を確認する。チェックリストにその項目を定める。

◇ 監査結果に基づき予防処置及び是正処置が講じられていることを確認する。

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。

一般には、委託元に開示義務がある。実施機関側で開示する場合は、委託元の保険者・事業所から開示の代理権限が与えられている必要があるので、契約の段階で協議しておく。開示する原本が電子情報か紙情報かも、契約条項に盛り込んでおくことが望ましい。

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。

① 対象：全ての従業者（役職者・パート等も含む）を対象

② 教育項目：個人情報保護に関する教育・内部監査員の育成教育

③ 研修欠席者への対応

④ 教育実施結果の有効性の評価（小テスト、アンケート等）と結果の記録

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。

① 個人情報の取得、利用及び提供に関する記録

② 本人からの開示請求に関する記録

③ 苦情・相談への対応に関する記録

④ その他個人情報マネジメントシステムの運用に関する記録（個人情報の特定、法令・国が定める指針その他の規範、個人情報のリスク分析、教育、緊急事態対応、個人情報の適正化、文書管理、運用確認、監査、是正・予防処置、マネジメントシステムの見直し等）

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。

【コメント】　運用確認の事例

個人別に操作ＩＤを設定できない場合は、端末操作履歴をとるために、操作時に操作者・開始時刻・終了時刻を記入することが規定されるが、その確認のために、毎週もしくは不定期に、記入の運用が行われていることを確認する必要がある。

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。

【コメント】

・ 監査に関しては、教育・訓練なしに真の運用はできない。教育・訓練は、個人情報を第一次的に取得(収集)する部署も含めて、特定健診・特定保健指導に係る部署は全て対象とする。

・ 是正措置は顕在化した不適合の原因を除去するための再発防止活動である。

・予防処置は、潜在する不適合の原因を除去するための未然防止活動である。

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。

① 監査結果及び個人情報保護マネジメントシステムの運用状況に関する報告
② 苦情を含む外部からの意見
③ 前回までの見直しの結果に対するフォローアップ
④ 個人情報の取扱いに関する法令、国の定める指針その他の規範の改正状況
⑤ 社会情勢、国民の認識、技術の進歩等の諸環境の変化
⑥ 実施機関の事業領域の変化
⑦ 内外から寄せられた改善のための提案

資　料　編

資料１　「標準的な健診・保健指導プログラム」（厚生労働省健康局）に記述されている個人情報保護

資料２　「特定健康診査・特定保健指導の円滑な実施に向けた手引」（厚生労働省保健局）に記述されている個人情報保護

資料３　特定健診・保健指導に向けた個人情報保護のポイント（産業医科大学　堀江正知）

資料４　特定健診・特定保健指導における共同利用（エム・ピー・オー　森口修逸）

資料５　アウトソーシング先の責務とガイドラインでの対応

資料６　健康情報システムの安全管理対策事例（エム・ピー・オー　森口修逸）

（１）健診施設のセキュリティ区画

（２）セキュリティ区画と安全管理

（３）技術的対策

（４）健康情報の電子的な保存に伴う運用上の留意事項

（５）個人情報の正確性の確保

資料７　電子的データ授受に伴う情報処理の留意事項

資料１　「標準的な健診・保健指導プログラム」（厚生労働省健康局）に記述されている個人情報保護（抜粋）

第２編　健診

第５章　健診データ等の電子化

（１）健診データ提出の電子的標準様式

１）基本的考え方

○　個人情報の保護には十分に留意する。

（４）生涯を通じた健診情報のデータ管理を行う場合の留意点

１）基本的考え方

○　医療保険者は、被保険者・被扶養者ごとに健診データを整理するため、一意性を保つことができる個人の固有番号を利用することが考えられる。なお、この場合は、個人情報の保護に十分配慮して行う必要がある。

２）個人の固有番号等を利用する場合の考え方

○　既存の保険者番号（法別番号と都道府県番号を含んだ８桁の数字）と一意性のある個人の固有番号（例：現在被保険者・被扶養者が使用している被保険者の記号・番号、職員番号、健診整理番号等）を用いる。

○　固有番号は、一度個人に発行した後は、その同じ番号を別の個人に再発行しないことが必要である。例えば、被保険者番号の場合は発行年度の西暦の下２桁を追加することで一意性を保つことができると考えられる。

○　被保険者証の記号・番号が個人毎の番号となっていない場合もあるため、生年月日やカタカナ名等、他の項目と組み合わせて個人を識別するか、枝番号を追加することで対応することが考えられる。

○　医療保険者間を異動した場合は、前に所属していた医療保険者において、健診データ管理に用いられて記号・番号を、異動した医療保険者において新しい被保険者番号等を発行し、差し替えることで、異動後の医療保険者は被保険者の健診データを管理することが可能となる。

第６章　健診の実施に関するアウトソーシング

（１）基本的考え方

○　個人情報については、その性格と重要性を十分認識し、適切に取り扱わなければならず、特に医療分野は、「個人情報の保護に関する基本方針（平成 16 年４月２日閣議決定）等において、個人情報の性質や利用方法等から、特に適正な取扱いの厳格な実施を確保する必要がある分野の一つとされていることから、委託先の事業者は個人情報を適切に取り扱わなければならない。なお、健診結果等の情報を取り扱う業務のみを委託する場合にも、委託先の事業者は（２）④に定める健診結果等の情報の取扱いに関する基準を遵守することが求められる。

（２）具体的な基準

④　健診結果等の情報の取扱いに関する基準

a　本プログラムにおいて定める電子的標準様式により、医療保険者に対して健診結果を安全かつ速やかにＣＤ－Ｒ等の電磁的方式により提出すること。

b　健診の受診者本人への通知に関しては、国が定める標準的な様式に準拠して行われるよう

にすること。

c　受診者の健診結果等が適切に保存・管理されていること。

d　正当な理由がなく、その業務上知り得た健診受診者の情報を漏らしてはならない。

e　個人情報の取扱いについては、個人情報の保護に関する法律及びこれに基づくガイドライン（「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日厚生労働省）、「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）、「国民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17年3月厚生労働省）を遵守すること。

f　医療保険者の委託を受けて健診結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」（平成17年3月厚生労働省）を遵守すること。

g　健診結果の分析等を行うため、医療保険者の委託を受けて健診結果を外部に提供する場合は、本来必要とされる情報の範囲に限って提供すべきであり、個人情報をマスキングすることや個人が特定できない番号を付すことなどにより、当該個人情報を匿名化すること。

第３編　保健指導

第６章　保健指導の実施に関するアウトソーシング

（３）保健指導アウトソーシングの留意事項

８）個人情報の管理

保健指導は対象者の生活そのものを把握することになり、その情報は個人として知られたくない情報であることもある。このため、保健指導を行った場合の記録の漏洩防止や、保健指導実施者に守秘義務をかけるなど、個人情報の管理が重要である。アウトソーシングを行う場合は、事業者がこのような規定を有しているか確認をするとともに、情報の管理状況を定期的に確認する必要がある。

（４）委託基準

１）基本的考え方

○　個人情報については、その性格と重要性を十分認識し、適切に取り扱われなければならず、特に、医療分野は「個人情報の保護に関する基本方針」等において、個人情報の性質や利用方法等から、特に適正な取扱いの厳格な実施を確保する必要のある分野の一つとされており、委託先の事業者は個人情報を適切に取り扱わなければならない。なお、保健指導の記録等の情報を取り扱う業務のみを委託する場合にも、委託先の事業者は２）④に定める保健指導の記録等の情報の取扱いに関する基準を遵守することが求められる。

２）具体的な基準

④　保健指導の記録等の情報の取扱いに関する基準

a　本プログラムにおいて定める電子的標準様式により、医療保険者に対して保健指導対象者の保健指導レベル、効果（腹囲、体重）等を安全かつ速やかにＣＤ－Ｒ等の電磁的方式により提出すること。

b　保健指導に用いた詳細な質問票、アセスメント、具体的な指導の内容、フォローの状況を記載したものが、適切に保存・管理されていること。

c　正当な理由がなく、その業務上知り得た保健指導対象者の情報を漏らしてはならない。

d　個人情報の取扱いについては、個人情報の保護に関する法律及びこれに基づくガイドライン（「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日厚生労働省）、「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）、「国民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17年3月厚生労働省）を遵守すること。

e　医療保険者の委託を受けて健診結果や保健指導結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守すること。

f　インターネットを利用した保健指導を行う場合には、「医療情報システムの安全管理に関するガイドライン」の 6.9 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に規定されているとおり、①秘匿性の確保のための暗号化、②通信の起点・終点識別のための認証、③リモートログイン制限機能により安全管理を行うこと。さらに、①インターネット上で保健指導対象者が入手できる情報の性質に応じて、パスワードを複数設けること（例えば、健診データを含まないページにアクセクスする場合には本人しか知りえない質問形式のパスワードとする等）、②インターネット上で健診データを入手できるサービスを受けることについて必ず本人の同意を得ること、③当該同意を得られない者の健診データは、当該サービスを受ける者の健診データとは別の保存場所とし、外部から物理的にアクセスできないようにすること等により、外部への情報漏洩、不正アクセス及びコンピュータ・ウィルスの浸入等の防止のための安全管理を徹底すること。

g　保健指導結果の分析等を行うため、医療保険者の委託を受けて保健指導結果を外部に提供する場合は、本来必要とされる情報の範囲に限って提供すべきであり、個人情報をマスキングすることや個人が特定できない番号を付すことなどにより、当該個人情報を匿名化すること。

第４編　体制・基盤整備、総合評価

第３章　健診・保健指導の実施・評価のためのデータ分析とデータ管理

（４）個人情報の保護とデータの利用に関する方針

１）基本的な考え方

医療保険者は、健診・保健指導で得られた健康情報の取扱いについては、個人情報の保護に関する法律及びこれに基づくガイドライン等を踏まえた対応を行う。その際には、受診者の利益を最大限に保証するため個人情報の保護に十分に配慮しつつ、効果的・効率的な健診・保健指導を実施する立場から、収集された個人情報を有効に利用することが必要である。

２）具体的な個人情報の保護とデータの利活用の方法

○　個人情報の取扱いについては、個人情報の保護に関する法律及びこれに基づくガイドライン（「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」、「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」、「国民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 17 年３月厚生労働省）を遵守すること。

○　医療保険者の委託を受けて健診結果や保健指導結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守すること。

○　医療保険者は、健診・保健指導データを都道府県に提出する場合には、健診・保健指導データのうち、氏名等の情報をはずし、何らかの整理番号を付番する等により、匿名化されたデータを作成すること。

○　上記の個人情報の保護に係る一定のルールを満たした上で、収集・蓄積された健診・保健指導の実施に係る者が、国・都道府県レベルで使用することができるような仕組みが望ましい。

○　国により都道府県毎に分類され、都道府県へ提供された健診・保健指導に係るデータについては、医療保険者による医療費適正化の一環として、保険者協議会等において、生活習慣病対策の企画立案・評価のために利活用されることが望ましい。

資料２　「特定健康診査・特定保健指導の円滑な実施に向けての手引」（厚生労働省保険局）に記述されている個人情報保護

５.アウトソーシング

５.１　委託基準

５.１.１　特定健康診査の外部委託に関する基準（告示　別表第１）

④　健診結果等の情報の取扱いに関する基準

・特定健康診査に関する電磁的記録を作成し、保険者に対して当該電磁的記録を安全かつ速やかに提出すること。
・特定健康診査の受診者本人への通知に関しては、受診者における特定健康診査の結果の経年管理に資する形式により行われるようにすること。
・受診者の特定健康診査結果等の保存及び管理が適切になされていること。
・高齢者の医療の確保に関する法律第 30 条に規定する秘密保持規定を遵守すること。
・個人情報の保護に関する法律及びこれに基づくガイドライン等を遵守すること。
・医療保険者の委託を受けて特定健康診査の結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守すること。
・健診結果の分析等を行うため、保険者の委託を受けて特定健康診査の結果に係る情報を外部に提供する場合には、本来必要とされる情報の範囲に限って提供するとともに、提供に当たっては、個人情報のマスキングや個人が特定できない番号の付与等により、当該個人情報を匿名化すること。

５.１.２　特定保健指導の外部委託に関する基準（告示　別表第２）

④　特定保健指導の記録等の情報の取扱いに関する基準

・特定保健指導に関する電磁的記録を作成し、保険者に対して当該電磁的記録を安全かつ速やかに提出すること。
・保険者の委託を受けて、保健指導に用いた詳細な質問票、アセスメント、具体的な指導の内容、フォローの状況等を保存する場合には、これらを適切に保存・管理すること。
・高齢者の医療の確保に関する法律第 30 条に規定する秘密保持規定を遵守すること。
・個人情報の保護に関する法律及びこれに基づくガイドライン等を遵守すること。
・医療保険者の委託を受けて特定保健指導の結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守すること。
・インターネットを利用した支援を行う場合には、「医療情報システムの安全管理にするガイドライン」を遵守し、次に掲げる措置等を講じることにより、外部への情報漏洩、不正アクセス及びコンピュータ・ウイルスの浸入等の防止のための安全管理を徹底すること。
　・秘匿性の確保のための適切な暗号化、通信の起点及び終点識別のための認証並びにリモートログイン制限機能により安全管理を行うこと。
　・インターネット上で保健指導対象者が入手できる情報の性質に応じて、パスワードを複数設けること（例えば、健診データを含まないページにアクセクスする場合には英数字のパスワードとし、健診データを含むページにアクセス場合には本人しか知りえない質問形式のパスワードとする等）。
　・インターネット上で健診データを入手できるサービスを受けることについては、必ず本人の同意を得ること。
　・本人の同意を得られない場合における健診データは、当該サービスを受ける者の健診データとは別の保存場所とし、外部から物理的にアクセスできないようにすること。

・保健指導結果の分析等を行うため、保険者の委託を受けて特定保健指導の結果に係る情報を外部に提供する場合には、本来必要とされる情報の範囲に限って提供するとともに、個人情報のマスキングや個人が特定できない番号の付与等により、当該個人情報を匿名化すること。

5-3　契約

5-3-4　個人情報の保護

委託すべき機関の適格性として、健診における精度管理も重要であるが、極めてセンシティブな個人情報である健診・保健指導データを厳重に管理できる機関であるか否かが非常に重要である。

医療保険者には、個人情報保護法に基づくガイドライン（「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」「国民健康保険組合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」等）が定められており、このガイドラインにおいて委託先の監督が求められていることから、個人情報の厳重な管理や、目的外使用の禁止等を委託契約書に定めるとともに、委託先の契約遵守状況を管理していくことが必要である。

本書巻末の附属資料に示している標準的な契約書の例では、第12条に個人情報の保護の条項を設け、具体的には契約書に附属する別紙として個人情報取扱注意事項を定めてあることから、参考にされたい。

附属資料14　　集合契約における標準的な契約書の例（抜粋）

（個人情報の保護）

第12条　乙および実施機関が当該業務を実施するに当たっては、特定健康診査あるいは特定保健指導の記録の漏洩を防止すると共に、実施担当者には守秘義務を課す等、関係法令を遵守することに加え、別紙個人情報取扱注意事項や「医療・介護関係事業者における個人情報の取扱いのためのガイドライン」（平成16年12月24日医政発第1224001号、薬食発第1224002号、老発第1224002号）及び各都道府県において定める個人情報の取扱いに係る条例等に基づき、必要な個人情報保護対策を講じ、上記の事項やガイドライン等を遵守するものとする。

2　前項の取り決めについては、乙と実施機関との契約等において両者遵守するものとする。

（業務等の調査等）

第13条　甲は、健診・保健指導機関に関する「重要事項に関する規程の概要」に関する乙及び実施機関の公表内容等に関し詳細を確認する等、甲が必要と認めるときは、乙に対し実施機関における業務の実施状況等を照会し、調査及び報告を求めることができる。

2　甲から前項の照会があった場合は、乙は速やかに対応するものとする。

別紙　　**個人情報取扱注意事項**

1　基本的事項

乙及び実施機関は、個人情報の保護の重要性を認識し、この契約による業務の実施に当たっては、個人の権利利益を侵害することのないよう、個人情報を適切に取り扱わなければならない。

2　秘密の保持

乙及び実施機関は、この契約による業務に関して知ることができた個人情報をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

3　収集の制限

(1)　乙及び実施機関は、この契約による業務を処理するために個人情報を収集するときは、

業務の目的を明確にするとともに、業務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

(2)　乙及び実施機関は、この契約による業務を処理するため個人情報を収集するときは、本人から収集し、本人以外から収集するときは、本人の同意を得た上で収集しなければならない。

4　利用及び提供の制限

乙及び実施機関は、この契約による業務に関して知り得た個人情報を契約の目的以外の目的のために利用し、又は第三者に提供してはならない。

5　適正管理

乙及び実施機関は、この契約による業務に関して知り得た個人情報の漏洩、滅失及びき損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。

6　再委託の禁止

乙及び実施機関は、この契約による業務を行うための個人情報の処理は、自ら行うものとし、第三者にその処理を提供してはならない。ただし、乙及び実施機関が、健恭一保健指導機関に関する「運営についての重要事項に関する規程の概要」において血液検査等の実施を委託することを予め明示しており、その明示している内容の範囲において業務の一部を委託する場合には、この限りではない。

7　資料等の返還等

乙及び実施機関は、この契約による業務を処理するために甲から引き渡され、又は乙及び実施機関自らが収集し、若しくは作成した個人情報が記録された資料等は、業務完了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に指示したときは、その指示に従うものとする。

8　従事者への周知

乙及び実施機関は、この契約による業務に従事している者に対して、在職中及び退職後において、その業務に関して知ることのできた個人情報を他に漏らしてはならないこと及び契約の目的以外の目的に使用してはならないことなど、個人情報の保護に関し必要な事項を周知するものとする。

9　実地調査

甲は、必要があると認めるときは、乙及び実施機関がこの契約による業務の執行に当たり取り扱っている個人情報の状況について、随時実地に調査することができる。

10　事故報告

乙及び実施機関は、この契約に違反する事態が生じ、又は生じるおそれがあることを知ったときは、速々かに甲に報告し、甲の指示に従うものとする。

資料３　特定健診・保健指導に向けた個人情報保護のポイント（抜粋）

産業医科大学　堀江正知　（へるすあっぷ 21:2007.8）

・　「健康情報」は、特に機微な情報なので、情報管理やセキュリティを徹底することが必要とされる。

◇ データ取扱者の留意点

・　非医療職がデータを取り扱う場合には、目的を具体的に特定したうえで、特定健診・保健指導の情報をどう取り扱うのかをよく検討し、内容を勝手に解釈したり、加工したりすることがないように注意をすることが大切である。

・　特定健診・保健指導の結果は、今後、後期高齢者医療制度における支援金の算定に影響するという点で、ほかの健康情報よりも機微な情報といえるかもしれない。腹囲等、支援金の算定に関係のある項目はプライバシーの保護には十分な注意が必要になるだろう。

◇ 電子情報の管理上の注意点

・　保険者は特定健診と特定保健指導の結果の記録を電子データで管理する。健診・保健指導を委託した機関からの結果提供、社会保険診療報酬支払基金への結果報告も電子データで行う。

・　電子情報の取扱いについては、「医療情報システムの安全管理に関するガイドライン」の遵守が求められる。

・　具体的には、組織で電子情報の取扱いに関するルールを決め、情報を私用のハードディスクに記録しない、パスワードで不正アクセスを防ぐ、アクセスのログを残すなど物理的、技術的安全策が不可欠になる。

・　また、情報を取り扱う人への教育も必要になる。個人情報にアクセスできる人も限定し、個人情報を連結不可能、匿名化する人を個人情報管理者とすることが望ましい。

◇ 被保険者等へ周知

・　保険者は、ホームページなどの情報伝達手段を用いて、新たな施策の説明に加え、特定健診結果等の利用目的を明確に示すことが必要になる。

◇ 事業者と保険者間における健診結果の取扱い

・　特定健診と労働安全衛生法における一般健診の健診項目が一致する見通しになったことから、被保険者の特定健診データは事業者から提供してもらうことが多いと考えられる。

・　高齢者医療確保法には、事業者は保険者の求めに応じて健診データを提供しなければいけないと規定されている。保険者が事業者からデータを提供してもらうことは、高齢者医療確保法に基づく提供なので、事業者は同意を得る必要はないが、事業者の取得した健診情報が、後に保険者に渡ることを各事業所の衛生委員会等を通じて説明し、労働者に周知しておくことが望ましい。

・　保険者に対して事業者から特定健診のデータ等の提供が求められる場合は、健康管理の目的で利用することなどを明確にしたうえで本人の同意を得るのが原則になる。「特定健康診査等基本方針（案）」では、被保険者に対する就業上の不利益な取扱いを未然に防ぐ観点から、事業者へのデータの流失防止措置を講じることが示されている。

◇ 事業主と共同して保健指導を行う場合

・　事業者と保険者の話し合いのもと、労働安全衛生法における保健指導のなかで特定保健指導を実施することになった場合には、健康情報は共同利用することになる。

・　個人情報保護法は、個人情報を共同利用する場合は、その項目、利用者の範囲、利用目的、および個人データの管理責任者の氏名等について、事前に本人に通知しているとき等においては、第三者提供にあたらないとしている。したがって、この場合は、衛生委員会の審議や

ホームページ等によって共同利用に関する必要事項を周知しておく必要がある。

◇ 他の保険者に提供する場合

・　退職や転職、転居などで加入する保険者が変わった場合など、特定健診等の記録の写しを異動先の保険者の求めに応じ、元の保険者は提供できることになっている。「特定健康診査及び特定保健指導の実施に関する基準(案)(省令案)では、他の保険者に特定健診等の記録を提供する場合には、あらかじめ加入者に対し、情報提供の趣旨、提供される内容について説明を行い、当該加入者の同意を得なければならない（ただし、写しの提供を求めた保険者において説明を行い、加入者の同意を得たときは例外とする）と定めている。

◇ 委託する際の留意点

・　多くの保険者が特定健診・保健指導の実施やデータ管理等を外部機関に委託して行うことになる。
・　委託に際し、保険者と委託先との間で、個人情報の取扱い方を明記した契約を交わす必要がある。また、高齢者医療確保法で委託先にも守秘義務が規定されている。
・　保険者には、委託先に対し、情報漏洩やデータの毀損、滅失等がないように安全管理を徹底するよう監督する義務がある。
・　委託先の事業者が、健診結果の分析等を行うため、健診結果を外部に提供する場合（再委託する場合)、本来必要とされる情報の範囲に限って提供し、個人情報をマスキングすることや個人情報が特定できない番号を付すことなどで、個人情報を匿名化する必要がある。これは「標準的な健診・保健指導プログラム(確定版)」のアウトソーシング基準に示されている。

◇ 保健指導で取得した情報を活用する場合

・　特定保健指導の場では、メタボリックシンドローム以外にもメンタルヘルスなどのさまざまな相談が寄せられることが想定される。その場で得た情報を活用していくべきである。保健指導者が「この情報は早期発見・早期介入につながる」と思ったときは、その情報を活用させてほしいと本人に了解を得たうえで、事業者や上司、家族、医療機関に伝えることはかまわないだろう。たとえ本人が拒否したとしても、本人の生命を守るという目的で必要があれば、最低限の情報は産業医や主治医など、情報を活用してうまく介入してくれる人に伝える必要がある。

◇ ＩＴ等を利用した保健指導の注意点

・　特定保健指導では、電話やメールによる支援が行われるため、対象者には、指導担当者から職場へ電話が来ることも想定される。
・　電話による保健指導で職場に連絡をする場合には、注意を払わないと本人以外の人に保健指導を行っていることが知られてしまう危険性がある。本人に電話でアクセスする際には、職場の人事担当者を介して連絡するなどの配慮が必要である。また、メールで保健指導を行う場合も、パスワードがわかれば他人があけてしまう恐れがあるため、メールに健康情報を書き込むことは、望ましくない。とくにタイトルにはメールの内容がわからないようにする。個人のメールや携帯電話に連絡するほうがのぞまし。その場合はアドレスや電話番号も厳重に管理しなければならない。

資料４　　特定健診・特定保健指導における共同利用

（株）エム・ピー・オー　代表取締役　森口修逸

１．事業者と保険者間における健診結果の取扱い

保険者が事業者（事業所）から特定健診結果データを得ることは、高齢者医療確保法に基づく提供なので、個人情報保護法上、事業者は本人の同意を得る必要はないが、あらかじめ、その旨を受診者になんらかの方法で、事業者と保険者が公表もしくは通知しておくことが望ましい。また、実施機関は、公表されている委託元の個人情報保護方針や利用目的の内容を把握しておく必要がある。

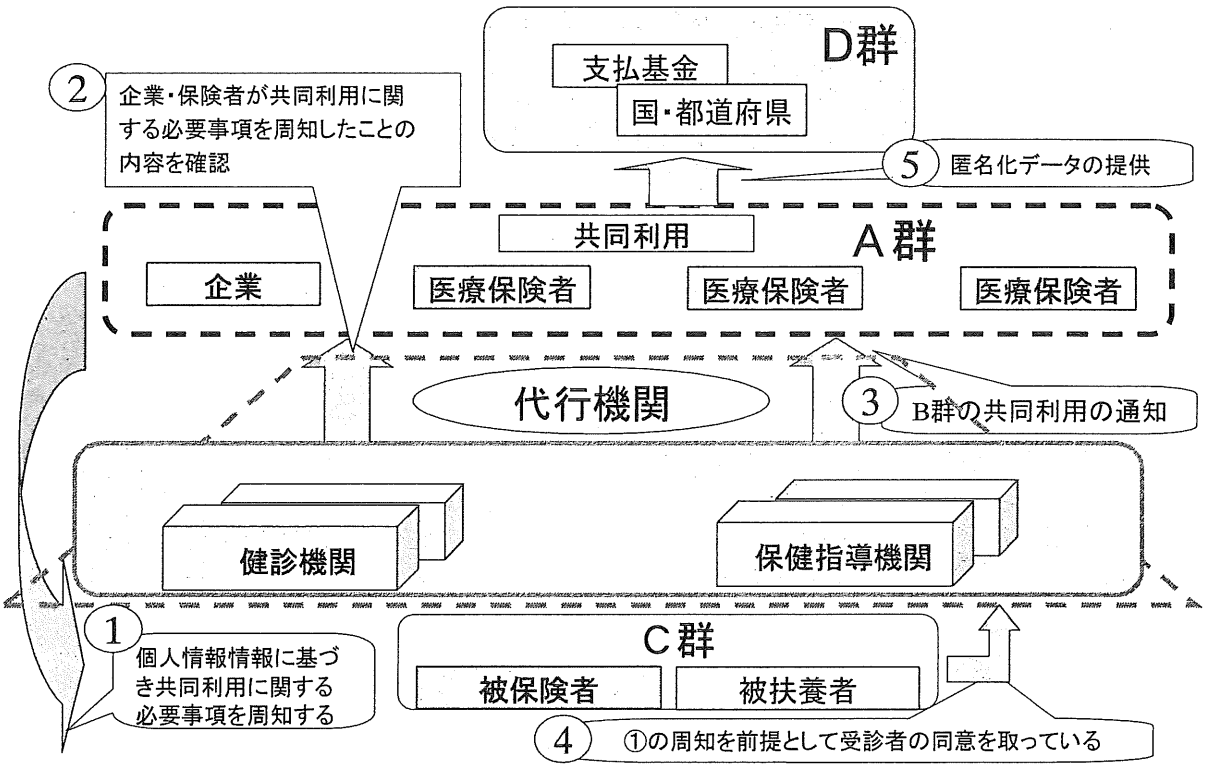


図　特定健診・保健指導における共同利用

２．データを提供する場合

ａ．　実施機関が特定健診・特定保健指導を行うために事業者・保険者のもつデータの提供を受ける場合は、保険者から受診者・利用者に書面で情報提供について周知されていることを事前に確認する。

ｂ．健診機関が連携する保健指導機関に特定健診等の記録を提供する場合には、予め受診者・利用者に対し、情報提供の趣旨、提供の内容について説明を行い、同意を得る。

ｃ．　実施機関は、事業者・保険者が受診者・利用者の個人情報を共同利用して特定健診・特定保健指導等を行う場合、以下の手順で利用目的等をあらかじめ確認しておく。（上図参照）

①　個人情報を共同利用する項目、利用者の範囲、利用目的、及び個人データの管理責任者の氏名等について、事前に本人に通知してあること。（衛生委員会の審議やホームページ等によって共同利用に関する必要事項が周知されていること。）

②　事業者及び保険者が、労働安全衛生法に基づく保健指導のなかで特定保健指導を実施する場合（個人

情報の共同利用)、事業者と保険者は、個人情報保護法に基づき共同利用に関する必要事項を周知されていること。

③　実施機関は委託先のため、受診者・利用者の個人情報を直接共同利用することはない。

④　事業者と保険者等が個人情報を共同利用する場合、共同利用に関する下記の必要事項が周知・公表されていることを確認する。

- 連携する実施機関同士が個人情報を共同利用すること
- 共同して利用される個人データの項目
- 共同して利用する機関の名称
- 共同利用する者の利用目的
- 当該個人データの管理について責任を有する者の氏名または名称

⑤　共同利用するもののうちで、原本の保管責任者を明確にする。

資料５　　アウトソーシング先の責務とガイドラインでの対応

	特定健診結果等の情報の取扱い	特定保健指導記録等の情報の取扱い	対　応
委託先から保険者に対しての電磁的記録による提出	①特定健診に関する電磁的記録を作成し、保険者に対して当該電磁的記録を安全かつ速やかに提出する。	①特定保健指導に関する電磁的記録を作成し、保険者に対して当該電磁的記録を安全かつ速やかに提出する。	【参考1】
委託先から本人に対して経年管理に資する形式	②特定健診の受診者本人への通知に関しては、受診者における特定健診の結果の経年管理に資する形式により行われるようにする。	—	未対応
委託先による結果情報の適切な保管	③受診者の特定健診結果等の保存及び管理が適切になされている。	②特定保健指導に用いた詳細な質問票、アセスメント、具体的な指導の内容、フォローの状況等を保存する場合には、これらを適切に保存・管理する。	3.4.3 適正管理
秘密保持規定の遵守	④高齢者医療確保法第 30 条に規定する秘密保持規定を遵守する。	③高齢者医療確保法第 30 条に規定する秘密保持規定を遵守する。	3.4.3 適正管理
個人情報保護の法律・ガイドライン等の遵守	⑤個人情報の保護に関する法律及びこれに基づくガイドライン等を遵守する。	④個人情報の保護に関する法律及びこれに基づくガイドライン等を遵守する。	ガイドライン全体
「医療情報システムの安全.管理に関するガイドライン」の遵守	⑥医療保険者の委託を受けて特定健診の結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守する。	⑤医療保険者の委託を受けて特定保健指導の結果を保存する場合には、「医療情報システムの安全管理に関するガイドライン」を遵守する。	3.4.3 適正管理
インターネット利用時の「医療情報システムの安全.管理に関するガイドライン」の遵守と付加規定	—	⑤インターネットを利用した支援を行う場合には、「医療情報システムの安全管理にするガイドライン」を遵守し、次に掲げる措置等を講じることにより、外部への情報漏洩、不正アクセス及びコンピュータ・ウィルスの浸入等の防止のための安全管理を徹底する。	3.4.3 適正管理 【参考1】
秘匿性の確保・通信起点終点の相互認証・リモートログイン制限	—	・秘匿性の確保のための適切な暗号化、通信の起点及び終点識別のための認証並びにリモートログイン制限機能により安全管理を行う。	セキュリティ区画と安全管理
本人認証のための複数パスワードの設定	—	・インターネット上で保健指導対象者が入手できる情報の性質に応じて、パスワードを複数設けること（例えば、健診データを含まないページにアクセクスする場合には英数字のパスワードとし、特定健診データを含むページにアクセス場合には本人しか知りえない質問形式のパスワードとする等）。	技術的対策2
本人の同意取得	—	・インターネット上で健診データを入手できるサービスを受けることについては、必ず本人の同意を得る。	3.4.2 取得、利用及び提供に関する原則

	特定健診結果等の情報の取扱い	特定保健指導記録等の情報の取扱い	対　応
同意取得不可の場合の措置	—	・本人の同意を得られない場合における健診データは、当該サービスを受ける者の特定健診データとは別の保存場所とし、外部から物理的にアクセスできないようにする。	
健診結果情報を外部に提供する場合の匿名化措置	⑦健診結果の分析等を行うため、保険者の委託を受けて特定健診の結果に係る情報を外部に提供する場合には、本来必要とされる情報の範囲に限って提供するとともに、提供に当たっては、個人情報のマスキングや個人が特定できない番号の付与等により、当該個人情報を匿名化する。	⑥保健指導結果の分析等を行うため、保険者の委託を受けて特定保健指導の結果に係る情報を外部に提供する場合には、本来必要とされる情報の範囲に限って提供するとともに、個人情報のマスキングや個人が特定できない番号の付与等により、当該個人情報を匿名化する。	【参考３】

注：特定健康診査・特定保健指導の円滑な実施に向けた手引き

５．アウトソーシング　5-1. 委託基準　5-1-3.特定保健指導の外部委託に関する基準（告示　別表第１及び第２）

資料６

健康情報システムの安全管理対策事例

（株）エム・ピー・オー　代表取締役　森口修逸

（１）健診施設のセキュリティ区画

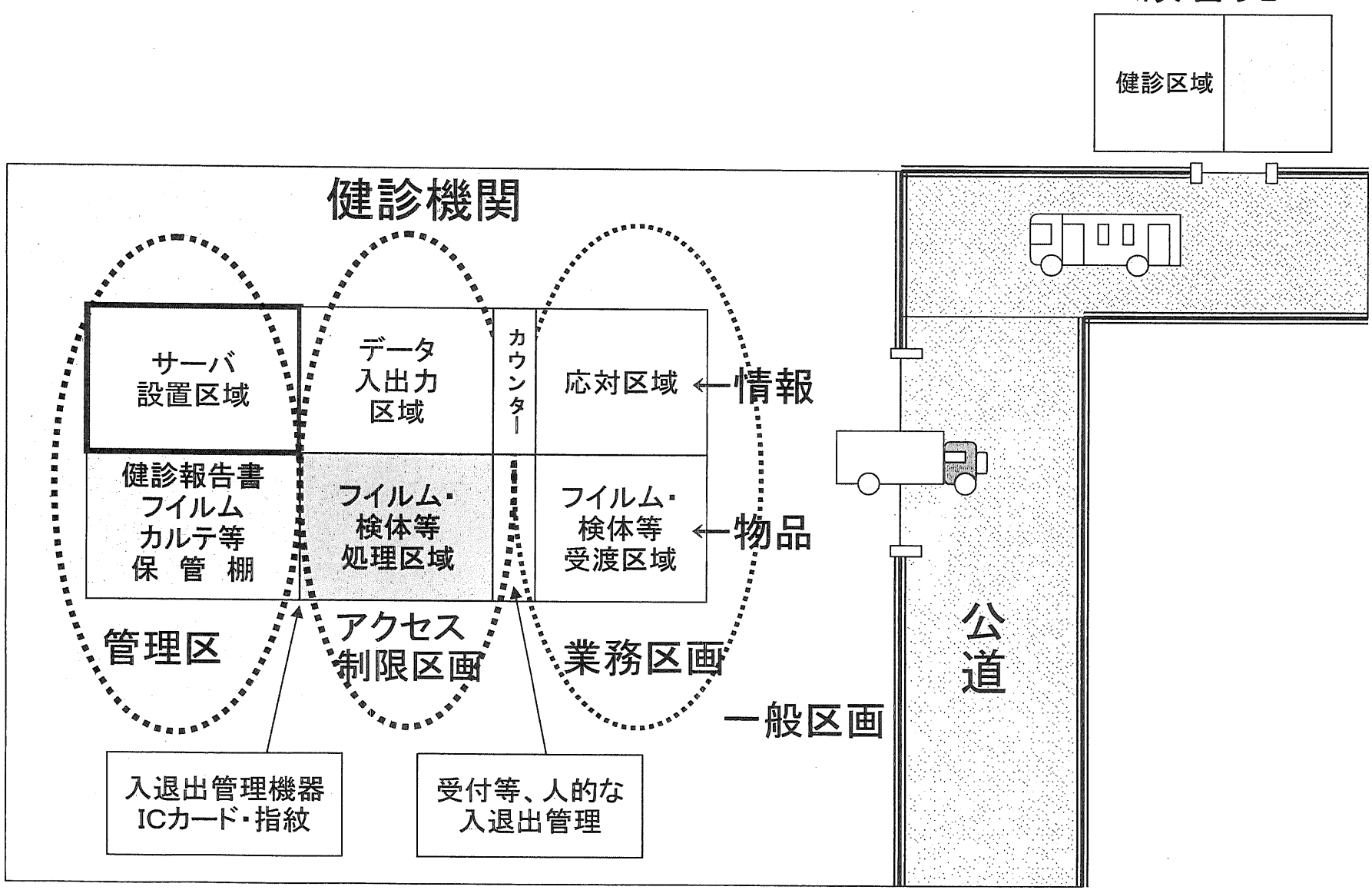
（２）セキュリティ区画と安全管理

（３）技術的対策

（４）健康情報の電子的な保存に伴う運用上の留意事項

（５）個人情報の正確性の確保

（１）健診施設のセキュリティ区画



（2）セキュリティ区画と安全管理

区画		管理対象	物理的対策						
			区画への入退管理			利用時間帯による管理	部屋の鍵管理	防犯設備等	①電子機器の設置 ②モバイル端末持込
				識別証	記録				
管理区画	健診報告書、フイルム、カルテ等保管区域 薬局倉庫、外出健診機器、医療材料等　保管区域 医療機器室 サーバ室	実施機関職員	①限られた担当職員のみ入室可の出入制限 ②限られた担当職員以外の職員が入室する際は、担当職員の同伴が必須 ③入退室記録をとる	職員バッジ着用	入退室記録をとる	時間外・休日の建物・各部屋の入退出は、警備員に連絡	サーバ室・カルテ庫等、各部屋の責任者による厳重な鍵管理	監視カメラ スプリンクラー等	1. 管理区画に設置するサーバに関し、情報システム部の実施事項 ①導入・設置・撤去する場合は、情報セキュリティ管理者の承認を得る ②施設内LANへの接続サーバは、施錠設備のあるサーバールームにまとめて設置し、サーバとサーバ上のデータを保護する。 ③サーバOS、データベース、利用ソフトウエアについて常に最新の状態を保つと同時に、最新のセキュリティパッチとアンチウィルスソフトの定義ファイル（パターンファイル）を適用 ④定期的にサーバのバックアップを行う。 ⑤サーバにセキュリティ侵害や障害が発生した場合は、ただちにサーバをネットワークから切断し、侵害、障害の状況を情報セキュリテイ管理者に報告
		外来の業者等	①限られた担当職員の同伴が必須 ②入退室記録をとる	受付で受取った識別証、もしくはあらかじめ許可を得た、業者自身の写真入り社員章を使用。	入退室記録をとる	時間外・休日の建物・各部屋の入退出は、警備員に連絡			
		患者・受診者の本人・家族等	入室不可						
	モノ	健診報告書、フイルム カルテ等、医薬品、外出健診機器、医療材料等	①整理して保管		持ち込んだ人・日時・棚番等を記録する。	原則、持ち込み持ち出し禁止			
	情報	医療機器、サーバ　等を厳重に管理							
アクセス制限区画	a. 事務オフィス・レントゲン操作室、CT操作室・臨床検査室・薬局等 b. フイルム・検体等　処理区域 c. ナースステーションの患者対応区域を除く部分 d. 医師控え室等、病院職員専用室、医師と患者の面談室 e. 健診データ処理・読影室	実施機関職員	①朝の開錠、夜の施錠を守衛がチェック。それ以外は入退室記録はとらない ②出入制限なし	・職員バッジ着用	・入退室記録は、特にとらない。（受付で入退館記録をとる）	時間外・休日の建物・各部屋の入退出は、警備員に連絡	（CT室・レントゲン室・各倉庫、共用のロッカー、机等の鍵） ・各担当が事務室内の保管庫に収納する。 ・ナースステーションは看護師の常駐を原則とし施錠しない。 ・処置室、観察室等は、通常は施錠しないが、長期間無人となる場合、看護主任が施錠し防災センターに預ける。	ICカード・指紋等による入退室管理	1. アクセス制限区画でのPC等の設置 ①PCは原則として、機密性の高い、独立したアクセス制限区画内で扱う。 ②コピー、FAXの設置を、総務部等管理できる場所に限定し、個人情報の複写・FAXを、決められたルールどおり行わせる。 2. PCの管理（1）：アクセス制限区画内 情報システム部は、PCの設置、移設、廃棄の管理を行う。 ①PCを設置する場合は、担当部署が「パソコンの設置申請書」を情報システム部が承認。 ②PCの勝手な移設は不可 ③許可なく私物PC等を持ち込み・接続・利用は不可 ④PCの利用開始、及び再インストール時は、必ず、OSのバージョンと最新のセキュリティ・パッチを推奨し管理。 　新たなソフトウエアをインストールする場合は許可を得る ⑤クライアントPCのセキュリティ・パッチ適用設定（Windowsなら「WindowsUpdate」機能）を自動適用に設定 ⑥メール設定：ウィルスへの防御上、電子メールソフトウエアをHTMLメールでなく、テキストメールで送信するよう設定 ⑦補助記憶媒体の付いた装置を外部に修理依頼する場合は、個人情報を含む機密情報を再生できない方法で消去した後に修理依頼。 3. PCの運用（1）：アクセス制限区画内 ①PCには、必ずログインパスワードを設定 ②帰宅時にはPCをログオフし、電源を切る ③電子記録媒体書き込みは許可された者以外は禁止 ④盗難による最低限のリスクを避けるために、パスワード設定及び、盗み見からの防御手段としてのパスワード付きスクリーンセーバの設　定やセキュリティフィルタを装着
		外来の業者等	①部屋毎に出入制限あり、職員の許可を得て、職員同伴の際に入室可 ②入退館記録をとる ③外来バッジ着用	・受付で受取った外来者識別証、もしくはあらかじめ許可を得た、業者自身の写真入り社員章を使用。	・入退室記録は、特にとらない。（受付で入退館記録をとる）	・職員が一人でもいない限り休診日・時間外は、外来者の入室不可。			
		患者・受診者の本人・家族等	・医師又は看護師の同席を必要とする。 ・ナースステーションで貸与する名札を着用する。	・不要 ・原則立ち入り禁止（入室必要時は職員の同行必須）。	患者・受診者本人および保護者以外の家族・知人等は、入退室記録をとる（受付で入退館記録をとる）	・特に定めない。			
	モノ	点滴ボトル・分封した医薬品・尿袋	①退社時には鍵のついたロッカーに保管 ② 各室内の個人情報については、外来者が接触できないように管理する。		・特に個別に取り扱うことはない。	・原則、持ち込み持ち出し禁止	・職員が取り扱わないときは、施錠した箱に入れる。		
	情報	検診票・画面・電子媒体・検査伝票・フイルム・カルテ・レセプト等							

業務区画	a. 取引先業者等との打合せスペース、検査センターや宅配便業者等との物品の受渡しを行う場所 b. 健診を行う場所・診察室・病棟 c. ナースステーション内の患者対応区域 d. 処置室、観察室、手術室等、患者への治療を行う区域	実施機関職員	①朝の開錠、夜の施錠を守衛がチェック。それ以外は入退室記録はとらない ②出入制限なし	・職員バッジ着用	朝の開錠、夜の施錠を守衛がチェック。それ以外は入退室記録はとらない	①平日・診療時間内のみ患者・業者の入室可。 ②休日・時間外に入る業者は、守衛等に届出	①ロッカー、机等の鍵は、各担当が管理する。 ②部屋の鍵は、職員の最終退出者が施錠し、守衛室に預ける。 ③ナースステーションは看護師の常駐を原則とするため施錠しない。 ④ 医師控え室等は、最終退室者が施錠し、守衛室に預ける。	守衛に依存	2. PCの管理(2):業務区画内 情報システム部は、PCの設置、移設、廃棄の管理を行う。 ①PCを設置する場合は、担当部署が「パソコンの設置申請書」を情報システム部が承認。 ②PCの勝手な移設は不可 ③許可なく私物PC等を持ち込み・接続・利用は不可 ④PCの利用開始、及び再インストール時は、必ず、OSのバージョンと最新のセキュリティ・パッチを推奨し管理 新たなソフトウエアをインストールする場合は許可を得る ⑤クライアントPCのセキュリティ・パッチ適用設定(Windowsなら「WindowsUpdate」機能)を自動適用に設定 ⑥メール・インターネットは使用禁止のため、メールソフト・ブラウザを削除 ⑦補助記憶媒体の付いた装置を外部に修理依頼する場合は、個人情報を含む機密情報を再生できない方法で消去した後に修理依頼 3. PCの運用(2):業務区画内 患者・受診者・取引先等、権限の無い人が画面を見、操作を行う可能性があるため、操作者は下記に留意する。 ①ログインは、バイオメトリクスが望ましいが、ID／パスワードの場合は、パスワードは英数8バイト以上、3ヶ月未満での更新を前提 ②盗難による最低限のリスクを避けるために、パスワード設定及び、盗み見からの防御手段としてのセキュリティフィルタを装着 ③離席時にはパスワード付きスクリーンセーバーで参照不可とするよう、1分以内に設定 ④帰宅時にはPCをログオフし、電源を切断
		外来の業者等	①出入制限なし ②入退室記録はとらない ③受付にある内線電話で受付担当者と連絡を取り、 a. 実施機関職員と取引先業者等との打合せ、検査センターや宅配便業者等との物品の受渡しを行う b. 受診者・患者は診療スペースへ入室 ④ 外来者の長時間作業で従業員が同伴できない場合は、事前申請が必要。(申請書様式を作成要)	受付で受取った外来者識別証、もしくはあらかじめ許可を得た、業者自身の写真入り社員章を使用。					
		患者・受診者の本人・家族等	①出入制限なし ②入退室記録は不要 ③ 職員が不在時は、外来者及び患者は入室不可。	不要					
	モノ	点滴ボトル・分封した医薬品・尿袋	・各室内の個人情報については、外来者が接触できないように管理する。		・特に個別に取り扱うことはない。	・個人情報は原則、持ち込み持ち出し禁止	・職員が取り扱わないときは、施錠した箱に入れる。	・ワイヤ等での盗難防止	
	情報	健診票・画面・検査伝票・フイルム・カルテ・レセプト・媒体等							
一般区画	入口から受付のスペース、待合室、病院内廊下、健診機関内廊下、守衛室の窓口付近	実施機関職員	不審者立ち入り禁止	職員バッジ着用	朝の開錠、夜の施錠を守衛がチェック。それ以外は入退室記録はとらない	①平日・診療時間内のみ患者・業者の入館可。 ②休日・時間外に入る業者は、守衛等に届出	(病院の出入口2箇所と事務室) ・夜間・休日の鍵の保管・管理は、守衛室にて行う。 ・鍵の授受については、特定職員緒の3名にのみ、守衛室にて行う事が出来る。	守衛に依存	・案内板等に、一般的な案内表示または、本人のみが判別できる記号等で表示(薬局での投薬の出来上がり表示番号等)
		外来の業者等 患者・受診者の本人・家族等		不要					
	あらゆるモノと情報		・個人情報の放置禁止。 ・不在時は鍵をかけること ・一般的な案内表示以外は、記号化・暗号化		・特に個別に取り扱うことはない。	・個人情報は原則、持ち込み持ち出し禁止		・ワイヤ等での盗難防止	
公道・公共区域	公道・公共区域		・他人は規制できない	特になし	特になし	特になし	特になし	警察に依存	なし
	あらゆるモノ		・個人情報の放置禁止。 ・不在時は鍵をかけること		・特に個別に取り扱うことはない。	・個人情報は原則、持ち込み持ち出し禁止	①落し物・忘れ物は遺失物 ②電車の網棚駐車時等の盗難防止に注意	・ワイヤ等での盗難防止	
	情報(インターネット)		・案内表示・ホームページ以外は、記号化・暗号化						
健診顧客先	業務区画 ・フイルム・検体等受渡 ・健診現場	実施機関職員	当該組織に依存	顧客先貸与のバッジ着用	当該組織に依存だが、原則、朝の開錠、夜の施錠を守衛がチェック	当該組織に依存だが、平日時間内のみ受診者・業者の入室可で、個人情報の持込み、持出し可	顧客企業による鍵管理 (盗難防止に注意)	顧客に依存	なし
		受診者の本人・家族等		受診表の携帯等で識別					
	モノ		個人情報の放置禁止 不在時は鍵をかけること		当該組織に依存だが、特に個別に取り扱うことはない。				
	情報								
	顧客先職員		医療職・衛生管理者を除いて、機微な個人情報に触れない	顧客先の管理だが、極力、顧客先の関係者と判別できる措置を依頼					

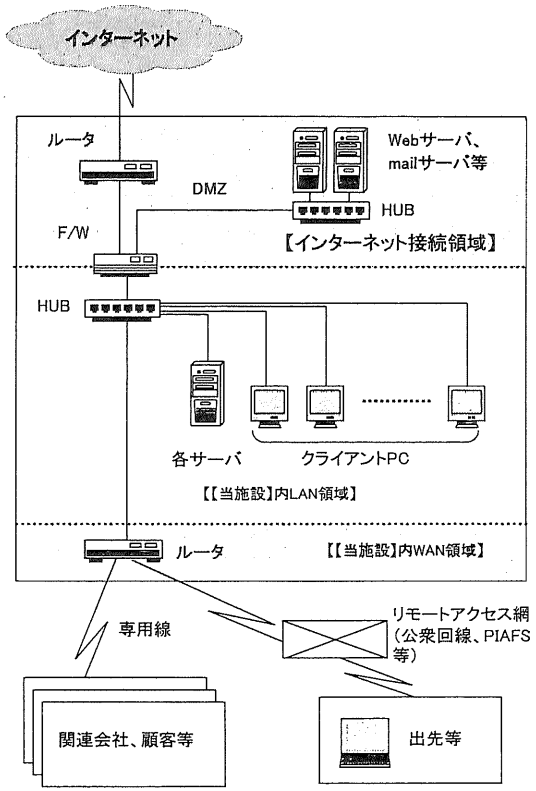
(3)技 術 的 対 策

a．情報システムへのアクセス管理

		管理策	具体例		管理策	具体例		管理策	具体例		管理策	具体例
利用者の識別及び認証	アクセスの識別と認証	①情報システム自身により、利用者の「アクセス権限」を許可	業務システム特有の画面の利用、帳票類の出力、データのダウンロード等	アクセス制御	①利用者本人を識別できる認証の機能を有すること。	指紋による認証や、IDとパスワード認証等	アクセス権限制御	①利用環境に対するアクセス制限。	ルータ、ファイアウォールでのコントロール等	動作確認時対応	①実個人データをテストデータとして使用しない	匿名化したデータか、テスト用に作成したデータを使用
		②利用者のアクセス権限の適宜・迅速な見直し	新規採用・昇格・異動・退職等、人事異動等による利用者の担当業務の変更等に対応		②利用端末の識別と認証を行う	MACアドレス認証、IPアドレス認証等		②情報システムの利用時間帯の制御	業務時間外や休業日でのアクセス禁止制御等		②情報システムの変更時に、運用環境のセキュリティが損なわれないよう検証後、稼働実施	
								③施設の外部からの接続時には、利用者の特別な本人認証を実施	ワンタイムパスワード、チャレンジ-レスポンス、暗号化技術、コールバック等			
アクセス権限の管理	アカウント管理	①新規アカウント、アクセス権限の変更の申請・発行管理を行う部署の設定		ユーザ認証管理	①システム、機器等に、必ずユーザ認証(パスワード)を設定		利用者のパスワード管理	①強固なパスワードの使用	8バイト以上の可変長とし、数字と英字を混在			
		②同一のアカウントを発行しないよう、また、複数の利用者で一つのアカウントを共有しないよう管理			②アカウント(ID)に、必ずユーザ認証(パスワード等)を組合せ			②パスワードの定期的・非定期的変更	3ヶ月以内に変更			
		③人事異動、退職等で不要となったアカウントは、定められた期間内に削除						③パスワードの守秘	口外したり、ヒント的な物品を身の回りに置かない			
								④パスワードを忘れた場合	利用者自身が情報システム部にその処置を依頼			
アクセスログと記録の管理	①定期的に情報システムのアクセスログを取得し、ログの解析を行う。 ②情報システムにアクセス記録機能がない場合は業務日誌等で操作の記録(操作者及び操作内容)を必ず行う。											

b．不正ソフトウエア・不正アクセス対策と管理

不正ソフトウェア対策	情報システム部によるウィルス対策・管理	①全ての利用者PCには、アンチウィルスソフトを導入 ②ウィルス定義ファイル（またはパターンファイル）の自動更新を最低1日1回更新 ③ファイルや電子メールにアクセスがあった場合、ウィルスを自動チェックする自動スキャン機能を有効化 ④PCの補助記憶領域全体のウィルスを定期スキャンする機能を有効にし、最低1週間に一度はスキャン ⑤ウィルス対策窓口を設置し、下記を実施 a．ウィルスに関する最新情報入手 b．セキュリティパッチ情報の実施 c．アンチウィルスソフト	PCユーザの運用上の留意事項	①不審な添付ファイルを開かない ②外部から受け取った電子記録媒体の利用には細心の注意を払う ③クライアントPCには、重要な個人情報ファイルを保存しない ④メール設定：ウィルスへの防御上、電子メールソフトウエアをHTMLメールでなく、テキストメールで送信するよう設定
ネットワーク上からの不正アクセス防止(ファイアウオールの導入等)	インターネット環境と業務システム環境の完全な分離 施設内のネットワーク環境を下記3つの領域で定義	①インターネット領域： インターネットと直接接続するネットワーク領域で、DMZ（非武装中立地帯）を含むグローバル・アドレス領域 ②施設内LAN領域： 施設内のLAN環境領域で、各種サーバ、クライアントPCが接続される領域 IPアドレスは基本的にプライベートアドレスを使用 ③施設内WAN領域： 関連会社及び顧客との間の専用線接続（VPN接続を含む）と、従事者が出先・自宅等からリモート接続可能領域	ネットワーク管理責任部署の実施事項	①ネットワーク機器、サーバは、設置責任者を定め、その一覧表は情報システム部で管理 ②施設内LANへのネットワーク機器の接続は、情報システム部に申請
			施設内WAN接続時の留意点	①情報システム部の許可なく、専用線接続及びリモートアクセス接続のためのネットワーク機器を接続不可 ②外部との接続時、接続する双方の責任者の決定 ③施設外の組織との接続には契約書を作成し、情報システム部の許可を獲得
インターネットの利用制限	業務システム上での利用禁止		インターネット接続環境	①インターネットと直接あるいはDMZを介して接続するネットワーク領域（DMZ上に、Webサーバ、mailサーバ及びDomain Nameサーバ等を設置）



c．紙・電子媒体等の取扱い

紙媒体の廃棄	1）施設内処理	各部門でシュレッダ処理、焼却、または溶融処理したのち廃棄
	2）施設外処理	施設内の指定された場所に提出し、機密保持契約を締結した廃棄業者にシュレッダで裁断し、かつ溶融処理を委託。 （専門の廃棄業者に処分委託の場合、廃棄処理済みを確認するため、マニフェストを要求）
電子媒体・PC等の廃棄・再利用	1）廃棄する場合	物理的に破壊し情報を再生不可にする。
	2）再生利用する場合	専用のデータ消去ソフトウェア等を用いて消去し、情報を再生不可にする。
ハードディスク付き装置等の修理依頼		個人情報を含む機密情報を、専用のデータ消去ソフトウェア等を用いて再生できない方法で消去した後に修理依頼に出す。

（４）健康情報の電子的な保存に伴う運用上の留意事項

a. 健診結果等を従来の紙による保存をせずに、電子的にのみ原本としての証拠性を要求される保存を行う場合、診療録の電子保存の3原則（真正性・見読性・保存性）を満たす必要がある。
［厚生労働省「医療情報システムの安全管理に関するガイドライン」の要求事項］
b. 真正性についての要求事項を早急に対応することが困難な場合は、当面、紙媒体と電子媒体の保存の併用が望ましい。
c. 要求される保存義務の期間（最低5年間）について、見読性と保存性に関して、下記対応を行うこと。

3原則	項目	実施例
真正性	1. 作成者の識別・認証	①利用者識別（生体認証がベター）と職分ごとのアクセス制御 ②運用管理規程と運用責任者の設定
	2. 記録の確定手順確立と作成責任者の識別情報・確定情報登録	①信頼できる時刻、確認画面、ログの取得、虚偽・書換対策 ②確定記録改竄、原本情報送信、 ③作成責任者認証、記録の確定規定
	3. 更新履歴の保存	①ログ情報の取得、照合・参照可能 ②ログの改竄対策、改竄の検知
	4. 代行操作	（略）
	5. 複数の操作者による共同作成	（略）
	7. ルールの遵守	◎従事者教育と運用監査
	8. リモート接続先の作成者の識別・認証	◎リモート保守、他機関からの接続の際の端末もしくは操作者の認証
	9. システムの改造や保守等で診療録等に触れる場合の管理	◎運用管理規程、監査、アクセスログ取得、ソフトウエアの変更管理
	10. 誤入力の防止	◎誤入力防止対策、発生状況の監視と有効性の評価
見読性	1. 個人情報の所在管理	◎紙・媒体等の作成日付ごとの所在管理
	2. 見読化手段の管理	◎記録メデイアに対応した表示手段（読み出し用ドライブ・プログラム等）の確保
	3. 見読目的に応じた応答時間とスループット	◎見読（参照）のための適切な応答時間の確保
	4. システム障害対策としての冗長性の確保	◎ハードデイスク2重化等の冗長なシステム 機器構成
	5. システム障害対策としてのバックアップデータの保存	◎日々のバックアップ取得
	6. システム障害対策としてのバックアップデータの保存　等	◎システム停止時の日常診療対応
保存性	1. ウィルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	◎ウイルス対策
	2. 不適切な保管・取扱による情報の滅失、破壊の防止	①保管場所・保存可能容量・リスク・レスポンス・バックアップ頻度・バックアップ方法の設定 ②許可を受けた人のみ入室可能情報に対するアクセス履歴破壊時のリカバリ
	3. 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止	◎記録媒体劣化対策のバックアップ、及び正常保存期間の明確化
	4. 媒体・機器・ソフトウェアの整合性不備による復元不能の防止	①システム変更時の移行性確保 ②データ移行の開示契約の明確化

（５）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、保存期間の設定手順、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。以下に、その各項目に関する管理策の事例を記す。

<table>
<tr><th>項　目</th><th>事　例</th></tr>
<tr><td>① 保有個人データの保存期間の設定</td><td>顧客先保険者の法的な保存義務の期間以上の保存を前提とし、個々の個人情報及びマネジメントシステムの記録について、保存期間、及び更新すべき期間について「個人情報取扱台帳」及び「記録一覧表」に定める。</td></tr>
<tr><td>② バックアップ手順の規定化</td><td>a．バックアップの確実な取得
媒体を複合化する。また、特定健診・特定保健指導のデータについては、当面、バックアップの観点から、健診結果等の紙媒体と電子媒体の両方を保管する。
b．各処理段階でのバックアップ手順と媒体の保管方法の規定化
処理プロセスごとの標準作業書（手順書）を作成する。</td></tr>
<tr><td rowspan="5">③ 入力誤り防止</td><td>a．入力時の照合・確認手続きの整備</td></tr>
<tr><td>b．保有する個人情報の本人からの申し出・要請への対応措置の規程化</td></tr>
<tr><td>（ア）本人から記載の誤りが指摘、もしくは、記載内容に変更が生じたとの連絡があった場合、速やかに個人情報管理責任者へ報告する。</td></tr>
<tr><td>（イ）保有する個人情報の改訂履歴を保存しつつ迅速に改訂を実施する。
・委託中等、当該個人情報が実施機関の外部に保管され、迅速な改訂が困難もしくは適切でない場合には、個人情報管理責任者がその更新時期を検討し、適切な時期に更新する。</td></tr>
<tr><td>（ウ）個人情報管理責任者は、要請の妥当性を検討し、その判断結果及び修正した場合はその修正結果を本人に報告し、その経緯を記録に残す。
・実施機関内で、指摘以外の関連文書の修正が必要と判断した時は、その検討結果及び対処結果を記録に残す。</td></tr>
<tr><td>（エ）実施機関内で保有する個人情報の修正必要性を発見した場合、個人情報管理責任者がその個人情報改訂の本人への通知可否を検討し、検討結果及び対処結果を記録に残す。
・本人への報告の要否については、個人情報保護委員会で審議する。</td></tr>
<tr><td>c．他所に原本が移動しコピーのみが自機関に存在する、個人情報についての処置</td></tr>
<tr><td rowspan="3">④ 取違え防止等</td><td>a．デジタルデータの活用に関する留意事項
保険者からの入手データのデジタル化を活用し、下記の対応等によりチェックを強化し、業務の正確性を図る。</td></tr>
<tr><td>・受診者・利用者の取違え・誤入力の防止対策
保険者等の受診者・利用者データの活用及び実施工程での名前の確認等により取違え・誤入力の防止
・受診者・利用者・保険者等への郵送先の誤り防止対策
保険組合コード・被保険者記号番号のチェックの強化</td></tr>
<tr><td>b．非デジタルでの個人情報の送受信に関する留意事項
特定保健指導において、はがきやFAXによる支援は原則行わないが、やむをえない場合、個人検査データ等の保護や誤送信に関する管理策を講じる。
個人検査データ等の保護や誤送信に関する管理策を講じる。
・はがきの場合
個人情報保護シール等による個人情報の漏洩防止。
・FAXの場合
検査データ等の個人情報を掲載しない等の対策や、対象者の同意を得たFAX番号に対して、電話でFAX受信の立会いを依頼後ただちに、氏名等の個人識別情報を付さないFAXを送信する等、誤送信防止の対策を講じる。</td></tr>
</table>

項　目	事　例
	a．入手時原本（委託元から入手した申請書、諸伝票・可搬型媒体等）の授受と管理方法
⑤ 授受確認	個人情報の原本が、改ざん、盗難、紛失、破壊、漏洩から守られるよう安全管理対策を施し、受取記録を保存する。受取記録は以下のいずれかによる。 (ア) 台帳で管理する場合 (イ) 台帳に代わる方法で管理する場合 ・ 日付入り確認印の押印による管理 ・ 連名簿、復命簿等による確認 ・ 宅配便等の帳票による管理
	b. 個人情報の授受時におけるチェック強化
	保険組合コード・被保険者記号番号・受診者・利用者データ等によるチェック強化
	c．ネットワークによる授受の場合のログの取得と保管
	送受信の記録を取得し、情報システム責任者により、定期的に運用確認を行う。 ・ 手動送受信の場合：送受信時刻・担当者名・送受信内容等、送受信の記録を残す。 ・ 自動送受信の場合：送受信のログを自動的に取得する。
	a. データの入力及び出力の正確性の確保
	b. データの改変の可能性の減殺等
	c. 責任の所在の明確化 詳細は、「資料5 健康情報システムの安全管理対策の考え方 1．物理的・技術的対策事例 (4)健康情報の電子的な保存のみの場合の留意事項」を参照。
⑥ 電子データの証拠能力及び証明力の確保	個人情報を電子的に取扱うシステムにおいては、下記の事項に特に留意したシステムを構築し、操作者の本人認証・アクセスログ・改訂前後の情報を記録として保存し、原情報及び改訂情報を、法的な記録保存年限に応じて保存する。
⑦ その他必要な対策	相互運用性の確認については、「【添付資料7】電子的データ授受に伴う情報処理の留意事項」を参照。

資料７　　電子的データ授受に伴う情報処理の留意事項

特定健診・特定保健指導の結果及び請求は電子データで管理するため、下記の点に留意する必要がある。

1．実施機関での電子保存を必須の契約条件とした受託

特定健診・特定保健指導の結果等の電子データのみによる保存に関しては、真正性・見読性・保存性の確保が必須のため、特定健診・特定保健指導の契約には注意を要する。実施機関としての保存は、これまで通り，紙媒体等での保存でよいが、委託元から特に、電子保存の要求がある場合は、電子保存の3原則に従う責任を負う。

2．実施機関から外部にて電子保存を委託する場合

電子データの保管能力のある、外部保存先の選定と契約と監督が必要である。要件の詳細は、「医療情報システムの安全管理に関するガイドライン　第9章」を参照。

3．相互運用性の確保

厚生労働省により定められたデータフォーマットで納品することが求められる。

a．情報システムの適用には、ベンダーパッケージのみ使用・ベンダーパッケージのカスタマイズ・実施機関自社開発の3パターンが考えられ、それぞれに関して、コスト・納期等の優位性および、リスクを検討する。

b．適用に関して、納品先との相互運用性の確認が必要である。

c．特に個別契約の場合、直接の納品先は事業所の安全衛生部門で、そののち、保険者に回付される。納品時にはフォーマットがチェックされないため、フォーマット不整合の発見が遅れ、責任の所在が不明確になる可能性があることに留意する。

4．電子的請求に関する留意事項

請求を、紙媒体を使用せず、電子的にのみ行う場合は、「電子商取引に関する管理策」（JIS Q 27002：「情報技術－セキュリティ技術 － 情報セキュリティマネジメントの実践のための規範」10.9）に関する検討が必要である。

5．納品のための媒体条件・セキュリティ条件

個別契約の場合は個々の委託元に、集合契約の場合は契約により定められた指定先に、それぞれ指示された媒体またはネットワーク・セキュリティ条件で納品する。契約時に、納品条件を明確化する必要がある。

6．匿名化処理に関する留意事項

a．処理担当者の任命

個人情報を連結可能もしくは連結不可能匿名化する場合は、代表者から任命された個人情報保護取扱者が行う。コンピュータにより処理するか否かは問わない。

b．モザイクアプローチ可能性の有無等の確認

利用目的に関して、疫学研究の倫理指針等への適合に関する倫理的観点からも、モザイクアプローチによる個人情報の活用の観点（実質的に個人が特定できてしまう場合あり）からの課題に関して、個人情報保護委員会で確認を行う。

特定健診・特定保健指導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　（社）新潟県労働衛生医学協会　参与
委　員　難波　英史　（医社）同友会　常務理事
委　員　小穴　信久　（社福）聖隷福祉事業団　聖隷保健事業部事業管理部部長
委　員　秦　　秀男　（社）岐阜県労働基準協会連合会　労働衛生センター事業推進部部長
委員代理　井上　英樹　（社福）聖隷福祉事業団　聖隷保健事業部事業管理部事務次長
専門委員　森口　修逸　（株）エム・ピー・オー　代表取締役

梶川　　清　（社）全国労働衛生団体連合会　専務理事
事務局　小池　慎也　（社）全国労働衛生団体連合会　企画調整部長

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

平成20年2月29日
1,045円(税込)

編　集　社団法人　全国労働衛生団体連合会
発　行　社団法人　全国労働衛生団体連合会
発行人　梶　川　　清
〒108-0014　東京都港区芝4－4－5
三田労働基準協会ビル
TEL　03-5442-5934
FAX　03-5442-5937