衛生検査所における
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　２月策定
平成２０年１０月改正
社団法人日本衛生検査所協会

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

本ガイドラインは、医療機関等から委託を受けて検体検査業務を遂行する衛生検査所が行う個人情報の適正な取扱いの確保に関する活動を支援するための指針として定めるものである。

２．本ガイドラインの構成及び基本的考え方

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」(平成15年法律第57号、以下「法」という。)第3条において、「個人情報が、個人の人格尊重の理念の下に慎重に取り扱われるべきものである」とされていることを踏まえ、個人情報を取り扱うすべての者は、その目的や様態を問わず、個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならない。

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。以下「基本方針」という。）及び国会における附帯決議において、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であると指摘されており、各衛生検査所における積極的な取組が求められている。

このことを踏まえ、本ガイドラインでは、法の趣旨に則り、衛生検査所における個人情報の適正な取扱いが確保されるよう、遵守すべき事項及び遵守することが望ましい事項をできる限り具体的に示しており、各衛生検査所においては、法令、基本方針及び本ガイドラインの趣旨を踏まえ、個人情報の適正な取扱いに取り組む必要がある。

具体的には、衛生検査所は、本ガイドラインの【法の規定により遵守すべき事項等】のうち、「しなければならない」等と記載された事項については、法の規定により厳格に遵守することが求められる。また、【その他の事項】については、法に基づく義務等ではないが、達成できるよう努めることが求められる。

なお、「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」（以下「省庁ガイドライン」という。）においても「医療機関等から委託を受けた業務を遂行する」事業者は、省庁ガイドラインのⅢ４．に沿って適切な安全管理措置を講ずることが求められている。

また、省庁ガイドラインによれば委託元である医療機関等は、委託先である衛生検査所等が同ガイドラインの趣旨を理解し、同ガイドラインに沿った対応を行う事業者である場合に委託先として選定し、委託先事業者における個人情報の取扱いについて定期的に確認し、適切な運用が行われていることを確認する等の措置を講ずる必要があると規定されている。

そのため、衛生検査所は、検体検査の受託範囲において、善良なる管理者として委託元である医療機関等と同等の注意をもって個人情報を適切に取り扱うことが求められている。

3．本ガイドラインが対象とする事業者の範囲

本ガイドラインが対象としている事業者の範囲は、日衛協を構成する全ての会員衛生検査所である。

法令上、「個人情報取扱事業者」としての義務等を負うのは、識別される特定の個人の数の合計が過去6ヶ月以内のいずれの日においても5,000 を超えない事業者（小規模事業者）を除くものとされている。しかし、省庁ガイドラインにおいては個人情報取扱事業者としての法令上の義務等を負わない医療機関等にも省庁ガイドラインを遵守する努力を求めることとなったため、会員衛生検査所についても規模の大小にかかわらず本ガイドラインを遵守する努力を求めるものである。

4．本ガイドラインの対象となる「個人情報」の範囲

法令上「個人情報」とは、生存する個人に関する情報であり、個人情報取扱事業者の義務等の対象となるのは、生存する個人に関する情報に限定されている。本ガイドラインは、衛生検査所が保有する生存する個人に関する情報のうち、主として検体検査の情報を対象とするものであり、検索可能なように体系的に整理されていない場合でも個人情報に該当する。

なお、省庁ガイドラインにおいては、「患者・利用者が死亡した後においても、医療・介護関係事業者が当該患者・利用者の情報を保存している場合には、漏えい、滅失又はき損等の防止のため、個人情報と同等の安全管理措置を講ずるもの」とされており、衛生検査所の保有する検査を受ける者(以下、「被検者」という。)の情報については、死亡した個人に関する情報も個人情報と同等の安全管理措置を講ずるものとする。しかし、衛生検査所において被検者の生死を判別することは困難であるため、個々の個人情報について格別生死を識別できる形での安全管理措置を求めるものではない。

5．衛生検査所が行う措置の透明性の確保と対外的明確化

法第3条では、個人の人格尊重の理念の下に個人情報を慎重に扱うべきことが指摘されている。

衛生検査所は、個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）及び個人情報の取扱いに関する明確かつ適正な規則を策定し、それらを対外的に公表することが求められる。また、被検者から当該本人の個人情報がどのように取り扱われているか等について知りたいという求めがあった場合は、当該規則に基づき、迅速に必要な措置を行うものとする。

個人情報保護に関する考え方や方針に関する宣言の内容としては、衛生検査所が個人の人格尊重の理念の下に個人情報を取り扱うこと及び関係法令等を遵守すること等を、個人情報の取扱いに関する規則においては、個人情報に係る安全管理措置の概要、本人等からの開示等の手続、第三者提供の取扱い、苦情への対応等について具体的に定めることが考えられる。

会員衛生検査所は、プライバシーポリシーは「(社)日本衛生検査所協会個人情報保護方針」(別表3 参照)に準拠し、個人情報の取扱い規則は「個人情報保護のための安全管理措置に関する解釈と対応策」(別表4 参照)等を参考に策定するものとする。

なお、利用目的等を広く公表することについては、以下のような趣旨があることに留意すべきである。

① 衛生検査所で個人情報が利用される意義について被検者の理解を得ること。

② 衛生検査所において、法を遵守し、個人情報保護のため積極的に取り組んでいる姿勢を対外的に明らかにすること。

6．責任体制の明確化と相談窓口の設置等

衛生検査所は、個人情報の適正な取扱いを推進し、漏えい等の問題に対処する体制を整備する必要がある。このため、個人情報の取扱いに関し、専門性と指導性を有し、事業者の全体を統括する組織体制・責任体制を構築し、規則の策定や安全管理措置の計画立案等を効果的に実施できる体制を構築するものとする。

また、個人情報の取扱いに関し被検者等からの相談や苦情への対応等を行う窓口機能等を整備し、被検者等の立場に立った対応を行う必要がある。

7．個人情報が研究に活用される場合の取扱い

法第50条第1項においては、憲法上の基本的人権である「学問の自由」の保障への配慮から、大学その他の学術研究を目的とする機関等が、学術研究の用に供する目的をその全部又は一部として個人情報を取り扱う場合については、法による義務等の規定は適用しないこととされている。従って、この場合には法の運用指針としての省庁ガイドラインは適用されるものではないが、これらの場合においても、法第50条第3項により、当該機関等は、自主的に個人情報の適正な取扱いを確保するための措置を講ずることが求められていることから、当該機関等の要請に基づき衛生検査所が被検者情報を提供するに当たっては、匿名化を行うほか、医学研究分野の関連指針（「ヒトゲノム・遺伝子解析研究に関する指針」、「遺伝子治療臨床研究に関する指針」、「疫学研究に関する倫理指針」、「臨床研究に関する指針」）とともに省庁ガイドラインの内容についても留意するものとする。

8．臨床試験における個人情報の取扱い

臨床試験は、薬事法及び関係法令(「医薬品の臨床試験の実施の基準に関する省令」(平成9年厚生省令28号)等)の規定や、関係団体等が定める指針に基づいて実施される。この場合、被験者の情報の取扱いにあたって、医師は臨床試験に参加する被験者の識別をコード化して行うこととされており、被験者識別コードと各被験者の対応表は実施医療機関にて保存されることとなっている。従って、通常、検体検査における被験者情報は、匿名化され、他の情報と容易に照合することが

できないため、個人情報には該当しない。しかし、特定の被験者個人が識別可能な状況になった場合は個人情報として適切に取り扱われなければならない。

９．　遺伝学的検査における個人情報の取扱い

遺伝学的検査等により得られた遺伝情報については、本人の遺伝子・染色体の変化に基づく体質、疾病の発症等に関する情報が含まれるほか、その血縁者に関わる情報でもあり、その情報は生涯変化しないものであることから、これが漏えいした場合には、本人及び血縁者が被る被害及び苦痛は大きなものとなるおそれがある。したがって、遺伝学的検査等により得られた遺伝情報の取扱いについては、UNESCO 国際宣言等（別表2 参照）、別表1 に掲げる指針及び関係団体等が定める指針を参考とし、特に留意する必要がある。

また、検査の実施に同意している場合においても、その検査結果が示す意味を正確に理解することが困難であったり、疾病の将来予測性に対してどのように対処すればよいかなど、本人及び家族等が大きな不安を持つ場合が多い。したがって、衛生検査所が、遺伝学的検査を受託する場合には、委託元の医療機関において、臨床遺伝学の専門的知識を持つ者により、遺伝カウンセリングが実施されることなどにより、本人及び家族等の心理社会的支援が行われていることを確認する必要がある。

注）臨床遺伝学および遺伝カウンセリングについての資格としては，日本人類遺伝学会と日本遺伝カウンセリング学会が認定している「臨床遺伝専門医」＜http://jshg.jp＞と「認定遺伝カウンセラー」＜http://www.kitasato-u.ac.jp/gene/dept/proposal.html＞がある.

１０．　検体検査以外の個人情報の取扱い

（1）　医師等医療関係者の個人情報

医師等医療関係者の個人情報は、法の対象であり、法に則り、適正に取得し、適正に取り扱わなければならない。

（2）　相談窓口利用者の個人情報

広報室等の会社相談窓口の利用者から寄せられる情報には、個人情報が含まれる場合が考えられる。従って相談窓口担当者及び連絡を受けた部門の担当者は、法に十分留意して情報を取り扱う必要がある。

（3）　従業者の個人情報

衛生検査所は、従業者の個人情報として、住所、生年月日、学歴、人事評価情報、健康診断情報、家族情報などの情報を有する。これらの取扱いについては、「雇用管理に関する個人情報の適正な取扱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日厚生労働省告示第259号）等を遵守するものとする。

１１．他の法令等との関係

衛生検査所は、個人情報の取扱いにあたり、法、基本方針及び本ガイドラインに示す項目のほか、個人情報保護又は守秘義務に関する他の法令等（刑法、関係資格法等）の規定を遵守しなければならない。

Ⅱ　用語の定義等

１．個人情報（法第２条第１項）

「個人情報」とは、生存する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、その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書き等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているか否かを問わない。

なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。

本ガイドラインは、衛生検査所が保有する検体検査にかかる個人情報を対象とするものであり、整理の形態に関わりなく個人情報に該当する。

（例）下記については、記載された氏名、生年月日、その他の記述等により特定の個人を識別することができることから、匿名化されたものを除き、個人情報に該当する。

○衛生検査所における個人情報の例

検体、検査依頼書、検査結果報告書、委託検査管理台帳、検査結果報告台帳、苦情処理台帳等

２．個人情報の匿名化

当該個人情報から、当該情報に含まれる氏名、生年月日、住所等、個人を識別する情報を取り除くことで、特定の個人を識別できないようにすることをいう。なお、必要な場合には、その人と関わりのない符号又は番号を付すこともある。

このような処理を行っても、事業者内で検体検査関係の個人情報を利用する場合は、事業者内で得られる他の情報や匿名化に際して付された符号又は番号と個人情報との対応表等と照合することで特定の被検者が識別されることも考えられる。法においては、「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの」についても個人情報に含まれるものとされており、匿名化に当たっては、当該情報の利用目的や利用者等を勘案した処理を行う必要がある。

３．個人情報データベース等（法第２条第２項）、個人データ（法第２条第４項）、保有個人データ（法第２条第５項）

「個人情報データベース等」とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した個人情報を含む情報の集合体、又はコンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則（例えば、五十音順、生年月日順など）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態においているものをいう。

「個人データ」とは、「個人情報データベース等」を構成する個人情報をいう。

「保有個人データ」とは、個人データのうち、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有するものをいう。ただし、①その存否が明らかになることにより、公益その他の利益が害されるもの、②６ヶ月以内に消去する（更新することは除く。）こととなるものは除く。

検査等の目的で、医療機関等において被検者から採取された血液等の検体は個人情報に該当し、利用目的の特定等（Ⅲ1．参照）、利用目的の通知等（Ⅲ2．参照）、適正な取得(Ⅲ3．参照)等の対象となることから、医療機関等からの業務委託を受ける衛生検査所は、医療機関等において特定された利用目的の達成に必要な範囲を超えて検体を取り扱ってはならない。また、これらの検査結果については、検索可能な状態として保存されることから、個人データに該当し、正確性の確保(Ⅲ3．参照)、安全管理措置等（Ⅲ4．参照）の対象となる。

また、衛生検査所の保有する検査結果は、あくまで医療機関等からの業務委託にもとづき処理が行われるものであり、衛生検査所が委託元である医療機関等の指示によらず、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供を行うことはできないこと、さらに、当該検査結果は、「診療情報の提供等に関する指針」により患者に対し積極的な提供が求められる診療情報の一部を構成するものであるとはいえ、その開示権限は医療機関の管理者にあり、衛生検査所には認められていない上、「臨床検査技師、衛生検査技師等に関する法律」第19条による守秘義務が課せられているため、衛生検査所が直接被検者に開示することはできないことから、保有個人データには該当しない。

４．本人の同意

個人情報の取扱いに当たって、情報の取得、利用目的の変更等本人の同意を必要とする場合の対応としては、衛生検査所の業務内容が医療機関等との委託契約内容に基づいて定まることから、契約内容に従って業務を遂行する限りにおいて、被検者本人の同意を必要とする場合は委託元においてその手続きが行われているものとして取り扱って差し支えない。

Ⅲ　衛生検査所の義務等

１．利用目的の特定等（法第１５条、第１６条）

（利用目的の特定）
法第十五条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
２ 個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。
（利用目的による制限）
法第十六条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
２ 個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
３ 前二項の規定は、次に掲げる場合については、適用しない。
一　法令に基づく場合
二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（１）利用目的の特定及び制限

衛生検査所が医療機関等から預託（社外の者に業務処理等を委託するために、保有する個人情報を預けること）を受ける個人情報の利用目的は、医療機関等が患者・利用者に対し院内掲示等の方法により公表した利用目的のうち、医療機関との間において締結した委託契約において定まる業務に従うものと考えられるが、検体検査については、医療法第15条の2並びに医療法施行令第4条の6において、「人体から排出され、又は採取された検体の微生物学的検査、血清学的検査、血液学的検査、病理学的検査、寄生虫学的検査又は生化学的検査の業務」と明確に規定されており、基本的には、被検者の個人情報を当該業務の受託以外の目的で利用することはできないものと考えられる。なお、検査料金の請求時に被検者別の請求明細を作成している場合、これも検体検査の受託目的に附帯するものと考えられる。

（２）利用目的による制限の例外

衛生検査所は、検体検査の受託目的の達成に必要な範囲を超えて個人情報を取り扱ってはならないが（法第16条第1項）、同条第3項に掲げる場合については、この限りではない。

① 法令に基づく場合

一般に刑事訴訟法第197条第2項に基づく照会、地方税法第72条の63（個人の事業税に係る質問検査権、各種税法に類似の規定あり）等がある。

警察や検察等の捜査機関の行う刑事訴訟法第197条第2項に基づく照会（同法第507条に基づく照会も同様）は、相手方に報告すべき義務を課すものと解されている上、警察や検察等の捜査機関の行う任意捜査も、これへの協力は任意であるものの、法令上の具体的な根拠に基づいて行われるものであり、いずれも「法令に基づく場合」に該当すると解されている。

② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

（例）

・健康増進法に基づく地域がん登録事業による国又は地方公共団体への情報提供
・がん検診の精度管理のための地方公共団体又は地方公共団体から委託を受けた検診機関に対する精密検査結果の情報提供
・児童虐待事例についての関係機関との情報交換
・医療安全の向上のため、院内で発生した医療事故等に関する国、地方公共団体又は第三者機関等への情報提供のうち、氏名等の情報が含まれる場合

④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

（例）

・国等が実施する、統計報告調整法の規定に基づく統計報告の徴集（いわゆる承認統計調査）及び統計法第8条の規定に基づく指定統計以外の統計調査（いわゆる届出統計調査）に協力する場合

【法の規定により遵守すべき事項】

・ 衛生検査所は、個人情報を取り扱うにあたって、その利用目的をできる限り特定しなければならない。
・ 衛生検査所は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

・ 衛生検査所は、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。なお、本人の同意を得るために個人情報を利用すること（同意を得るために被検者の連絡先を利用して電話をかける場合など）、個人情報を匿名化するために個人情報に加工を行うことは差し支えない。
・ 個人情報を取得する時点で、本人の同意があったにもかかわらず、その後本人から利用目的の一部についての同意を取り消す旨の申出があった場合は、その後の個人情報の取扱いについては、本人の同意が取り消されなかった範囲に限定して取り扱う。
・ 衛生検査所は、合併その他の事由により他の事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
・ 利用目的の制限の例外（法第16条第3項）に該当する場合は、本人の同意を得ずに個人情報を取り扱うことができる。

【その他の事項】
・ 利用目的の制限の例外に該当する「法令に基づく場合」等であっても、利用目的以外の目的で個人情報を取り扱う場合は、当該法令等の趣旨をふまえ、その取り扱う範囲を真に必要な範囲に限定することが求められる。
・ 衛生検査所の保有する検査結果は、あくまで医療機関等からの業務委託にもとづき処理が行なわれるものであり、「法令に基づく場合」等であっても、可能な限り委託元の医療機関等の了解を得てから、警察や検察等の捜査機関へ回答することが望ましい。

２．利用目的の通知等（法第１８条）

（取得に際しての利用目的の通知等）

法第十八条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

２　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

３　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

４　前三項の規定は、次に掲げる場合については、適用しない。

一　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

三　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

四　取得の状況からみて利用目的が明らかであると認められる場合

【法の規定により遵守すべき事項等】

- 衛生検査所は、個人情報を取得するにあたって、あらかじめその利用目的を公表しておくか、個人情報を取得した場合、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
- 利用目的の公表方法としては、事業所内に掲示するとともに、可能な限りホームページへの掲載等の方法により、なるべく広く公表する必要がある。
- 衛生検査所は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

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）

（適正な取得）
法第十七条　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。
（データ内容の正確性の確保）
法第十九条　個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

【法の規定により遵守すべき事項等】
- 衛生検査所は、偽りその他の不正の手段により個人情報を取得してはならない。
- 衛生検査所は、法第23条に規定する第三者提供制限違反をするよう強要して個人情報を取得してはならない。また、他の事業者に指示して不正の手段で個人情報を取得させ、その事業者から個人情報を取得してはならない。
- 衛生検査所は、検体検査の受託という利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

【その他の事項】
- 衛生検査所は、個人データの内容の正確性、最新性を確保するため、具体的なルールを策定したり、技術水準向上のための研修の開催などを行うことが望ましい。

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）

（安全管理措置）
法第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
（従業者の監督）
法第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
（委託先の監督）
法第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（１）衛生検査所が講ずるべき安全管理措置

① 安全管理措置

衛生検査所は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的、及び技術的安全管理措置を講じなければならない。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講ずる。

② 従業者の監督

衛生検査所は、①の安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない。なお、「従業者」とは、当該事業者の指揮命令を受けて業務に従事する者すべてを含むものであり、また、雇用関係のある者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員など）のほか、取締役、執行役、理事、監事等の役員、また、派遣社員等を含むものである。

（２）安全管理措置として考えられる事項

衛生検査所は、その取り扱う個人データの重要性にかんがみ、個人データの漏えい、滅失またはき損の防止その他の安全管理のため、その規模、従業者の様態等を勘案して、以下に示すような取組のほか、「個人情報保護のための安全管理措置に関する解釈と対応策」（別表4 参照）を参考に、必要な措置を行うものとする。特に、安全管理措置を検討するにあたっては、可能な限り、リス

クの源泉となる「個人情報を持たない、作らない」ことを念頭におき、例えば、検体、検査依頼書、同入力票、請求明細書、その他諸報告類について、用途に応じた保存期限を定め、短期間で確実・安全な方法により廃棄するとか、匿名化を行うべきである。

また、同一事業者が複数の施設を開設する場合、当該施設間の情報交換については第三者提供に該当しないが、各施設ごとに安全管理措置を講ずるなど、個人情報の利用目的を踏まえた個人情報の安全管理を行う。

① 個人情報保護に関する規程の整備、公表

・ 衛生検査所は、保有個人データの開示手順を定めた規程その他個人情報保護に関する規程を整備し、相談窓口体制も含めて、ホームページへの掲載を行うなど、被検者等に対して周知徹底を図る。
・ また、個人データを取り扱う情報システムの安全管理措置に関する規程等についても同様に整備を行うこと。

② 個人情報保護推進のための組織体制等の整備

・ 従業者の責任体制の明確化を図り、具体的な取組みを進めるため、個人情報保護に関し十分な知識を有する管理者、監督者等を定めたり、個人情報保護の推進を図るための委員会等を設置する。
・ 各部門や各事業所で行っている個人データの安全管理措置について定期的に自己評価を行い、見直しや改善を行うべき事項について適切な改善を行う。

③ 個人データの漏えい等の問題が発生した場合等における報告連絡体制の整備

・ 個人データの漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合、2) 個人データの取扱いに関する規程等に違反している事実が生じた場合、又は兆候が高いと判断した場合における責任者等への報告連絡体制の整備を行う。
・ 個人データの漏えい等の情報は、苦情等の一環として、外部から報告される場合も想定されることから、苦情への対応を行う体制との連携も図る。（Ⅲ 10. 参照）

④ 雇用契約時における個人情報保護に関する規程の整備

・ 雇用契約や就業規則において、就業期間中はもとより離職後も含めた守秘義務を課すなど従業者の個人情報保護に関する規程を整備し、徹底を図る。なお、特に、臨床検査技師、衛生検査技師については、「臨床検査技師、衛生検査技師等に関する法律第19条」により守秘義務規定が設けられており、その遵守を徹底する。

⑤　従業者に対する教育研修の実施

・　取り扱う個人データの適切な保護が確保されるよう、従業者に対する教育研修の実施等により、個人データを実際の業務で取り扱うこととなる従業者の啓発を図り、従業者の個人情報保護意識を徹底する。

・　この際、派遣労働者についても、「派遣先が講ずべき措置に関する指針」（平成11年労働省告示第138号）において、「必要に応じた教育訓練に係る便宜を図るよう努めなければならない」とされていることを踏まえ、個人情報の取扱いに係る教育研修の実施に配慮する必要がある。

⑥　物理的安全管理措置

・　個人データの盗難・紛失等を防止するため、以下のような物理的安全管理措置を行う。
　－　入退館（室）管理の実施
　－　盗難等に対する予防対策の実施
　－　機器、装置等の固定など物理的な保護

⑦　技術的安全管理措置

・　個人データの盗難・紛失等を防止するため、個人データを取り扱う情報システムについて以下のような技術的安全管理措置を行う。
　－　個人データに対するアクセス管理（ＩＤやパスワード等による認証、各職員の業務内容に応じて業務上必要な範囲にのみアクセスできるようなシステム構成の採用等）
　－　個人データに対するアクセス記録の保存
　－　個人データに対するファイアウォールの設置

⑧　個人データの保存

・　個人データを長期にわたって保存する場合には、保存媒体の劣化防止など個人データが消失しないよう適切に保存する。
・　個人データの保存に当たっては、本人からの照会等に対応する場合など必要なときに迅速に対応できるよう、インデックスの整備など検索可能な状態で保存しておく。

⑨　不要となった個人データの廃棄、消去

・　不要となった個人データを廃棄する場合には、焼却や溶解など、個人データを復元不可能な形にして廃棄する。
・　個人データを取り扱った情報機器を廃棄する場合は、記憶装置内の個人データを復元不可能な形に消去して廃棄する。
・　これらの廃棄業務を委託する場合には、個人データの取扱いについても委託契約において明確に定める。

（3）業務を再委託する場合の取扱い

①　再委託先の監督

衛生検査所は、医療機関等から受託した検査等個人データの取扱いの全部又は一部を再委託する場合、法第20条に基づく安全管理措置を遵守させるよう受託者に対し、必要かつ適切な監督をしなければならない。

「必要かつ適切な監督」には、委託契約において委託者が定める安全管理措置の内容を契約に盛り込み受託者の義務とするほか、業務が適切に行われていることを定期的に確認することなども含まれる。

また、再委託を行う衛生検査所は、医療機関等に対する受託者としての善管注意義務を負うとともに、再委託先に対する監督責任を負うこととなり、業務を再々委託した場合で、再々委託先が不適切な取扱いを行ったことにより、問題が生じた場合は、医療機関等や再委託及び再々委託した衛生検査所が責めを負うこともあり得る。

このため、衛生検査所が再委託又は再々委託を行う場合は、本ガイドラインに沿った対応を行う委託先を選定するとともに、「必要かつ適切な監督」を具体化するため、「個人情報保護に関する覚書(対医療機関用)」（別表5 参照）、「個人情報保護に関する覚書(対検査会社用)」(別表5 参照)を締結する等個人情報の保護が徹底されるよう管理監督しなければならない。

②　業務を委託する場合の留意事項

衛生検査所は、個人データの取扱いの全部又は一部を再委託する場合、以下の事項に留意すべきである。

- 個人情報を適切に取り扱っている事業者を委託先（受託者）として選定する
- 契約において、個人情報の適切な取扱いに関する内容を盛り込む（委託期間中のほか、委託終了後の個人データの取扱いも含む。）
- 受託者が、委託を受けた業務の一部を再々委託することを予定している場合は、再々委託を受ける事業者の選定において個人情報を適切に取り扱っている事業者が選定されるとともに、再々委託先事業者が個人情報を適切に取り扱っていることが確認できるよう契約において配慮する
- 受託者が個人情報を適切に取り扱っていることを定期的に確認する
- 受託者における個人情報の取扱いに疑義が生じた場合（被検者等からの申出があり、確認の必要があると考えられる場合を含む。）には、受託者に対し、説明を求め、必要に応じ改善を求める等適切な措置をとる

(参考)　医療機関等における業者委託に関する関連通知等

上記の留意事項のほか、委託する業務に応じ、関連する通知等を遵守する。

- 「医療法の一部を改正する法律の一部の施行について」（平成5年2月15日健政発第98号）の「第3 業務委託に関する事項」
- 「病院、診療所等の業務委託について」（平成5年2月15日指第14号）

（4）個人情報の漏えい等の問題が発生した場合における二次被害の防止等

個人情報の漏えい等の問題が発生した場合には、二次被害の防止、類似事案の発生回避等の観点から、個人情報の保護に配慮しつつ、可能な限り事実関係を公表するとともに、都道府県の所管課等に速やかに報告する。

【法の規定により遵守すべき事項等】

- 衛生検査所は、その取り扱う個人データの漏えい、滅失又はき損の防止その他個人データの安全管理のために必要かつ適切な措置を講じなければならない。
- 衛生検査所は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
- 衛生検査所は、個人データの取扱いの全部又は一部を再委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

【その他の事項】

- 衛生検査所は、安全管理措置に関する取組を一層推進するため、安全管理措置が適切であるかどうかを一定期間ごとに検証するほか、必要に応じて外部機関による検証を受けることで、改善を図ることが望ましい。

５．個人データの第三者提供（法第２３条）

（第三者提供の制限）

法第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

2　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、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いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

3　個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、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かなければならない。

4　次に掲げる場合において、当該個人データの提供を受ける者は、前三項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、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いているとき。

5　個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、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かなければならない。

（1）第三者提供の取扱い

事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならないとされており、本人の同意を得る必要がある。しかし、そもそも医療機関から預託を受けた個人情報は、検体検査を実施する目的のために利用するものであり、「臨床検査技師、衛生検査技師等に関する法律第19条」の守秘義務を有することからも第三者への提供はできないものである。また、親子兄弟会社・グループ会社の間で個人データを交換する場合も、法により例外と認められる場合を除き、第三者提供とされるので、注意を要する。

省庁ガイドラインでは、医療機関等において本人の同意を必要とするケースとして次の事例をあげているが、衛生検査所においては、回答を行ってはならない。

(例)

・ 民間保険会社からの照会

被検者が民間の生命保険に加入しようとする場合、生命保険会社から被検者の検査結果等について照会があった場合、回答をしてはならない。

・ 学校からの照会

学校の教職員等から、児童・生徒の検査結果に関する問い合わせがあった場合、回答をしてはならない。

・ マーケティング等を目的とする会社等からの照会

健康食品の販売を目的とする会社から、高血圧の被検者の存在の有無について照会された場合や要件に該当する被検者を紹介して欲しい旨の依頼があった場合、被検者の有無や該当する被検者の氏名等を回答してはならない。

（2）第三者提供の例外

ただし、次に掲げる場合については、本人の同意を得る必要はない。

① 法令に基づく場合

医療法に基づく立入検査、児童虐待の防止等に関する法律に基づく児童虐待に係る通告等、法令に基づいて個人情報を利用する場合である。

② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

(例)

・ 健康増進法に基づく地域がん登録事業による国又は地方公共団体への情報提供

・ がん検診の精度管理のための地方公共団体又は地方公共団体から委託を受けた検診機関に対する精密検査結果の情報提供

・ 児童虐待事例についての関係機関との情報交換

・ 医療安全の向上のため、院内で発生した医療事故等に関する国、地方公共団体又は第三者機関等への情報提供のうち、氏名等の情報が含まれる場合

④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

(例)

・ 国等が実施する、統計報告調整法の規定に基づく統計報告の徴集（いわゆる承認統計調査）及び統計法第8条の規定に基づく指定統計以外の統計調査（いわゆる届出統計調査）に協力する場合

（3）「第三者」に該当しない場合

① 他の事業者等への情報提供であるが、「第三者」に該当しない場合

法第23条第4項の各号に掲げる場合の当該個人データの提供を受ける者については、第三者に該当せず、本人の同意を得ずに情報の提供を行うことができる。

(例)

・ 検査等の業務を委託する場合

② 同一事業者内における情報提供であり、第三者に該当しない場合

同一事業者内で情報提供する場合は、当該個人データを第三者に提供したことにはならないので、本人の同意を得ずに情報の提供を行うことができる。

(例)

・ 同一事業者が開設する複数の施設間における情報の交換
・ 当該事業者の職員を対象とした研修での利用（ただし、第三者提供に該当しない場合であっても、当該利用目的が公表されていない場合には、個人が特定されないよう匿名化する必要がある）
・ 当該事業者内で経営分析を行うための情報の交換

（4）その他留意事項

・ 他の事業者への情報提供に関する留意事項

他の事業者への情報提供であっても、①法令に基づく場合など第三者提供の例外に該当する場合、②「第三者」に該当しない場合、③個人が特定されないように匿名化して情報提供する場合などにおいては、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、情報提供する上で必要とされていない事項についてまで他の事業者に提供することがないようにすべきである。

６．保有個人データに関する事項の公表等（法第２４条）

（保有個人データに関する事項の公表等）
法第二十四条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
一　当該個人情報取扱事業者の氏名又は名称
二　すべての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く。）
三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）
四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの
2　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次の各号のいずれかに該当する場合は、この限りでない。
一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合
二　第十八条第四項第一号から第三号までに該当する場合
3　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

（保有個人データの適正な取扱いの確保に関し必要な事項）
令第五条　法第二十四条第一項第四号の政令で定めるものは、次に掲げるものとする。
一　当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
二　当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

（１）被検者からの開示等請求への対応

衛生検査所は、保有する個人データがⅡ.3のとおり保有個人データに該当しないことから、法的には、被検者からの開示等の請求に対応する義務(法第24条～30条)を負わない。

衛生検査所は、被検者に対し、医療機関との委託契約上、自己に対応する権限がないことを通知する。また、守秘義務上問題がなければ、被検者に対し、委託者である医療機関等の名を示した上で医療機関等に対して直接請求するよう案内するとともに、委託契約の趣旨に基づき、医療機関等に対し、被検者より開示

等の請求があったことを報告しなければならない。

（２）その他の開示請求への対応

医師等医療従事者、従業者等の個人情報をデータベースとして保有する場合は保有個人データに該当し、法第24条～第30条の適用を受けることから、適切な対応を行わなければならない。

【法の規定により遵守すべき事項等】

- 衛生検査所は、保有個人データに関し、(ｱ) 当該個人情報取扱事業者の氏名又は名称、(ｲ) すべての保有個人データの利用目的（法第18条第4項第1号から第3号までに規定された例外の場合を除く）、(ｳ) 保有個人データの利用目的の通知、開示、訂正、利用停止等の手続の方法、及び保有個人データの利用目的の通知又は開示に係る手数料の額、(ｴ) 苦情の申出先等について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む）に置かなければならない。
- 衛生検査所は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、上記の措置により利用目的が明らかになっている場合及び法第18条第4項第1号から第3号までの例外に相当する場合を除き、遅滞なく通知しなければならない。
- 衛生検査所は、利用目的の通知をしない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。
- 法施行前から保有している個人情報についても同様の取扱いを行う。

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）

（開示）

法第二十五条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

三　他の法令に違反することとなる場合

2　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの全部又は一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

3　他の法令の規定により、本人に対し第一項本文に規定する方法に相当する方法により当該本人が識別される保有個人データの全部又は一部を開示することとされている場合には、当該全部又は一部の保有個人データについては、同項の規定は、適用しない。

（個人情報取扱事業者が保有個人データを開示する方法）

令第六条法第二十五条第一項の政令で定める方法は、書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）とする。

（１）開示の原則

衛生検査所は、本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、書面の交付による方法等により、遅滞なく、当該保有個人データを開示しなければならない。

但し、衛生検査所が保有する検査結果は、「臨床検査技師、衛生検査技師等に関する法律」第１９条による守秘義務などが課せられているため、保有個人データには該当しない。

（２）開示の例外

開示することで、法第25条第1項の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。第2号の「事業者の業務の著しい支障を及ぼすおそれがある場合」としては、例えば、同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問合せ窓口が占有される

ことによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼす場合があげられる。

【法の規定により遵守すべき事項等】

- 衛生検査所は、本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、遅滞なく、当該保有個人データを開示しなければならない。また、当該本人が識別される保有個人データが存在しないときにその旨知らせることとする。ただし、開示することにより、法第２５条第１項の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。
- 開示の方法は、書面の交付又は求めを行った者が同意した方法による。
- 衛生検査所は、求められた保有個人データの全部又は一部について開示しない旨を決定したときは、本人に対し、遅滞なく、その旨を通知しなければならない。また、本人に通知する場合には、本人に対してその理由を説明するよう努めなければならない（Ⅲ10．参照）。
- 他の法令の規定により、保有個人データの開示について定めがある場合には、当該法令の規定によるものとする。

【その他の事項】

- 法定代理人等、開示の求めを行い得る者から開示の求めがあった場合、原則として本人に対し保有個人データの開示を行う旨の説明を行った後、法定代理人等に対して開示を行うものとする。
- 衛生検査所は、保有個人データの全部又は一部について開示しない旨決定した場合、本人に対するその理由の説明に当たっては、文書により示すことを基本とする。また、苦情への対応を行う体制についても併せて説明することが望ましい。

８．訂正及び利用停止（法第２６条、第２７条）

（訂正等）

法第二十六条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

２　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知しなければならない。

（利用停止等）

法第二十七条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第十六条の規定に違反して取り扱われているという理由又は第十七条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

２　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第二十三条第一項の規定に違反して第三者に提供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

３　個人情報取扱事業者は、第一項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

【法の規定により遵守すべき事項等】

- 衛生検査所は、法第26条、第27条第1項または第2項の規定に基づき、本人から、保有個人データの訂正等、利用停止等、第三者への提供の停止を求められた場合で、それらの求めが適正であると認められるときは、これらの措置を行わなければならない。
- ただし、利用停止等及び第三者への提供の停止については、利用停止等に多額の費用を要する場合など当該措置を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。
- なお、以下の場合については、これらの措置を行う必要はない。
  ① 訂正等の求めがあった場合であっても、(ｱ) 利用目的から見て訂正等が必要でない場合、(ｲ) 誤りである指摘が正しくない場合又は(ｳ) 訂正等の対象が事実でなく評価に関する情報である場合
  ② 利用停止等、第三者への提供の停止の求めがあった場合であっても、手続違反等の指摘が正しくない場合
- 衛生検査所は、上記の措置を行ったとき、又は行わない旨を決定したときは、本人に対し、遅滞なく、その旨を通知しなければならない。また、本人に通知する場合には、本人に対してその理由を説明するよう努めなければならない。

【その他の事項】

- 衛生検査所は、訂正等、利用停止等又は第三者への提供の停止が求められた保有個人データの全部又は一部について、これらの措置を行わない旨決定した場合、本人に対するその理由の説明に当たっては、文書により示すことを基本とする。その際は、苦情への対応を行う体制についても併せて説明することが望ましい。
- 保有個人データの訂正等にあたっては、訂正した者、内容、日時等が分かるように行われなければならない。
- 保有個人データの字句などを不当に変える改ざんは、行ってはならない。

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）

（開示等の求めに応じる手続）

法第二十九条　個人情報取扱事業者は、第二十四条第二項、第二十五条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求め（以下この条において「開示等の求め」という。）に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。

２　個人情報取扱事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、個人情報取扱事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。

３　開示等の求めは、政令で定めるところにより、代理人によってすることができる。

４　個人情報取扱事業者は、前三項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

（手数料）

法第三十条　個人情報取扱事業者は、第二十四条第二項の規定による利用目的の通知又は第二十五条第一項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。

２　個人情報取扱事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

（開示等の求めを受け付ける方法）

令第七条　法第二十九条第一項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる事項は、次に掲げるとおりとする。

一　開示等の求めの申出先

二　開示等の求めに際して提出すべき書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

三　開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

四　法第三十条第一項の手数料の徴収方法

（開示等の求めをすることができる代理人）

令第八条　法第二十九条第三項の規定により開示等の求めをすることができる代理人は、次に掲げる代理人とする。

一　未成年者又は成年被後見人の法定代理人

二　開示等の求めをすることにつき本人が委任した代理人

（1）開示等を行う情報の特定

衛生検査所は、本人に対し、開示等の求めに関して、その対象となる保有個人データを特定するに足りる事項の提示を求めることができるが、この場合には、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した措置をとらなければならない。

また、保有個人データの開示等については、本人の求めにより、保有個人データの全体又は一部が対象となるが、当該本人の保有個人データが多岐にわたる、データ量が膨大であるなど、全体の開示等が困難又は非効率な場合、衛生検査所は、本人が開示等の求めを行う情報の範囲を特定するのに参考となる情報を提供するなど、本人の利便を考慮した支援を行うものとする。

（2）代理人による開示等の求め

保有個人データの開示等については、本人のほか、①未成年者又は成年被後見人の法定代理人、②開示等の求めをすることにつき本人が委任した代理人により行うことができる。

【法の規定により遵守すべき事項等】

- 衛生検査所は、保有個人データの開示等の求めに関し、本人に過重な負担を課すものとならない範囲において、以下の事項について、その求めを受け付ける方法を定めることができる。
  - (ｱ) 開示等の求めの受付先
  - (ｲ) 開示等の求めに際して提出すべき書面の様式、その他の開示等の求めの受付方法
  - (ｳ) 開示等の求めをする者が本人又はその代理人であることの確認の方法
  - (ｴ) 保有個人データの利用目的の通知、又は保有個人データの開示をする際に徴収する手数料の徴収方法
- 衛生検査所は、本人に対し、開示等の求めに関して、その対象となる保有個人データを特定するに足りる事項の提示を求めることができるが、この場合には、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した措置をとらなければならない。
- 保有個人データの開示等の求めは、本人のほか、未成年者又は成年被後見人の法定代理人、当該求めをすることにつき本人が委任した代理人によってすることができる。
- 衛生検査所は、保有個人データの利用目的の通知、又は保有個人データの開示を求められたときは、当該措置の実施に関し、手数料を徴収することができ、その際には実費を勘案して合理的であると認められる範囲内において、手数料の額を定めなければならない。

【その他の事項】

・ 衛生検査所は、以下の点に留意しつつ、保有個人データの開示等の手続を定めることが望ましい。
  - 開示等の求めの方法は書面によることが望ましい。
  - 開示等を求める者が本人（又はその代理人）であることを確認する。
  - 開示等の求めがあった場合、速やかに保有個人データの開示等をするか否か等を決定し、これを開示の求めを行った者に通知する。
  - 保有個人データの開示等の求めに応じる手続を定める場合には、本人に過重な負担を課すものとならない範囲で、方法等を指定することができる。
  - 保有個人データについての開示の可否については、事業者の内部に設置する委員会等において検討した上で速やかに決定することが望ましい。

１０．理由の説明、苦情対応（法第２８条、第３１条）

（理由の説明）

法第二十八条　個人情報取扱事業者は、第二十四条第三項、第二十五条第二項、第二十六条第二項又は前条第三項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。

（個人情報取扱事業者による苦情の処理）

法第三十一条　個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

２　個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めおなければならない。

【法の規定により遵守すべき事項等】

- 衛生検査所は、本人から求められた保有個人データの利用目的の通知、開示、訂正等、利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨本人に通知する場合は、本人に対して、その理由を説明するよう努めなければならない。
- 衛生検査所は、個人情報の取扱いに関する苦情の適切かつ迅速な対応に努めなければならない。また、衛生検査所は、苦情の適切かつ迅速な対応を行うにあたり、苦情への対応を行う窓口機能等の整備や苦情への対応の手順を定めるなど必要な体制の整備に努めなければならない。

Ⅳ ガイドラインの見直し等

１．必要に応じた見直し

個人情報の保護に関する考え方は、社会情勢や国民の意識の変化に対応して変化していくものと考えられる。本ガイドラインについても必要に応じ検討及び見直しを行うものとする。

２．本ガイドラインの発効

本ガイドラインは、平成１７年４月１日に発効するものとする。

別表１　個人情報に関する法令、基本方針、指針及び通知

【法令】

○個人情報の保護に関する法律（平成15年5月30日法律第57号）

○個人情報の保護に関する法律施行令（平成15年12月10日政令第507号）

【基本方針、指針及び通知】

○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）

○労働者の個人情報保護に関する行動指針（平成12年12月20日）

○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日厚生労働省国事第259号）

○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（平成16年10月29日厚生労働省労働基準局長通知）

○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

○個人情報保護に関する法律についての経済産業分野を対象とするガイドライン

○経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン

○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

○「ヒトゲノム・遺伝子解析研究に関する倫理指針」（平成13年3月29日文部科学省・厚生労働省・経済産業省国事第1号）

○「遺伝子治療臨床研究に関する指針」（平成14年3月27日文部科学省・厚生労働省告示第1号）

○「疫学研究に関する倫理指針」（平成14年6月17日文部科学省・厚生労働省告示第2号）

○「臨床研究に関する倫理指針」（平成15年7月30日厚生労働省告示第255号）

別表２ UNESCO 国際宣言等

○「ヒト遺伝情報に関する国際宣言」（UNESCO October 16, 2003）

○「遺伝学的検査に関するガイドライン」（平成１５年８月遺伝医学関連１０学会：日本遺伝カウンセリング学会、日本遺伝子診療学会、日本産科婦人科学会、日本小児遺伝学会、日本人類遺伝学会、日本先天異常学会、日本先天代謝異常学会、日本マススクリーニング学会、日本臨床検査医学会（以上五十音順）、家族性腫瘍研究会）

別表３

社団法人日本衛生検査所協会個人情報保護方針

〔基本的な考え方〕

当協会は、検体検査業を通じて国民の健康の保持増進に寄与することを目的として、事業活動を行っております。この検体検査の受託にあたっては、検査データの高い信頼性と迅速な提供を確保するために、検査を受ける者（以下「被検者」という。）の個人情報を取得いたしますが、これらの情報は、個人の人格尊重の理念の下慎重に取り扱われるべきものと深く認識いたしております。
当協会では、個人情報の重要性の認識に立ち、その適正な取り扱いを確保するため、下記の行動指針を制定し、個人情報保護に関する法令及びその他規範を遵守することを会員衛生検査所に指導してまいります。

〔行　動　指　針〕

1. 基本原則
   - 検体検査の受託にあたり取得する被検者の個人情報を、適切な安全管理措置を講ずることによって保護管理いたします。
   - 個人情報に関する法令及びその他規範を遵守し、さらには当協会の策定したコンプライアンス・プログラムに基づいて個人情報を保護いたします。また、このコンプライアンス・プログラムは適宜見直しを行い、継続的に改善を図ります。
2. 情報収集の原則
   - 検体検査は、医療機関等と個人情報取扱委託契約を結んで実施いたします。
   - 医療機関等より取得する被検者の個人情報は、受託した検体検査の実施に必要な範囲のものといたします。
3. 情報利用の原則
   - 検体検査の受託に際し取得する被検者の個人情報は、受託した検体検査の実施目的以外には利用いたしません。
   - 医療機関等の要請により、医療の向上を目的として検査結果を活用させていただく場合がありますが、被検者氏名など個人を特定できるような形での情報開示は行いません。
4. 情報提供・開示の原則
   - 受託した検体検査の一部を他の検査機関等に再委託する場合は、個人情報を適切に取扱っている検査機関等を選定するとともに、その取扱いについて定期的に確認をいたします。
   - 検査結果は医師の総合的診断における重要な判断情報の一部であり、衛生検査所が被検者本人又はその代理人等に直接、情報提供又は開示等を行うことはありません。

5.　安全管理の原則

- 個人情報保護管理者の設置をはじめ内部における責任体制を確保し、不正アクセス、紛失、改ざん、漏洩等の危険防止を図るため、必要かつ適切な保護措置を講じます。
- 個人情報の適切な保護が確保できるよう、教育研修の実施等を通じて、従業者の個人情報の保護意識の啓発を図ってまいります。
- 検体検査を再委託する場合には、委託先において個人情報保護の措置が確保されるよう、委託契約により、委託元と委託先の責任を明確に定め、定期的に確認をいたします。

本個人情報保護指針に関するご質問、ご意見等につきましては、下記のお問合せ窓口までご連絡ください。

平成16年11月25日

〒102－0084　東京都千代田区二番町五番地
西山興業二番町ビル内

社団法人日本衛生検査所協会　事務局
TEL　03－3262－2326
FAX　03－3234－9669

別表４　個人情報保護のための安全管理措置に関する解釈と対応策

No.	項目・内容	解釈・対応
組織的安全管理措置(①組織体制)		
1	従業者の役割・責任の明確化 （職務分掌規程・職務権限規程・契約書・職務記述書等）	個人情報保護に必要な基本的職務には個人情報保護に関する基本方針及び計画の策定、規程・手順等の整備、教育・研修、監査、苦情・相談、セキュリティ対策実施等があるが、これらの職務を従業者に分担し、役割・責任を明確にして規定する必要がある。 (例) ・　「個人情報保護管理者（CPO)」：組織全体の個人情報コンプライアンスプログラムの統轄責任者(トップマネジメントレベル) ・　「個人情報管理責任者（CPP)」：苦情・相談対応責任者、内部監査責任者、システム運用責任者、教育・研修責任者、セキュリティ対策実施責任者等(本部、事業部、部レベル) ・　「個人情報取扱責任者」：個人情報取扱の実務責任者(課、係、営業所レベル) ・　「個人情報取扱担当者(CPA)」：個人情報取扱の実務担当者(担当者レベル) (注)　組織の必要性によっては、CPO 及び CPP をメンバーとして委員会組織を設け、個人情報保護方針の決定、個人情報保護計画の策定、監査結果等をもとにした個人情報保護計画の評価・改善、危機対応等重要事項の決定を行うことも考えられる。 (個人情報保護規程)
2	個人情報保護管理者(CPO)の設置	個人情報保護に関する最高責任者であり、①個人情報管理責任者(部長レベル)の選任と指揮・監督、②個人情報特定のための手順・方法の確立と指揮・監督、③個人情報保護のための個人情報保護計画の策定(組織、役割、業務方法、研修計画等)、④個人情報保護規程及び計画に規程された事項の実施に関する指揮・監督、違反行為の是正、⑤監査報告に基づく個人情報保護計画等の評価・改善など個人情報保護のコンプライアンスプログラムに全責任を負う者の設置が必要である。社長または管理部門統轄役員が考えられる。(必須事項) (個人情報保護規程)
3	個人データの取扱い(取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業)作業責任者の設置及び作業担当者の限定	医療機関からの検査依頼データ、従業者の人事データ、顧客の属性データ等の個人情報資産については、ライフサイクル毎に作業内容を明確にし、作業責任者を任命するとともに、作業担当者(一般社員、派遣社員、契約社員、アルバイト等)は極力限定する必要がある。 なお、組織的には、No.1 の「個人情報取扱責任者」が作業責任者、「個人情報取扱担当者」が作業担当者に対応する。(情報システム管理規程)

No.	項目・内容	解釈・対応
4	個人データを取り扱う情報システム運用責任者の設置及び担当者(システム管理者を含む)の限定	システムの規模にもよるが、受注処理システム、検査システム、顧客管理システム、請求システム、人事システム、統合データベース、ネットワークシステム等のシステム毎にシステム運用管理者(上記No.1 個人情報取扱責任者)をおき、全体のシステム責任者としてシステム部長等をシステム運用責任者(上記No.1 個人情報管理責任者)とすることが考えられる。 (情報システム管理規程)
5	個人データ取扱いに係わるそれぞれの部署の役割と責任の明確化	個人データの取扱に係わる基本的な職務(個人情報保護に関する基本方針の策定、個人情報保護規程等の制定・改廃、個人情報保護規程等の実施、個人情報保護規程等の教育・研修、個人情報保護規程等の実施状況の監査、苦情・相談対応等)の責任部署を設け、その役割と責任を規定する。 (例) ・ 人事部:「部長は、個人情報保護管理者の指名により、教育担当責任者として、規程に定められた事項を理解し、遵守するための教育訓練を企画・運営する責任を負う。」 (個人情報保護規程)
6	監査責任者の設置	監査責任者は監査の実施とその報告の権限と責任を負う者であり、代表者が監査や情報システムに関する知識はもちろんのこと、個人情報保護や JIS Q15001 に関する知識に習熟している者を指名する必要がある。 (個人情報監査規程)
7	監査実施体制の整備	監査の実施組織は、監査部門を組織の内部に設置する。しかし、独立性、客観性の観点より、個人情報取扱部門と同一でないことが求められる。特に、システム監査人は、情報システム部門に属してはならない。 人材の面で監査部門の設置が困難な場合は、プロジェクトチームの編成や外部のシステム監査企業に委託することも検討する。 (個人情報監査規程)
8	個人データ取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の代表者等への連絡報告体制の整備	事実または兆候の発生部署・レベル（組織階層）毎に、個人情報の種類（検査依頼データ、検査結果データ、人事情報等）とその主管部門等を基準に、個人情報管理組織の構成員（担当者・管理者・責任者）ごとに、各自の報告先・報告方法を規定する。 (個人情報保護緊急時対応規程)

No.	項目・内容	解釈・対応
9	個人データの漏洩等の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への連絡報告体制の整備	個人情報の種類、事故の種類(漏洩、不正アクセス、紛失、改竄、破壊)と規模、事故の状況(日時、場所、原因等)、想定される影響等について個人情報管理組織に基づいて、担当者・管理者・責任者ごとに、各自の報告先・報告方法を規定する。なお、事故については、苦情として外部から情報がもたらされるケースがあるので苦情対応部門との連携を行う必要がある。 (個人情報保護緊急時対応規程、苦情相談規程)
10	漏洩等の事故による影響を受ける可能性のある本人への情報提供体制の整備	漏洩、不正アクセス、紛失、改竄、破壊等の事故に会った個人情報を特定し、その内容を医療機関に対し報告する。その報告内容、報告者、報告方法等について規定する。 (個人情報保護緊急時対応規程、苦情・相談規程)
11	漏洩等の事故発生時における主務大臣及び認定個人情報保護団体（日衛協）への報告体制の整備	漏洩、不正アクセス、紛失、改竄、破壊等の事故に会った個人情報を特定し、その内容を厚生労働大臣及び日衛協に対し報告する。その報告内容、報告者、報告方法等について規定する。 (個人情報保護緊急時対応規程、苦情・相談規程)
組織的安全管理措置(②規程の整備運用)		
1	個人データの取扱に関する規程等の整備とそれらに従った運用	情報の収集、利用、提供、委託、管理、開示・訂正・削除等個人データの取扱に関する基本事項を規程化するとともに、作業マニュアル、使用帳票類の整備を行う。 (個人情報保護規程)
2	個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用	個人情報保護規程に定めるものの内、システムを使って処理する業務についての安全管理措置を定める。規定化にあたっては、下記「組織的安全管理措置個人データの取扱いに関する規程(①～⑤)」の事項について規定する。 (個人情報保護規程、情報システム管理規程)
3	個人データの取扱に係る建物、部屋、保管庫等の安全管理規程等の整備とそれらに従った運用	管理対象設備の特定、管理者の特定、入退室管理簿の制定、入退室手順の制定、施錠管理等について規定する。 (個人情報保護規程、入退室管理規程)
4	個人データの取扱委託にかかる受託者の選定基準、委託契約書のひな型等の整備とそれに従った運用	委託先の安全管理レベルの評価シートを作成し、評価結果に基づき委託先を選定する。そのための評価基準(選定基準)と手順を規定する。 (外部委託管理規程)

No.	項目・内容	解釈・対応
5	定められた規程等に従って業務手順が適切に行われたことを示す監査証跡の保持(情報システム利用申請書、アクセス記録等) ※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業員に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館(室)記録、個人データのアクセスの記録(誰がどのような操作を行ったかを記録)、教育受講者一覧表等がある。	個人情報の取得から廃棄にいたる全過程において、帳票に基づく作業を行うこととし、その帳票上に、「実施」「確認」「承認」「報告」といった規定に基づく認証行為を行い、監査証跡として保存することが必要である。 (例) ・ 検査依頼書の取得：「個人情報預かり書」「個人情報受払簿」 ・ 検査報告書の持参：「個人情報受払簿」 ・ 個人情報の廃棄：「個人情報廃棄証明」 (文書・記録管理規程)
組織的安全管理措置(③取扱台帳)		
1	個人データ取扱台帳の整備（取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限等）	自社内で取り扱っている個人情報の洗い出しを行い、管理すべき個人情報を特定する。この作業を通じ特定した個人情報について、左記属性のほか、その名称・種類、業務内容、取扱部署・責任者・担当者を記入した「個人情報取扱明細書」を作成・綴じ込みを行い、「個人情報取扱台帳」として維持管理する。 (情報資産取扱規程)
2	個人データ取扱台帳の内容の定期的な確認による最新状態の維持	確認責任者、確認周期、確認方法を規定する。 (情報資産取扱規程)
組織的安全管理措置(④評価・見直し)		
1	監査計画の立案、計画的監査(外部監査、内部監査)の実施	事業年度毎に、基本計画（監査対象、重点監査テーマ、実施体制、スケジュール）と個別計画(監査対象、監査目的、監査の範囲・手続、スケジュール、責任者と業務分担)を立て、計画的に監査を行う。 (個人情報保護監査規定)
2	監査実施結果の取りまとめと代表者への報告	監査実施結果を「システム監査報告書」として取りまとめ、報告会等を開催して代表者に報告する。 (個人情報保護監査規定)

No.	項目・内容	解釈・対応
3	監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善	監査実施結果、環境の変化、情報の技術変化に対応して、定期的に安全管理措置の見直し及び改善を実施する。 (個人情報保護監査規定)
組織的安全管理措置(⑤事故・違反対処)		
1	事実関係、再発防止策等の公表	事故発生時の対応については、危機管理組織の設置、連絡体制、責任者の役割、業務内容、教育訓練等について危機管理マニュアルを作成し、それに基づいた事実関係の究明、再発防止策の決定、公表等を行う必要がある。 (個人情報保護緊急時対応規程)
2	その他、①事実調査、②影響範囲の特定、③影響を受ける可能性のある本人及び主務大臣への報告、④原因の究明、⑤再発防止策の検討・実施の実施	同上 (個人情報保護緊急時対応規程)
組織的安全管理措置 個人データの取扱いに関する規程(①取得・入力)		
1	個人データを取得する際の作業責任者の明確化（以下「取得」という） (作業責任者の明確化)	検査依頼書、顧客(医師)属性情報、人事情報、患者情報(調剤薬局)等の個人情報を取得する際、個人情報の正確な授受、記載内容の確認、取得時における法の要求事項（「利用目的の明示」、「本人の同意」、「正当な手段による取得」等）の履行確認、情報の搬送等に責任を有する者を明確にする。(営業所長、係長等が想定される) (個人情報管理規程、情報資産取扱規程)
2	取得した個人データを情報システムに入力する際の作業責任者の明確化（以下「入力」という） (作業責任者の明確化)	社内牽制のため、個人情報の取得の作業責任者と入力の作業責任者は兼務を避ける必要がある。 (個人情報管理規程、情報資産取扱規程)
3	取得・入力する際の手続の明確化 (手続の明確化と手続に従った実施)	現行の業務フローを見直し、個人情報保護の要求内容と比較し、問題となる取扱いを識別、是正した上で、手順書として明確化する。 見直しは、「正確な処理」、「完全性の確保」、「不正防止」の観点から実施し、必要により入力内容の確認、承認等の手順を組み込むことが重要である。 (個人情報管理規程、情報資産取扱規程)

No.	項目・内容	解釈・対応
4	定められた手続による取得・入力の実施 (手続の明確化と手続に従った実施)	同上 (個人情報管理規程、情報資産取扱規程)
5	権限を与えられていない者が立ち入れない建物等での入力作業の実施 (手続の明確化と手続に従った実施)	入力データや機器の盗難防止、無権限者の不正使用等を防止し、万が一事故が発生した時の原因究明を容易にするため、施錠の効く建物(部屋)等で作業を行うこととし、入退室管理（氏名、入退室時刻等）施錠管理を実施する。 (入退室管理規程)
6	個人データを入力できる端末の、業務の必要性に基づく限定 (手続の明確化と手続に従った実施)	個人情報資産に損害を与える直接的な原因である漏洩、不正アクセス、データの改竄・破壊といった行為の発生可能性を高める要因である端末の数を減少させるためや事故が発生した時の原因究明を容易にするために、極力、個人データに入力できる端末そのものを限定する。 端末のアクセス記録を定期的に確認し、不正アクセス等を監視する。 （アクセス管理規程）
7	個人データを入力できる端末に付与する機能の、業務の必要性に基づく限定（例：個人データを閲覧だけできる端末では、CD-R 、USB メモリ等の外部記録媒体を接続できないようにする） (手続の明確化と手続に従った実施)	上記と同様のリスクコントロールの考え方に基づき、限定した端末が有する機能についても、業務上必ずしも必須な機能でなければ、取除く必要がある。 （アクセス管理規程）
8	個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定 (作業担当者の識別、認証、権限付与)	個人データの取得及び入力は担当者として指名された者以外は行うことができないこと、指名の方法などを定め、作業担当者を限定し、識別可能な状態に置く。作業責任者と同様、極力、取得担当者と入力担当者の兼務を避けることが好ましい。 （アクセス管理規程）
9	ID とパスワードによる認証、生体認証等による作業担当者の識別 (作業担当者の識別、認証、権限付与)	アクセス者の本人確認をどのような方法で行うか、またその方法により操作した者を正当な作業担当者と見なす旨を規定に定める。ID とパスワード、暗号、IC カード、指紋等の方法が考えられる。 （アクセス管理規程）
10	作業担当者に付与する権限の限定 (作業担当者の識別、認証、権限付与)	取得・入力に必要な操作・作業内容を分析し、できる作業を限定し、その内容を規定する。 （アクセス管理規程）

No.	項目・内容	解釈・対応
11	個人データの取得・入力業務を行う作業担当者に付与した権限の記録 (作業担当者の識別、認証、権限付与)	作業担当者別の業務内容を権限記録簿等を作成し、管理担当者はID・パスワードの付与、貸与、抹消等の管理と併せ権限内容の見直し等も行う。 (アクセス管理規程)
12	手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認 (作業担当者及びその権限の確認)	個人情報取扱責任者等の管理者は、定期的に、取得・入力作業にかかる作業表、入力帳票、管理帳票を監査し、手続の不明確なものはないか、手続どおりに実施されているか、作業担当者の不明確な操作はないか、権限は正確に付与されているかなど、規程に定められた取扱手順が遵守されているかを確認することとし、その旨規定する。 (個人情報保護監査規定)
13	アクセスの記録、保管と、権限外作業の有無の確認 (作業担当者及びその権限の確認)	個人情報取扱責任者等の管理者は、アクセスログを採り、権限外の作業の有無を確認し、違反する取扱いがあった場合は、端末の使用停止も含め厳正に対処する旨規定する。 (アクセス管理規程)
組織的安全管理措置 個人データの取扱いに関する規程(②移送・送信)		
1	個人データを移送・送信する際の作業責任者の明確化 (作業責任者の明確化)	他の作業責任者と別の者を指名するのが適切な対応ではあるが、兼務となる場合も考えられるので、その場合は、作業の中で、再検・確認・承認等の手続を組み込むなど、牽制面で留意する必要がある。 (個人情報保護規程)
2	個人データを移送・送信する際の手続の明確化 (手続の明確化と手続に従った実施)	移送については、紙、メディア(CD、MO、FD等)等の媒体を使って、運搬、郵送、宅配、FAX、テレックス等により行うことが考えられる。この場合、申請・承認手続、持出記録、受払記録、暗号化、受領確認手段(郵便の場合は配達証明郵便)等を手順として規定する。また、送信による場合も、作業者の特定、送信理由の限定、申請・承認手続、暗号化、受領確認手段等を規程化する。なお、オープンネットワークを使用した送信は極めてリスクが高いこともあり、「原則禁止」することも考えられる。 (個人情報保護規程、情報資産取扱規程) (媒体管理規程、ネットワーク管理規程)

No.	項目・内容	解釈・対応
3	定められた手続による移送・送信の実施 (手続の明確化と手続に従った実施)	同上 (情報資産取扱規程、媒体管理規程、ネットワーク管理規程)
4	個人データを移送・送信する場合の個人データの暗号化(例えば、公衆回線を利用して個人データを送信する場合)移送時における宛先確認と受領確認(例えば、配達記録郵便等の利用) (手続の明確化と手続に従った実施)	同上 (情報資産取扱規程、媒体管理規程、ネットワーク管理規程)
5	FAX、テレックス等における宛先番号確認と受領確認 (手続の明確化と手続に従った実施)	宛先相違を避けるため、電話による事前の番号確認と事後の受領確認を徹底することや事前にテストパターンを送信し宛先確認を行う等の送信手順を明確にするとともに、FAX 番号の登録相違を避けるため、登録時に複眼登録を行うとか、定期的なメンテ手順を規定する。 (情報資産取扱規程)
6	個人データを記した文書を FAX、テレックス等に放置することの禁止 (手続の明確化と手続に従った実施)	左記内容を規定する。 (情報資産取扱規程)
7	暗号鍵やパスワードの適切な管理 (手続の明確化と手続に従った実施)	暗号鍵やパスワードの管理者を明確にするとともに、登録・変更・抹消の手続を明確にする。 (アクセス管理規程、媒体管理規程)
8	個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.8 と同趣旨により、移送・送信できる作業担当者を限定する必要がある。 (アクセス管理規程、ネットワーク管理規程)
9	ID とパスワードによる認証、生体認証等による作業担当者の識別 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.9 と同趣旨により、規定化する必要がある。 (アクセス管理規程)

No.	項目・内容	解釈・対応
10	作業担当者に付与する権限の限定(例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない) (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.10 と同趣旨により、規定する必要がある。 (アクセス管理規程)
11	個人データの移送・送信業務を行う作業担当者に付与した権限の記録 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.11 と同趣旨により、規定する必要がある。 (アクセス管理規程) (媒体管理規程)
12	手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.12 と同趣旨により、規定する必要がある。 (個人情報保護監査規程)
13	アクセスの記録、保管と、権限外作業の有無の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.13 と同趣旨により、規定する必要がある。 (アクセス管理規程、媒体管理規程)
組織的安全管理措置 個人データの取扱いに関する規程(③利用・加工)		
1	個人データを利用・加工する際の作業責任者の明確化 (作業責任者の明確化)	個人情報を利用・加工するケースは、医療機関との検査依頼内容、検査結果(報告書)、請求明細等にかかる確認・照会・照合・変更・追加・訂正等の要請に伴う問い合わせ対応、再作成、データ提供等が考えられるが、不正アクセス、紛失、改竄、破壊、漏洩リスクが極めて高い工程といえる。従って、委託元の要請であることの確認、要請内容の妥当性の確認、要請経緯の明確化と保存、利用・加工経緯の明確化と保存、情報資産・媒体の在庫管理・受払管理、利用承認ルールの導入による作業責任の明確化と保存(無権限者による処理の排除)、牽制機能の導入(要請を受ける者と、データベースにアクセスする者を分けるなど)等の手続きを規定し、文書による運用を実施する必要がある。 (個人情報保護規程)
2	個人データを利用・加工する際の手続の明確化	例えば、「個人情報利用・加工申請・承認書」(申請者、利用および加工目的・理由・内容、媒体等)、「利用・加工作業報告書」(作業担当者名、

No.	項目・内容	解釈・対応
	(手続の明確化と手続に従った実施)	作業責任者名、作業内容、データ保護措置等)、「媒体管理記録簿」(媒体管理責任者名、媒体種類、保管場所、搬送記録、受払記録、媒体廃棄経緯等)による運用を考える。 (情報資産取扱手順)
3	定められた手続による利用・加工の実施 (手続の明確化と手続に従った実施)	同上 (情報資産取扱手順)
4	権限を与えられていない者が立ち入れない建建物等での利用・加工の実施 (手続の明確化と手続に従った実施)	個人データの取扱いに関する規程(①取得・入力)No.5 と同趣旨により、規定する必要がある (入退室管理規程)
5	個人データを利用・加工できる端末の、業務の必要性に基づく限定 (手続の明確化と手続に従った実施)	個人データの取扱いに関する規程(①取得・入力)No.6 と同趣旨により、規定する必要がある。 (アクセス管理規程)
6	個人データを利用・加工できる端末に付与する機能の、業務の必要性に基づく、限定(例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする) (手続の明確化と手続に従った実施)	個人データの取扱いに関する規程(①取得・入力)No.7 と同趣旨により、規定する必要がある。 (アクセス管理規程)
7	個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.8 と同趣旨により、規定する必要がある。 (アクセス管理規程)
8	ID とパスワードによる認証、生体認証等による作業担当者の識別 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.9 と同趣旨により、規定する必要がある。 (アクセス管理規程)
9	作業担当者に付与する権限の限定(例えば、個人データの閲覧することのみが業務上必要とされる作業担当者に対し、複写、複製を行う権限は必要ない) (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.10 と同趣旨により、規定する必要がある。 (アクセス管理規程)

No.	項目・内容	解釈・対応
10	個人データの利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等の記録 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.11と同趣旨により、規定する必要がある。 (アクセス管理規程)
11	手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.12と同趣旨により、規定する必要がある。 (個人情報保護監査規程)
12	アクセスの記録、保管と権限外作業の有無の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.13と同趣旨により、規定する必要がある。 (アクセス管理規程)
組織的安全管理措置 個人データの取扱いに関する規程(④保管・バックアップ)		
1	個人データを保管・バックアップする際の作業責任者の明確化 (作業責任者の明確化)	データの正確性を確保し、不正アクセス、不正使用等を排除するため、個人情報資産目録の情報資産毎に、その重要性レベルを設定し、保管・バックアップ方法（FD・CD・MO等、PCハード、部署共通サーバ、全社サーバ等)、保管管理者、アクセス権限者、作業責任者を明確にし、規定する。 (情報システム管理規程、情報資産取扱規程)
2	個人データを保管・バックアップする際の手続の明確化 （個人データ、OS、アプリケーションのバックアップ等） (手続の明確化と手続に従った実施)	例えば、「個人データ保管管理記録簿」を設定し、保管・バックアップの申請・承認、保管・バックアップ作業の実行経緯記録、アクセスの承認・記録等を手順として規定する。 (情報システム管理規程) (各種データバックアップ手順、HP管理規程、媒体管理規程)
3	定められた手続による保管・バックアップの実施 (手続の明確化と手続に従った実施)	同上 (情報システム管理規程) (各種データバックアップ手順、HP管理規程、媒体管理規程)
4	個人データを保管・バックアップする場合の個人データの暗号化 (手続の明確化と手続に従った実施)	個人情報の保管・バックアップに当たっては暗号化することを規定するとともに、信頼できる暗号化技術の選択・使用、複数の暗号方式の組合せ使用、暗号化・復号化を行う時点の設定等について規定する。 (情報システム管理規程、情報資産取扱規程、媒体管理規程)

No.	項目・内容	解釈・対応
5	暗号鍵やパスワードの適切な管理 (手続の明確化と手続に従った実施)	管理者を明確にし、暗号鍵やパスワードの登録・変更・抹消の手続きを明確に定める。 (アクセス管理規程、媒体管理規程)
6	個人データを記録している媒体を保管する場合の施錠管理 (手続の明確化と手続に従った実施)	個人データを記録している媒体の保管は施錠できる場所とし、情報の重要度に応じ、保管庫、金庫、それらの併用等の方法による旨明記する。 (媒体管理規程)
7	個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理 (手続の明確化と手続に従った実施)	保管する部屋、保管庫等を特定し、鍵の保管責任者を明確にする。鍵の「保管管理簿」を設け、保管責任者、鍵等の変更の都度記録をとるとともに、「鍵使用記録簿」を設け保管場所の開閉管理を行うようなルールを設ける。 なお、個人のデスクへの保管は禁止する。 (情報資産取扱規程、入退室管理規程)
8	個人データのバックアップから迅速にデータが復元できることのテストの実施 (手続の明確化と手続に従った実施)	テストの実施者、テストの実施責任者、実施サイクル等を規定する。 (情報資産取扱規程)
9	個人データのバックアップに関する各種事象や障害の記録 (手続の明確化と手続に従った実施)	例えば、「バックアップ作業記録簿」を設け、作業担当者、作業責任者に報告を義務付ける。 (情報資産取扱規程)
10	個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.8 と同趣旨により、規定する必要がある。 (アクセス管理規程)
11	ID とパスワードによる認証、生体認証等による作業担当者の識別 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.9 と同趣旨により、規定する必要がある。 (アクセス管理規程)
12	作業担当者に付与する権限の限定 （例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない） (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.10 と同趣旨により、規定する必要がある。 (アクセス管理規程)

No.	項目・内容	解釈・対応
13	個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理）の記録 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.11と同趣旨により、規定する必要がある。 (アクセス管理規程)
14	手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.12と同趣旨により、規定する必要がある。 (個人情報保護監査規程)
15	アクセスの記録、保管と権限外作業の有無の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.13と同趣旨により、規定する必要がある。 (アクセス管理規程)
組織的安全管理措置 個人データの取扱いに関する規程(⑤消去・廃棄)		
1	個人データを消去する際の作業責任者の明確化 (作業責任者の明確化)	個人データの取扱いに関する規程(④保管・バックアップ)No.1において規定した保管・バックアップ方法（FD・CD・MO等、PCハード、部署共通サーバ、全社サーバ等）毎に、個人データの消去にかかる作業責任者を規定する方法が考えられる。 (情報システム管理規程、個人情報保護規程)
2	個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化 (作業責任者の明確化)	部署毎に一名程度設置する。 (情報システム管理規程、情報資産取扱規程)
3	消去・廃棄する際の手続の明確化 (手続の明確化と手続に従った実施)	保管媒体の消去・廃棄は用済み後速やかに行うことを原則とし、保存期限のあるものについては期限到来後速やかに行うことを明記する。 消去の方法については、媒体の種類毎に、紙であればシュレッダーによる裁断もしくは焼却又は溶解の方法によるとか、磁気媒体であれば物理的に破壊または記載された電子情報を確実に消去又は読み取り不能にしてからごみとして処理する方法による等を明記する。 また、PCの廃棄については、ハードディスクの破壊やデータソフトの使用によるデータの完全消去を行ってから専門業者へ委託する等の方法を明記する。さらには、廃棄記録の記載、廃棄の立会い実施、廃棄専門業者に委託する場合の廃棄証明取得、申請・承認手続き等を明記し、一連の手続きとして規定する。 (情報システム管理規程、情報資産取扱規程、媒体管理規程)

No.	項目・内容	解釈・対応
4	定められた手続による消去・廃棄の実施 (手続の明確化と手続に従った実施)	同上 (情報システム管理規程、情報資産取扱規程、媒体管理規程)
5	権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施 (手続の明確化と手続に従った実施)	個人データの取扱いに関する規程(①取得・入力)No.5 と同趣旨により、規定する必要がある。 (入退室管理規程)
6	個人データを消去できる端末の、業務の必要性に基づく限定 (手続の明確化と手続に従った実施)	部署共通または全社サーバに保管されているファイルへアクセスできる端末を制限することを規定する。 (情報システム管理規程、情報資産取扱規程、アクセス管理規程)
7	個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に一回または複数回上書きする） (手続の明確化と手続に従った実施)	左記を規定化する。 (情報システム管理規程、情報資産取扱規程、媒体管理規程)
8	個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する） (手続の明確化と手続に従った実施)	左記を規定化する。 (媒体管理規程)
9	個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.8 と同趣旨により、規定する必要がある。 (情報資産取扱規程、アクセス管理規程)
10	ID とパスワードによる認証、生体認証等による作業担当者の識別 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.9 と同趣旨により、規定する必要がある。 (アクセス管理規程)
11	作業担当者に付与する権限の限定 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.10 と同趣旨により、規定する必要がある。 (アクセス管理規程)
12	個人データの消去・廃棄を行う作業担当者に付与した権限の記録 (作業担当者の識別、認証、権限付与)	個人データの取扱いに関する規程(①取得・入力)No.11 と同趣旨により、規定する必要がある。 (アクセス管理規程)

No.	項目・内容	解釈・対応
13	手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.12と同趣旨により、規定する必要がある。 (個人情報保護監査規程)
14	アクセスの記録、保管、権限外作業の有無の確認 (作業担当者及びその権限の確認)	個人データの取扱いに関する規程(①取得・入力)No.13と同趣旨により、規定する必要がある。 (アクセス管理規程)
人的安全管理措置（①非開示契約の締結）		
1	従業者の採用時又は委託契約時における非開示契約の締結（雇用契約または委託契約時における非開示契約条項は、契約終了後も一定期間有効であるようにする）	就業規則、委託契約書等の中で秘密保持の義務、義務の内容、対象者、契約違反時の措置、義務の存続期間等を定め、について、従業者(役員、正社員、契約・嘱託・パート・アルバイト・派遣社員等)からは採用時に誓約書等を徴求する等の措置を講ずる。 （就業規則、委託契約書）
2	非開示契約に違反した場合の措置に関する規程の整備（情報システムの開発・保守関係者、清掃担当者、警備員等なども含める）	同上 （就業規則、委託契約書）
人的安全管理措置（②周知・教育・訓練）		
1	個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知	個人情報保護規程、就業規則等を備え付け、常時閲覧できる状態にするとともに、携行可能なサマリー版を作成する等により、周知徹底を図る。 （個人情報保護規程、就業規則）
2	個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施	教育目的、教育研修計画の策定（研修開催頻度、教育テーマ、研修階層、研修対象者）、教育責任者等に関する基本事項を規定し、毎年、計画的かつ継続的に教育・訓練を実施する。 (個人情報保護教育訓練規程)
3	従業者に対する教育・訓練が必要かつ適切に実施されていることの確認	教育研修記録を作成し、内部監査でチェックする。 (個人情報保護教育訓練規程、個人情報保護監査規程)

No.	項目・内容	解釈・対応
物理的安全管理措置（①入退館(室)管理）		
1	個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施	外来者、従業者の入退室管理の実施されている室内での作業を行う。特に重要度によっては入室制限を行うとか、身分証の常時着用とか、外来者には入室許可証を発行する等規定する必要がある。 （入退室管理規定）
2	個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置	上記管理の行われている室内への情報システムの設置を義務化する。 （入退室管理規定）
物理的安全管理措置(②盗難等に対する対策)		
1	離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置の禁止	左記内容を規定する。 （情報資産取扱規定）
2	離席時のパスワード付きスクリーンセイバ等の起動	ID・パスワード等の操作をせずに離席した時に権限者以外の操作を防止するために、パスワード付きスクリーンセイバ機能を起動することが有効である。スクリーンセイバ機能の使用を義務付ける。 (アクセス管理規定)
3	個人データを含む媒体の施錠保管	個人データの取扱いに関する規程(④保管・バックアップ)№6と同趣旨により、規定する必要がある。 (媒体管理規定)
4	氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管	左記内容を規定する。 (ネットワーク管理規定)
5	個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止	左記内容を規定する。 （情報資産取扱規定）
物理的安全管理措置(③機器・装置等の保護)		
1	個人データを取り扱う機器・装置等の、安全管理上の脅威（盗難、破壊、破損など）や環境上の脅威（漏水、火災、停電など）からの物理的な保護	安全管理上の脅威や環境上の脅威から保護するために、各種のハードウェアの重要度に応じて、設置場所等の基準を定める。例えば、安全管理上からは外部から容易に侵入し難い場所(出入り口の出入りが管理されている場所、防犯設備・施錠設備が整備された場所等)、環境上からは防火対策(防火設備の設置等)・地震対策(耐震構造等)・出水対策(建物上階等)の行われた場所に設置するよう定める。 (ネットワーク管理規定、アクセス管理規定)

No.	項目・内容	解釈・対応
技術的安全管理措置(①個人データへの識別・認証)		
1	個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業者本人であることの識別と認証の実施(例えば、ID とパスワードによる認証生体認証等) ※ ID とパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID を停止する等の措置を講じることが望ましい。	個人情報を管理する情報システムは、個人別の識別を、原則として実施する。また、パスワードの管理について、管理部署の明確化、設定・運用ルールの明確化、変更手続の明確化を行う必要がある。 左記内容について規定する。 (アクセス管理規程)
2	個人データへのアクセス権限を有する各従業者が使用できる端末又はアドレス等の識別と認証(例えば、MAC アドレス認証、IP アドレス認証等)の実施	アクセス権限者とその使用端末の対応関係を明確にし、アクセス制限(無権限者の不正使用を監視)に利用する必要がある。使用端末 (MAC アドレス)とアクセス権限者(IP アドレス)の対応表等による管理を行う。 (アクセス管理規程)
技術的安全管理措置(②個人データへのアクセス制御)		
1	個人データへのアクセス権限を付与すべき従業者数の最小化	申請・承認時に、各所属長やシステム管理者が必要性をチェックするとか、退職、転属等の異動時にタイムリーにアクセス権限を変更・削除する手続を明確化する必要がある。 (アクセス管理規程)
2	識別に基づいたアクセス制御(パスワード設定をしたファイルが誰でもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っているものが特定され、かつ、アクセスを許可する者に変更がある	ファイルの種類、重要度にもとづき、アクセス権限を階層的に設定し、アクセス時の申請・承認ルールを導入することが考えられる。

No.	項目・内容	解釈・対応
	たびに、適切にパスワードを変更する必要がある)	(アクセス管理規程)
3	従業者に付与するアクセス権限の最小化	上記措置等にもとづき、権限テーブル、部署別・業務別の権限の限定を行う。 (アクセス管理規程)
4	個人データを格納した情報システムへの同時利用者数の制限	DOS 攻撃、セキュリティホール攻撃、不正アクセスへの対処を想定していると考えられる (ネットワーク管理規程)
5	個人データを格納した情報システムの利用時間の制限 (例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等)	業務の特性も考慮し、休業日や業務時間外等の時間帯の使用は原則禁止する。 (アクセス管理規程)
6	個人データを格納した情報システムへの無権限アクセスからの保護 (例えば、ファイアウォール、ルータ等の設定)	ファイアウォール、ルータ等の設定、侵入検知システムの導入、ログ監視等の保護策を講ずる。 (アクセス管理規程、ネットワーク管理規程)
7	個人データにアクセス可能なアプリケーションの無権限利用の防止 (例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる従業者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等) ※ 情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。	検査システム、人事情報システムなどのアプリケーション毎に ID、パスワードでの識別・認証を行うか、または業務上必要でない端末にはアプリケーション自体をインストールしないといった対応が必要である。

No.	項目・内容	解釈・対応
	※特権ユーザーに対するアクセス制御については、トラステッド OS やセキュア OS 等の利用が考えられる。	（アクセス管理規程）
8	個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションの脆弱性有無の検証）	脆弱性検査ツール、パスワード検査ツール等によるテストの実施または外部委託による検証作業の実施を検討する。(Web の侵入テストなどの実施を想定している） （ネットワーク管理規定）
技術的安全管理措置(③個人データへのアクセス権限の管理)		
1	個人データにアクセスできる者を許可する権限管理の適切な実施（例えば、個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする）	アクセス権限の承認者、作業担当者の責任と権限を明確にし、管理者の作業をパスワードにより保護することが必要。 （アクセス管理規程）
2	個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施	アクセス権限を重要度に応じて階層化し、アクセス時には当該階層権限者の承認がないとアクセスできないようなルールを作る。 （アクセス管理規程）
技術的安全管理措置(④個人データへのアクセス記録)		
1	個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）	個人データへのアクセスログが採れる仕組みを構築し、ログ記録は永久保管とする。その上で、責任者を決めて、定期的にログ記録を確認・分析し、不正なアクセスまたはおそれのあるアクセスについて対応を行う。個人データへのアクセスログの記録が困難な場合には、システムへのアクセスログで代替することも検討する。 （アクセス管理規程）
2	採取した記録の漏洩、滅失及びき損からの適切な保護 ※ 個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。	ログの記録ファイルへのアクセス制限を行い、改竄・漏洩等から保護する。 （アクセス管理規程）

No.	項目・内容	解釈・対応
技術的安全管理措置(⑤不正ソフトウェア対策)		
1	ウイルス対策ソフトウェアの導入	コンピュータウィルス対策として、ソフトウェアの導入、更新頻度、ウィルス発見時の対応等を規定する。 （情報システム管理規程、ネットワーク管理規程）
2	OS、アプリケーション等に対するセキュリティ対策用修正ソフトウェア(いわゆるセキュリティパッチ)の適用	セキュリティホール（ソフトウェアの設計ミスなどによって生じた、システムのセキュリティ上の弱点）を放置すると、悪意のあるユーザに不正にコンピュータを操作されてしまう可能性があるため、セキュリティパッチ（セキュリティホールが発覚した時に配布される修正プログラム）を使用し修正する。セキュリティホールについての定期点検、情報収集・分析・対策等について規定する。 （情報システム管理規程、ネットワーク管理規程、HP 管理規程）
3	不正ソフトウェア対策の有効性・安定性の確認 （例えば、パターンファイルや修正ソフトウェアの更新の確認）	パターンファイル(ウィルス定義ファイル)の更新の実施、頻度等について規定する。 （情報システム管理規程、ネットワーク管理規程）
技術的安全管理措置(⑥移送・通信時の対策)		
1	移送時（運搬、郵送、宅配便等）における紛失・盗難した際の対策 （例えば、媒体に保管されている個人データの暗号化）	媒体の暗号化を行う。(顧客との合意が前提) (媒体管理規定)
2	盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを通信する際（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）の、個人データの暗号化	伝送の暗号化を行う。 (媒体管理規定)
技術的安全管理措置(⑦動作確認時の対策)		
1	情報システムの動作確認時のテストデータとして個人データを利用することの禁止	個人データをテストデータとして使用することを禁止し、やむを得ず使用する場合の条件と承認ルールを規定する。 (情報システム管理規定)

No.	項目・内容	解釈・対応
2	情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証	システム変更時のセキュリティへの影響の検証を行うこと、およびその方法、実施責任者等について規定する。 (情報システム管理規定)
技術的安全管理措置(⑧情報システムの監視)		
1	個人データを取り扱う情報システムの使用状況の監視	情報システムの使用状況の監視項目として、セキュリティ違反、大量データのダウンロードなどの項目を設ける。 (情報システム管理規定、アクセス管理規定、媒体管理規定)
2	個人データへのアクセス状況(操作内容も含む)の監視 ※ 個人データを取り扱う情報システムを監視する内容が個人情報に該当する場合があることに留意する。	ログ監視ツールを導入する。 (アクセス管理規定)

(注) 本表は、経済産業省の「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン」(平成16年6月)の安全管理措置について、「JISQ15001」、「プライバシーマーク制度における監査ガイドライン(第一般)」、プライバシーマーク取得企業のヒアリング等を参考に、解釈と対応についてまとめたものです。

別表５　　個人情報保護に関する覚書

(以下、甲という)と　　(以下、乙という)は、甲が乙に臨床検査を委託するに当たり、検査を受ける者(以下、被検者という)の個人情報の保護について、以下のとおり覚書（以下、本覚書という）を締結する。

第１条（定義）

本覚書で「個人情報」とは、甲が乙に臨床検査を委託するに当たって乙に提供する情報及び乙が当該臨床検査を行うことによって取得する情報のうち、生存する被検者及び死亡した被検者の個人に関する情報（被検者の氏名、生年月日、検体、検査結果、結果に対する評価、検査所見など）であって、当該情報に含まれる氏名、生年月日などによって特定の個人を識別することができるもの（他の情報と容易に照合して特定の個人を識別することができることとなるものを含む）を言う。

第２条（法令の遵守）

乙は、被検者の個人情報の取扱いに際しては、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下、法という）その他個人情報の保護に関する法令を遵守するとともに、関係省庁等の作成した個人情報保護に関するガイドラインに従うものとする。

第３条（利用目的の特定）

乙は、臨床検査を受託するに当たって甲から提供された被検者の個人情報は、甲から受託した臨床検査の目的でのみ利用することとし、この利用目的の達成に必要な範囲を超えて個人情報を取り扱わない。但し、法１６条３項各号に掲げる場合その他法令に基づく場合は、この限りではない。

第４条（安全管理措置）

乙は、次条以下に定めるところに従い、個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のために、必要かつ適切な措置を講ずる。

第５条（従業者の監督）

乙は、その従業者に個人情報を取り扱わせるに当たっては、個人情報の安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行う。

第６条（委託先の監督）

乙は、甲から受託した臨床検査を他の検査機関等(研究機関、病理診断医等を含む。以下、

同様とする)に委託するときは、当該検査にかかる個人情報の安全管理が図られるよう、当該検査機関等に対し、必要かつ適切な監督を行う。

第７条（不要となった個人情報の廃棄）

乙は、不要となった個人情報を廃棄する場合には、裁断するなどして個人情報を復元できない形にして廃棄する。

第８条（安全管理措置の監督）

１．甲は、必要があると認めたときは、乙に対し、個人情報の安全管理状況について、書面による報告を求めることができる。

２．甲は、必要があると認めたときは、乙による個人情報の安全管理状況を確認することができる。

第９条（連絡及び善後措置）

乙は、個人情報の漏えい等の事故が乙ないし乙の委託先において発生した場合又は発生の可能性が高いと判断した場合、並びに、個人情報の取扱いについて本覚書に違反している場合又はその兆候が高いと判断した場合は、直ちに甲にその旨を連絡し善後措置を講ずる。

第１０条（個人情報の第三者提供）

乙は、法２３条１項各号に掲げる場合その他法令に定める場合を除くほか、個人情報を第三者に提供してはならない。

第１１条(相手方への連絡など)

１．甲及び乙は、被検者より、法の規定により個人情報の開示、訂正、追加、削除又は利用停止を求められた場合には、被検者の同意を得たうえで、相手方に対して速やかにその旨を通知する。

２．被検者が乙に対して前項の請求を行った場合には、乙の保有する個人情報が甲からの臨床検査の委託に当たって提供されたものであることに鑑み、被検者からの請求に対しては甲において対処するよう努めるものとし、乙は、これに必要な協力を行う。

第１２条（存続期間）

本覚書の存続期間は、甲・乙間の臨床検査の委託契約の存続期間と同一とする。

第１３条（別途協議）

本覚書に定めのない事項及び本覚書の内容について疑義が生じた場合は、甲・乙互いに

誠意をもって協議して決定するものとする。

本覚書の成立を証するため、本書 2 通を作成し、各々記名押印の上、各々その１通を保有するものとする。

平成　　年　　月　　日

甲

乙

別表６

個人情報保護に関する覚書

委託者　　(以下、甲という)と受託者　　(以下、乙という)は、甲が乙に臨床検査を委託するに当たり、検査を受ける者(以下、被検者という)の個人情報の保護について、以下のとおり覚書（以下、本覚書という）を締結する。

第１条（定義）

本覚書で「個人情報」とは、甲が乙に臨床検査を委託するに当たって乙に提供する情報及び乙が当該臨床検査を行うことによって取得する情報のうち、生存する被検者及び死亡した被検者の個人に関する情報（被検者の氏名、生年月日、検体、検査結果、結果に対する評価、検査所見など）であって、当該情報に含まれる氏名、生年月日などによって特定の個人を識別することができるもの（他の情報と容易に照合して特定の個人を識別することができることとなるものを含む）を言う。

第２条（法令の遵守）

乙は、被検者の個人情報の取扱いに際しては、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下、法という）その他個人情報の保護に関する法令を遵守するとともに、関係省庁等の作成した個人情報保護に関するガイドラインに従うものとする。

第３条（利用目的の特定）

乙は、臨床検査を受託するに当たって甲から提供された被検者の個人情報は、甲から受託した臨床検査の目的でのみ利用することとし、この利用目的の達成に必要な範囲を超えて個人情報を取り扱わない。但し、法１６条３項各号に掲げる場合その他法令に基づく場合は、この限りではない。

第４条（安全管理措置）

乙は、次条以下に定めるところに従い、個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のために、必要かつ適切な措置を講ずる。

第５条（規程の整備など）

１．乙は、本覚書に定められた義務を履行するため、個人情報保護のために必要な諸規程を整備する。

２．乙は、個人情報に関する管理責任者及び甲に対する報告の責任者を定め、その者の氏名、部署名及び、連絡先などを、本覚書締結後、速やかに甲に対して書面で連絡するものとし、変更があった場合も同様とする。

第６条（従業者の監督）

乙は、その従業者に個人情報を取り扱わせるに当たっては、個人情報の安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行う。

第７条（管理体制）

乙は、第三者ないし臨床検査に関与しない乙の従業者が入手できないよう、個人情報の記録された媒体（紙、電磁的記録など媒体の種類を問わない）の漏えい対策（執務室への入退室管理、媒体の施錠保管、データファイルへのパスワード設定や暗号化等を含む）を講じる。

第８条（複製等の禁止）

１．乙は、甲の事前の承諾がある場合を除き、個人情報に加工（それが委託の内容である場合を除く）、改ざんを加えてはならない。

２．乙は、甲の事前の承諾がある場合、及び、管理上必要なバックアップを作成する場合を除き、個人情報について複製（コピー機による複写、電磁的記録の複製等方法は問わない）をしてはならない。

第９条（再委託の原則的禁止及び実施時の条件）

１．乙は、甲から受託した臨床検査を再委託してはならない。但し、甲の書面による承諾がある場合はこの限りでない。

２．乙は、臨床検査を再委託する場合には、当該委託先との間で本覚書に定める内容を含む個人情報の保護に関する契約を締結し、当該委託先に対し、個人情報の保護が徹底されるよう管理監督する。

３．乙は、再委託先に個人情報を預託する場合には、預託する個人情報の内容、方法、相手の氏名及び連絡先を、速やかに甲に書面にて報告しなければならない。

４．乙の委託先において個人情報の漏洩等の事故が発生したときは、これによって甲が被った損害を乙は賠償しなければならない。

第１０条（検証）

乙は、本覚書に定める事項が自己の組織内において継続的に遵守されるよう、個人情報の保護対策について適宜検証ないし是正を行う。

第１１条（管理、及び保管状況についての報告及び検査）

１．甲は、必要があると認めたときは、乙に対し、個人情報の管理及び保管状況について、書面による報告を求めることができる。

２．甲は、必要があると認めたときは、乙による個人情報の管理及び保管状況を随時検

査することができる。この場合、乙は検査に協力しなければならない。

第１２条（連絡及び善後措置）

乙は、個人情報の漏えい等の事故が乙ないし乙の委託先において発生した場合又は発生の可能性が高いと判断した場合、並びに、個人情報の取扱いについて乙が本覚書に違反している場合又はその兆候が高いと判断した場合は、直ちに甲に対してその旨及びその内容を連絡し、善後措置を講ずる。

第１３条（個人情報の第三者提供）

乙は、法２３条１号各項に掲げる場合その他法令に定める場合を除くほか、個人情報を第三者に提供してはならない。但し、乙が臨床検査を他の検査会社に委託する場合は、この限りではない。

第１４条（相手方への連絡など）

1. 甲及び乙は、被検者より、法の規定により個人情報の開示、訂正、追加、削除又は利用停止を求められた場合には、被検者の同意を得たうえで、相手方に対して速やかにその旨を通知する。
2. 被検者が乙に対して前項の請求を行った場合には、乙の保有する個人情報が甲からの臨床検査の委託に当たって提供されたものであることに鑑み、被検者からの請求に対しては甲において対処するよう努めるものとし、乙は、これに必要な協力を行う。

第１５条（個人情報の返還ないし廃棄）

乙が、臨床検査の結果、検査に対する評価、検査所見などを甲に報告するなどして委託の目的を終了した場合の個人情報の返還ないし廃棄に関しては、別途甲、乙間で協議して定めるものとし、乙は、責任をもって個人情報を返還ないし廃棄する。

第１６条（保証）

乙は甲に対し、本覚書締結までの３年間に、乙において情報の漏えい事故が発生していないことを保証する。

第１７条（損害賠償）

乙は、この覚書記載の事項に違反したことによって甲に生じた損害を賠償しなければならない。

第１８条（存続期間）

本覚書の存続期間は、甲・乙間の臨床検査の委託契約の存続期間と同一とする。

第１９条（残存義務）

１．第８条、第１２条、第１３条、第１５条、及び第１７条に基づく義務は、本覚書が効力を失った後も残存するものとする。

２．乙は、甲から受託した臨床検査に関与した従業者に対し、乙との雇用契約、委任契約などの契約関係の終了後においても、秘密保持義務を負わせるものとし、これに必要な措置を講ずるものとする。

第２０条(別途協議)

本覚書に定めのない事項及び本覚書の内容について疑義が生じた場合は、甲・乙互いに誠意をもって協議して決定するものとする。

第２１条（管轄）

本覚書に関して紛争が生じた場合は、○○地方裁判所を、当該紛争に関する第一審の専属管轄裁判所とする。

本覚書の成立を証するため、本書 2 通を作成し、各々記名押印の上、各々その１通を保有するものとする。

平成　　年　　月　　日

甲

乙