

臨床検査業界における個人情報保護の取り組みについて

当業界は、個人情報保護法(以下「法」という。)と「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(厚生労働省平成 16 年 10 月) 」(以下「指針」という。)を基本とし、その他「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(経済産業省平成 16 年 6 月)」、JISQ15001 の要求基準等を参考に個人情報保護体制を構築する必要がある。

個人情報保護対策は、いろいろな法律やガイドラインがでているために、なにを根拠とするべきか解りにくいのが実情と思われるため、ここでは厚生労働省の指針に記載されている医療業界における個人情報の特殊性を考慮しつつ、法の求める義務事項を確認し、JISQ15001 要求事項や一般産業界での取り組み事例等を参考に具体的な方策を示した。

1. 指針における臨床検査会社の位置づけ

厚生労働省の指針の中でもっとも最初に確認しておかなければならない重要な点は、検体検査の事業者は「医療機関の委託をうけて業務を遂行する事業者」と位置づけられ、「適切な安全管理措置を講ずること」が求められたことである。

このため検体検査に限っていえば、法の上では、後述の「個人情報」「個人データ」に関する義務事項を課せられる(「保有個人データ」に関する義務事項は課せられない)ことになり、委託元である医療機関による監督のもと保護対応を進めることとなることを押えておく必要がある。

また、薬局、介護事業、高齢者福祉サービス等の事業を行なっている場合、これらの事業は、法及び指針の全ての義務事項の対象となることに注意する必要がある。

(参考) 厚生労働省指針における対象となる範囲

「本指針が対象とする事業者の範囲は、 病院、診療所、助産所、薬局、訪問看護ステーション等の患者に対し直接医療を提供する事業者、 介護保険法に規定する居宅サービス事業、居宅介護支援事業及び介護保健施設を営む事業、老人福祉法に規定する老人居宅生活支援事業及び老人福祉施設を営む事業その他高齢者福祉サービス事業を行う者である。

なお、**検体検査**、患者等や介護サービス利用者への食事の提供、施設の清掃、医療事務の業務など、**医療・介護関係事業者から委託を受けた業務を遂行する事業者**においては、本指針の 4(安全管理措置、従業員の監督及び委託先の監督(法第 20 条～第 22 条))に沿って適切な安全管理措置を講ずることが求められるとともに、当該委託を行う医療・介護関係事業者は、業務の委託にあたり、本指針の趣旨を理解し、本指針に沿った対応を行う事業者を委託先として選定するとともに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を行い、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。」

2. 個人情報保護法において保護対象となる情報

(1) 情報の定義

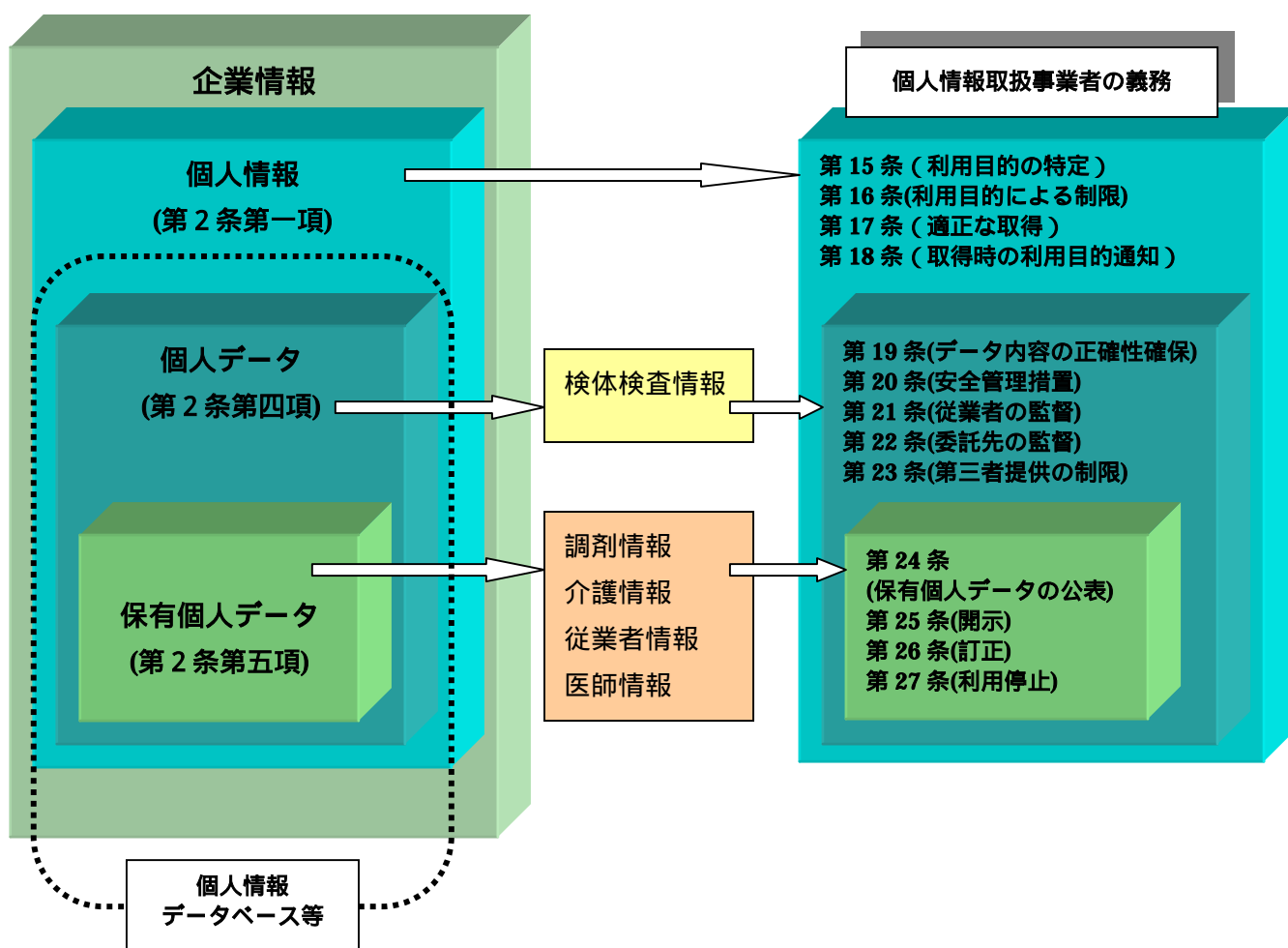
情報種別	内容	備考
個人情報	<p>生存する「個人に関する情報」であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）をいう。</p> <p>「個人に関する情報」</p> <ul style="list-style-type: none"> ・ 氏名、性別、生年月日等個人を識別する情報 ・ 個人の身体、財産、職種、肩書き等の属性に関して、事実、判断、評価を表す全ての情報 	<p>個人情報の例(作成・保存が義務付けられている記録)</p> <p>衛生検査所</p> <ul style="list-style-type: none"> ・ 委託検査管理台帳 ・ 検査結果報告台帳 ・ 苦情処理台帳 <p>薬局</p> <ul style="list-style-type: none"> ・ 処方箋 ・ 調剤録 <p>指定福祉用具貸与事業者</p> <ul style="list-style-type: none"> ・ ケアプラン ・ サービス提供記録 ・ 苦情の内容等の記録
個人データ	<p>「個人情報データベース等」を構成する個人情報をいう。</p> <p>「個人情報データベース等」</p> <ul style="list-style-type: none"> ・ 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物 ・ コンピュータを用いていない場合であっても、カルテや指導要録等、紙面で処理した個人情報を一定の規則（例えば、五十音順、年月日順等）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置いているもの。 	
保有個人データ	<p>個人データのうち、その企業（個人情報取扱事業者）がデータの開示、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権限を持ち（その企業が収集した情報であり、委託などで預かっている情報ではないということ）なおかつ保有する期間が6カ月以上のものをいう。</p>	<p>検査目的で患者から採取した検体は個人情報に該当し、医療機関においては、利用目的の特定、通知等の対象となり、患者の同意を得ずに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扱うことはできない。また、検査結果は個人データに該当し、第三者提供、開示の対象となる。</p>

(2) 情報間の関係

「企業が保有するすべての情報」 「個人情報」 「個人データ」 「保有個人データ」

(3) 情報と企業が法的に負う義務の関係

「個人情報」「個人データ」「保有個人データ」のいずれであるかによって、企業(個人情報取扱事業者)が法的に負う義務は異なっている。具体的には、データの公表、開示、訂正、利用停止などの義務を負うのは、保有個人データについてだけである。また、データの安全管理(安全管理措置)が法的に義務付けられているのは個人データ(保有個人データを含む)であり、個人情報には義務付けられていない。



図表のとおり、「個人情報」、「個人データ」、「保有個人データ」の順に、課せられる義務は重くなっている。このため『必要のない個人情報は持たない、個人情報を持つ場合も必要のないデータベース化はしない、不要になった個人情報は速やかに廃棄する』という姿勢が求められる。

3. 個人情報取扱事業者の義務の内容

(1) 「個人情報」に関して課せられる義務事項（第15条～第18条）

事項	個人情報保護法の内容	備考(解釈・事例等)
利用目的の特定 (第15条)	<p>個人情報を取り扱うに当たっては、その「利用目的」を可能な限り具体的に、そして最終的にどのような目的で個人情報を利用するかを特定しなければならない。</p> <p>検体検査事業者の利用目的は、医療機関が患者に対して公表する利用目的、すなわち「検体検査業務の委託」にしたがう。</p> <p>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（本人が想定することが困難でない範囲内）を超えて行ってはならない。</p> <p>変更された利用目的は、本人に通知するか、又は公表しなければならない。</p>	<p><u>通知方法</u></p> <p>面談：口頭またはちらし等の文書を渡す 電話：口頭または自動応答装置等で知らせる 隔地者間：電子メール、FAX等による送信、または文書の郵便等による送付</p> <p><u>公表方法</u></p> <p>自社ホームページへの掲載、自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備え置き・配布等</p>
利用目的による制限 (第16条)	<p>あらかじめ<u>本人の同意</u>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。(利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得る必要がある。)</p> <p>合併、分社化、営業譲渡等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<u>本人の同意</u>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。(承継前の利用目的の達成に必要な範囲内で取り扱う場合は目的外利用にはならず、本人の同意を得る必要はない。)</p>	<p><u>本人の同意を得る方法</u></p> <p>同意する旨を本人から口頭又は書面（電子的方式等で作られる記録を含む。）で確認する</p> <p>本人が署名又は記名押印した同意する旨の申込書等文書を受領し確認する</p> <p>本人からの同意する旨のメールを受信する</p> <p>本人による同意する旨の確認欄へのチェック</p>

事項	個人情報保護法の内容	備考(解釈・事例等)
適正な取得 (第 17 条)	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。	
取得に際しての利用目的の通知等 (第 18 条)	<p>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。(個人情報を取得する場合は、あらかじめその利用目的を公表していることが望ましい。)</p> <p>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、磁気的方式等で作られる記録を含む。)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。(口頭による個人情報の取得にまでは当該義務は及ばない。)</p> <p>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。</p> <p>薬局、介護事業を営む場合は、患者・利用者等に利用目的をわかりやすく示すため、自明の利用目的でも公表する、事業所内掲示についての注意を喚起する、希望者には説明書を交付する等特段の配慮が求められる。</p>	<p>本人に通知又は公表が必要な事例(あらかじめ公表していない場合)</p> <p>インターネット上で本人が自発的に公表している個人情報を取得する場合</p> <p>インターネット、官報、職員録等から個人情報を取得する場合</p> <p>電話による問合せやクレームのように本人により自発的に提供される個人情報を取得する場合</p> <p><u>契約書、その他書面記載の個人情報を取得する場合で、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場合(保険証、問診票)</u></p> <p>申込書・契約書に記載された個人情報を本人から直接取得する場合</p> <p>アンケートに記載された個人情報を直接本人から取得する場合</p>

(2) 「個人データ」に関して課せられる義務事項(第 19 条～第 23 条)

事項	個人情報保護法の内容	備考(解釈・事例等)
データ内容の正確性の確保 (第 19 条)	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	

事項	個人情報保護法の内容	備考(解釈・事例等)
<p>安全管理措置 (第 20 条)</p>	<p>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。</p>	<p><u>組織的、人的、物理的、及び技術的安全管理措置</u> 別冊「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」を参照</p>
<p>従業員の監督 (第 21 条)</p>	<p>従業員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(第 20 条に基づく安全管理措置を遵守させるよう)、当該従業員に対する必要かつ適切な監督を行わなければならない。</p> <p>(注) 従業員」とは、個人情報取扱事業者の組織内において直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員(正社員、契約社員、嘱託社員、パート社員、アルバイト社員等)のみならず、取締役、執行役、理事、監査役、監事、派遣社員も含まれる。</p>	<p><u>従業員のモニタリング(ビデオおよびオンラインによる)を実施する上での留意点</u></p> <p>雇用管理に関する個人情報の取扱いに関する下記重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じ協議を行い、また、その重要事項を定めたときは、労働者等に周知することが望ましい。</p> <p>(重要事項)</p> <p>モニタリングの目的、即ち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業員に明示すること</p> <p>モニタリングの実施に関する責任者とその権限を定めること</p> <p>モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底する</p>

事項	個人情報保護法の内容	備考(解釈・事例等)
		<p>こと</p> <p>モニタリングの実施状況については、適正に行われているか監査、又は確認を行うこと</p>
<p>委託先の監督 (第 22 条)</p>	<p>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。</p> <p>(注)「必要かつ適切な監督」には、<u>委託契約</u>において委託者である個人情報取扱事業者が定める<u>安全管理措置の内容を契約に盛り込む</u>とともに、当該契約の内容が遵守されていることを、予め定めた間隔で定期的に確認することも含まれる。</p> <p>【個人データの取扱いを委託する場合に契約書への記載が望まれる事項】</p> <ul style="list-style-type: none"> ・委託者及び受託者の責任の明確化 ・個人データの安全管理に関する事項 ・個人データの漏えい防止、盗用禁止に関する事項 ・委託契約範囲外の加工、利用の禁止 ・委託契約範囲外の複写、複製の禁止 ・委託処理期間 ・委託処理終了後の個人データの返還・消去・廃棄に関する事項 ・再委託に関する事項 ・再委託を行うにあたっての委託者への文書による報告 ・個人データの取扱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の確認 	<p>厚生労働省のガイドラインにおいて検体検査は、医療機関を委託元とすることが明記され、臨床検査会社は受託者として、医療機関と同等の安全管理措置義務(第 20 条)を負うこととなった。</p> <p>再委託を行う場合、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者(医療機関)がその責めを負うことがあり得るので、再委託する場合は注意を要する。</p>

事項	個人情報保護法の内容	備考(解釈・事例等)
	<ul style="list-style-type: none"> ・ 契約内容が遵守されなかった場合の措置 ・ セキュリティ事件・事故が発生した場合の報告と連絡に関する事項 	
<p>第三者提供の制限 (第23条)</p>	<p>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。</p> <p>法令に基づく場合</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>第三者への提供を利用目的とすること 第三者に提供される個人データの項目 第三者への提供の手段又は方法 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</p> <p>なお、 の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、または</p>	

事項	個人情報保護法の内容	備考(解釈・事例等)
	<p>本人が容易に知り得る状態に置かなければならない</p> <p>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。</p> <p>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</p> <p>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</p> <p>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(なお、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)</p>	<p>第三者提供に当たらないケース</p> <p><u>委託先への提供</u></p> <p>この場合は特に本人の同意や通知は必要ないと考えられるが、「委託先の監督義務(第22条)」が定められており、委託先の過失等により個人情報が漏えいした場合の責任は、委託元の管理責任が問われることに注意が必要。</p> <p><u>グループによる共同利用</u></p> <p>資本関係のある企業グループが個人情報を相互に提供する場合が考えられる。個人情報取得時に利用目的を通知する際、その利用目的の中にグループ間で利用すること、グループの範囲等も含めておくことが望ましい。</p>

(3) 「保有個人データ」に関して課せられる義務事項(第24条～第27条)

事項	個人情報保護法の内容	備考(解釈・事例等)
<p>保有個人データに関する事項の公表等(第24条)</p>	<p>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。</p> <p>当該個人情報取扱事業者の氏名又は名称</p> <p>すべての保有個人データの利用目的(利用目的を本人に通知し、又は公表することにより、</p>	<ul style="list-style-type: none"> 検体検査データは保有個人データに該当しない。したがって、以下の保有個人データに関するの義務規定(第24条～第27条)については適用を受けない。

事項	個人情報保護法の内容	備考(解釈・事例等)
	<p>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、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等を除く)</p> <p>保有個人データの利用目的の通知及び開示に係る手数料の額(定めた場合に限る)並びに保有個人データの利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止又は消去、第三者への提供の停止の求めの手續</p> <p>保有個人データの取扱いに関する苦情及び問い合わせの申出先</p> <p>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。</p> <p>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</p> <p>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</p> <p>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。</p>	<ul style="list-style-type: none"> 調剤薬局、介護関係事業等の情報主体(本人)から情報を取得する事業者は第24条～第27条の義務を負う。
開示 (第25条)	<p>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。)を求められたときは、本人に対し、書面の交付による方法(求めを行った者が同意している場合には電子メール、電話等様々な方法が可能である。書面の交付による方法は同意がなくても可能との意味である。)により、遅滞なく、当該保有個人デ</p>	

事項	個人情報保護法の内容	備考(解釈・事例等)
	<p>ータを開示しなければならない。</p> <p>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。</p> <p>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（医療機関等において、病名等を開示することにより、本人の心身状況を悪化させるおそれがある場合）</p> <p>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</p> <p>他の法令に違反することとなる場合</p> <p>前項の規定に基づき求められた保有個人データの全部また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。</p>	<p>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、事実上問い合わ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おそれがある場合</p>
<p>訂正等 (第 26 条)</p>	<p>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「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。</p> <p>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。</p>	<p><u>訂正を行う必要がない事例</u></p> <ul style="list-style-type: none"> ・ 利用目的から見て訂正等が必要ではない場合や誤りである旨の指摘が正しくない場合 ・ 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

事項	個人情報保護法の内容	備考(解釈・事例等)
<p>利用停止等 (第 27 条)</p>	<p>本人から、同意のない目的外利用、不正な取得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「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。</p> <p>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。</p> <p>本人から、同意のない第三者提供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。</p> <p>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。</p> <p>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。</p>	

4. 個人情報保護対応の進め方

個人情報保護対応を進めるにあたって重要なことは、個人情報資産の所在、取扱・保管・管理状況等についての現状把握・分析(リスク評価)を行い、個人情報保護法の要求事項とのギャップを分析することによって自社の課題を明確にすることです。そして、抽出した課題にもとづいて個人情報保護に関する基本方針を策定し、管理体制の整備、規定・手順等の策定、教育・訓練の実施と進めていくことになります。

(1) 個人情報保護対策推進体制の構築

個人情報保護対策を進めていくには、まず、社長をトップとする推進部署の設置が必要となります。

組織形態はプロジェクト方式、委員会方式等が考えられます。

(2) 現状調査・分析

前記(1)で決定した推進部署が中心となって、まず、自社の個人情報を全て洗い出し、その取扱い状況、保管状況等現状の管理体制を調査し、想定される脅威(持ち出し、不正コピー、紛失、盗難、システムダウン、不正アクセス、通信回線上の盗聴、内部者による不正コピー・盗難・紛失・操作ミス・データ消去等)の発生可能性を評価することによって、対策の方向性を明らかにする必要があります。

個人情報調査

項目	内容
情報の種類	被験者情報、社員・従業者情報、顧客情報
業務名	検査、営業、人事
情報資産名	検査データ、従業者名簿、苦情処理台帳、
入手方法	顧客からFDにより入手、システムから帳票出力
入手元	顧客、本人、名簿業者
情報形態(媒体)	書類、出力帳票、FD、MO、CD-R
利用目的	検査、顧客管理、従業者管理
保管方法・場所	CP、キャビネット、机の引出し
施錠の有無	有、無
保管期間	ヶ月、年、ルールなし
持出先、持出方法	社内、外部委託先、第三者
廃棄方法	業者委託、シュレッダー、一般ごみ、データ消去ソフト
情報件数	概算

設備・室のリスク調査

項目		内容
施設全体	出入口	不審者の識別が可能な受付の設置、防犯カメラの設置等
	郵便物	盗難防止構造
	入退室	施錠、入退室管理状況
事務室	受付	不審者の識別が可能な受付の設置
	郵便物	無人受渡しの有無、入室制御
	来訪者管理	入退室管理、入門証・パッチの発行等、入室制限区域設定
	受付の視覚	受付から PC 画面を遮断、受付近辺に出力装置未設置等
	動線管理	来訪者動線上に PC、出力装置未設置等
	フロア管理	机上への書類・FD 等の放置、スクリーンセーバ利用等
	商談区域	商談区域から PC 画面を遮断・出力装置未設置等
	施錠保管	個人情報書類・FD 等の施錠保管、媒体の持ち出し記録等
会議室	廃棄	廃棄時のデータ消去、シュレッダー利用、廃棄業者管理等
	情報管理	書類の放置、ホワイトボード・黒板の消し忘れ、ごみ箱等
通路等	その他	不要なアクセスポートの設置等
		書類の放置、不要なアクセスポートの設置、出力装置未設置

リスク評価

項目	内容
情報資産名	「個人情報調査表」にリストアップした情報を記載
情報属性	PC データ、HDD データ、書類、紙等
重要度・機密度	機密性の観点から重要度を評価(公開・社外秘・秘密・極秘等)
プロセス	脅威が入手、保管、配布、提供、廃棄のどの工程に関連するか
想定される脅威	持ち出し、不正コピー、紛失、盗難、システムダウン、不正アクセス、通信回線上の盗聴、内部者による不正コピー・盗難・紛失・操作ミス・データ消去等
脅威への既存対策	物理的対策(入退室管理、施錠保管、機器・装置の物理的保護等)、技術的対策(アクセス制御、暗号化、不正ソフト対策等)、人的対策(誓約書提出、教育・訓練の実施等)の内容
既存対策の有効性	有効性を脆弱性により評価(十分、不十分、未対応等)
リスク判定	機密度と脆弱性によりリスクをランク付けする
追加的管理策	リスク判定にもとづき追加的な管理策を検討する

(3) 個人情報保護基本方針の策定

個人情報保護基本方針は、日衛協の基本方針を参考にして、個人情報取扱事業者に公開が求められている個人情報保護に関する考え方を自社の方針として明確にします。

特に、検体検査事業だけではなく、調剤薬局、介護事業等を行っている場合は個人情報保護法の要求する義務事項のレベルが違うため、レベルに合わせた方針策定が必要となります。

(4) 個人情報保護管理体制の整備

個人情報保護体制およびその責任と権限を明確にする必要があります。

個人情報保護に必要な組織体制としては、個人情報保護を推進する全社組織体制、個人情報保護部門の組織体制、管理責任者および担当者、苦情・相談窓口、監査部門等があり、おおよそ別紙のような体制が考えられます。

(5) 個人情報保護規定・手順書の策定

個人情報保護のための規程類は次のような体系で整備する必要があります。

個人情報保護方針

全社的な基本方針で、全従業員へ周知させるとともに外部へも公開する。個人情報保護方針に盛り込む事項は以下のとおりとなります。(日衛協方針ご参照)

- ・ 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること
- ・ 個人情報への不正アクセス、個人情報の紛失、破壊、改竄および漏洩などの予防並びに是正に関すること
- ・ 個人情報に関する法令及びその他の規範を遵守すること
- ・ 個人情報管理体制の継続的改善に関すること

個人情報保護規程

個人情報保護の関係文書の全体像をイメージできる中核文書となります。

- ・ 前段は、目的、適用範囲、用語の定義などを記載する
- ・ 次に基本方針、経営陣の責任、社内体制、各職務の役割と責任を記載する
- ・ 中核部分は個人情報保護法第4章の条文に沿って、直接管理策を記載するか、他の文書を参照する
(必要に応じ、個人情報保護規程の具体的な運用を定める下位文書として個人情報保護要領を設ける)

マネジメント系規程類

マネジメントシステムに関連のある規程類を作成します。

- ・ 文書・記録管理規程、内部監査規程、教育訓練規程

リスク評価に基づく詳細管理策に対応する規程・手順書類

リスク評価の結果実施した管理策について、新規に作成するかまたは既存規程を改定します。

- ・ 情報資産取扱規程、入退室管理規程、アクセス管理規程、媒体管理規程、ネットワーク管理規程、HP 管理規程、情報システム規程
- ・ 苦情相談処理規程、開示・訂正等処理規程
- ・ 外部委託管理規程、緊急時対応規程、

(6) 教育・訓練の実施

教育・訓練は、個人情報保護の安全管理措置の中でも極めて重要な意味を有しており、全ての従業員が受講できるよう、研修頻度、方法等を定めた研修プログラムと年間計画にもとづき実施し、研修記録をのこしておく必要があります。研修効果をあげるためには、研修対象者別に「採用時研修」「定期研修」「階層別研修」「全員研修」等の研修プログラムを準備するとか、少人数による研修を行うなどの工夫も必要と思われます。

個人情報保護組織体制図(参考例)

