④技術的安全管理措置

技術的安全管理措置としては、以下のようなことが考えられます。

ア．物理的なセキュリティ対策

事業所への不法侵入によるパソコン本体の盗難や、外出の際、車上荒らしによるノートパソコンの盗難を防ぐことを目的とします。

a）セキュリティワイヤーによる対策

セキュリティワイヤーとは、鋼線でできたワイヤーで、机や柱など固定できるものにパソコンをつなぎ、盗難を防止します。キーの使用や、ダイヤルで番号をあわせないとはずせない仕組みになっていて、ワイヤーも簡単には切断できない強度なので、大切なパソコンを盗難から守るのに適しています。

＜セキュリティワイヤー＞

b）USBフラッシュメモリによるデータの携帯

個人情報が格納されたノートパソコンは、極力携帯することは避け、必要なデータだけを、USBフラッシュメモリなどの記憶媒体に格納し、持ち運びます。また、万一に備えて、パスワードによるロック機能や、データ自体を暗号化するUSBフラッシュメモリを使うのがよいでしょう。

＜USBフラッシュメモリ＞

c）パソコンのレイアウト（設置場所）

経営や会計に関するデータを保存しているパソコンは、不特定多数が出入りする場所で使用することを避けたほうがよいでしょう。また、個人情報を保存しているパソコンも同様で、どうしても共用施設内で使用する場合は、パーテーションなどで外部から遮っておくなどの対策も必要となります。

イ．最低限行っておくべきセキュリティ対策

パソコンを利用する場合に、ログインIDの設定や離席時の対策、ウィンドウズアップデートなど、最低限行っておくべき対策があります。

a）OSのバージョンアップ

OSとは、オペレーティングシステム（OperatingSystem）の略で、パソコンを動かすための基礎となるシステムです。WindowsXPなどが有名ですが、このOSにもいくつかのバージョンがあり、古いOSの場合は、ログインIDの管理ができない場合や、業務で使用するには、不都合な場合があります。できるだけ、最新のものを使用した方がよいでしょう。

【業務として不都合なOS】	【業務として使用すべきOS】
Windows 95	Windows 2000
Windows 98	Windows XP Professional Edition
Windows Me	Windows XP Home Edition

b）ロングインIDとパスワード

パソコンを起動させる場合に、ログインIDやパスワード入力することにより、その本人だけが使用できるように設定することが大切です。この確認作業のことを、認証といいますが、パソコン購入時の設定のままでは、このログイン管理をしなくても使える設定となっている場合がありますので、注意が必要です。また、パスワードは、絶対第三者に知られないようにすると同時に、定期的に変更することも必要となります。

c）ウィンドウズアップデート

OSの機能も日々バージョンアップされています。OSを開発したときには、気付かなかった不具合や、新しい機能の追加などに対応する必要があります。OS自体を最新のものすることを、ウィンドウズアップデートといいます。自動的にウィンドウズアップデートをおこなう機能もありますが、[スタート]→[すべてのプログラム]→[WindowsUpdate]を選択することにより、実行できます。

d）離席時の対策

パソコンを使用中に離席する場合は、編集中のファイルを開いたままにしておくことは、好ましいことではありません。この場合は、一旦ログオフをするか、パスワード付のスクリーンセイバーを設定しておいてください。

e）バックアップ

人為的なミスや災害などにより、大切なデータを失ってしまう場合があります。その対策も、セキュリティ上必要なことです。データをパソコン以外の記憶媒体に保存しておくことを、バックアップといいます。定期的にバックアップをしておいてください。一般的には、バックアップ用の記憶媒体には、MOやCDなどが使われ、これらの媒体も個人情報が保存されていますので、管理は厳重にして、鍵がかかる保管庫などに入れておいてください。

f）データの消去

パソコンを売却や下取り、譲渡、廃却（リサイクル）などで手放すときには、重要データや個人情報を、完全に消去することが必要です。しかし、ハードディスクを再フォーマットしても、データを完全に消去することはできません。データを完全に消去するソフトを使用するか、廃棄する場合は、ハードディスクを取り外すなどが必要となります。

g）アクセスログの管理

アクセスログとは、いつ、誰が、どの情報を閲覧、書き込みしたかを記録したものです。アクセスログを管理することにより、万一の事故の際に、誰が、何をおこなったのかを特定することができます。また、外部からの不正なアクセスやその兆候を知ることができますので、対策もたてやすくなります。

h）電源のバックアップ

サーバーなどを使用している場合は、電源の確保も必要となってきます。停電、ブレーカ落ち、人為的なコンセント抜け、電圧変動などに備え、自力で電力を確保する準備が必要です。そのための機器として、UPS（無停電電源装置）があります。UPSのバッテリーに常時エネルギーを蓄えておくことで、突然の電源トラブルが発生しても、即座に自動でバッテリー運用に切り替わり、安定して電力を供給することができます。

ウ．利用環境や目的に応じて導入すべきセキュリティ対策

パソコンは、利用目的によって、さまざま使われ方をしています。また、事業所によってもパソコン環境は異なりますので、その環境に応じたセキュリティ対策が必要となってきます。セキュリティのレベルを高める方法として、セキュリティ専用のハードまたはソフトを導入する方法もあります。

インターネット・ネットワークは、情報の取得、共有する上で必要となる仕組みです。しかし、外部や複数のパソコンとの情報のやりとりにより、1台のパソコンだけを使用する場合と比べると、リスクが高まり、それに有効な対策を講じる必要があります。

■インターネット・ネットワークに関するリスク

・コンピュータウイルス　・不正侵入（無線LAN対策）
・スパイウェア　・有害サイトへのアクセス
・フィッシング

■電子メールに関するリスク

・スパムメール　・迷惑メール

●セキュリティ専用のハード

・生態認証システム・セキュリティロックシステム

●セキュリティ専用のソフト

・ウイルス対策ソフト　・セキュリティロックシステム

a）生体認証システム

パソコンへのログオンなど、キーボードでのパスワード入力のかわりに、指紋センサーに指先をつけ、本人かどうかを判断する仕組みです。この他にも、静脈認証や瞳認証など認証システムもありますが、一般的に、コストは高めです。

＜指紋認証＞

b）セキュリティロックシステム

USBフラッシュメモリなどを用いて、その機器を鍵として、パソコンにロックをかける仕組みです。IDカードのように首からぶら下げて、一定範囲外へと移動してしまった場合には、自動的にロックがかかるタイプや、携帯電話を鍵として用いるタイプもあります。

c）ウイルス対策ソフト

ウイルスを感知し、侵入を防ぐソフトですが、最近ではウイルスだけでなく、ネットワーク間の不正アクセスに対応したものや、スパムメールなどを防ぐ機能などがついた総合ウイルス対策ソフトが発売されています。しかし、ウイルスは、日々新しいものが作られるため、定期的な対策ソフトの更新が必要となります。この更新は、多くの場合、購入後1年間は無料ですが、それ以降は有料となるため、更新手続きが必要となります。この更新作業を怠ると、新しいウイルスに対応することはできませんので、注意してください。

技術的安全管理措置における用語解説

コンピュータウイルスとは

他人のコンピューターに勝手に入り込んで悪さをするプログラム。ディスクに保存されているファイルの破壊などをする。ウイルスは、インターネットからダウンロードしたファイルなどを通じて感染する。最近では、Eメールを介して感染するタイプのウイルス(ワーム)もある。大抵は、使用者の知らないうちに感染する。また、ネットワークを利用している場合は、ネットワークを介して、他のパソコンにも感染する。

スパイウェアとは

パソコンを使うユーザの行動や個人情報などを収集したりするソフト。得られたデータは、マーケティング会社など、スパイウェアの作成元に送られる。

フィッシングとは

金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺。「釣り」を意味する「fishing」が語源。

不正侵入とは（無線LAN対策）

あるコンピューターへの正規のアクセス権を持たない人が、ソフトウェアの不具合などを悪用してアクセス権を取得し、不正にコンピューターを利用する、あるいは試みること。とくに無線LANを使用している場合は、第三者が利用できないように、パスワードなどを必ず設定すること。

有害サイトへのアクセスとは

そのサイトを閲覧しただけで、ウイルスに感染するホームページ。または、Webブラウザに過剰な負荷をかけたり、ブラウザのセキュリティホールを悪用したりして、ブラウザやシステムを異常動作させようとするWebページへのアクセスをいう。

（4）業務委託先の監督

個人情報取扱事業者が業務を外部委託する場合、「第三者への情報提供」には当たりません。

ただし、利用者や社会に対して全ての責任を負うのは、当該事業者であり、「委託先の監督」が義務付けられています。従って、委託先の定期的チェックを行うことや、相応の（業務委託に相当する部分の）賠償リスクを転嫁することは、当然のことです。

また、委託先の選別は、規模や規程の有無という形式的な部分のみで行われている傾向もありますが、委託先がこれまでの実績があり信頼も置けるなら、個人情報取扱事業者として対応していることをしっかりと理解してもらい、自分達と同様の規制等体制を整えることを、共に実行していく方法もあります。育てていく、つまり、一緒に個人情報保護対策を進めていくということです（顔の見える信頼関係は規模や形式に勝ることも少なくありません）。

例 業務委託内容確認書

業務委託内容に関する確認書（個人情報保護の遵守）

甲（　　）と乙（　　）は業務委託に関し、個人情報保護に万全な配慮をもってこれにあたることとし、以下の内容を確認する。

第1条
乙は、甲より委託を受けた業務（以下、本件業務）の実施に際して知りえた個人情報については、厳重に管理し、正当な理由なく第三者に開示、提供、漏洩してはならない。

第2条
乙は、前条の義務を履行するため、自己の組織内に個人情報の安全管理に関する責任者を定め、十分な安全管理対策を講じなくてはならない。

第3条
乙は、本件業務における個人情報の安全管理に関する状況を、定期的に甲に対して報告するものとする。また、甲は、いつでも乙の個人情報の安全管理の状況について報告を求め、検査することができる。

第4条
乙は、本確認書にもとづく安全管理措置の内容を、自己のすべての従業員が、在職中、退職後を通じて遵守することを保証するものとする。

第5条
乙は、本件業務に関して、自ら保管する個人情報が漏洩したことにより甲に損害が生じた場合には、これを賠償するものとする。

第6条
本確認は、本件業務委託契約の終了後も有効に存続する。

年　　月　　日

甲　　印

乙　　印

（5）第三者提供

保護法では、個人情報取扱事業者が第三者に個人データを提供する際には、事前に本人の同意を取っておく必要があります。

もっとも、居宅サービス事業者の場合、介護保険法によって利用者の個人情報を第三者に提供する際には、事前に本人の同意を取っておくことが義務付けられているので、この点については、すでに習慣化されており、特に問題はないと思います。

しかし、利用者の個人情報を第三者に提供する際に、居宅サービス業務の一環として、事前に本人の同意を取ることが習慣化していても、それ以外の場面では、うっかり事前に本人の同意を取ることを忘れてしまう傾向があります。たとえば、利用者の情報を、会報誌やニュースレターに無断で載せてしまうような場合です。このような場合も、第三者提供に該当するので、必ず事前に、本人の同意を文書で取るように習慣化しておきましょう。

例 会報誌等に関するお伺い

ご利用者・ご家族様へ

（会社名）

（代表者名）

当社会報誌における個人情報の取扱いに関するお伺い

当社では、定期（適宜）に会報誌を作成し、ご利用者及びご家族の皆様に配布させていただいておりますが、掲載に関して同意していただける場合、また、掲載を希望されない場合につきましてお伺い申し上げます。
遠慮なくお申し出下さい。

1. 会報誌への掲載（苗字・お写真等）に同意します。

2. 利用者及び家族宅への配布（対象）に限って同意します。

3. 会報誌への掲載（苗字・お写真等）に同意しますが、以下について配慮してください。

〔　　〕

4. 会報誌への掲載を希望しません。

年　月　日

ご本人　印

ご家族　印

（6）保有個人データの開示、訂正、利用停止等

法令により、個人情報取扱事業者は、個人情報の開示、訂正、利用停止等の請求に、一部の例外を除き、応えなければなりません。

ただし、安易な開示、訂正、利用停止等は、かえって法令違反や、プライバシー侵害を招く恐れもありますので、一定のルールに従って行うことが大切です。

以下、それぞれの「請求書」及び「回答」例を紹介します。

①開示

例　情報開示請求書

年　　月　　日

個人情報開示請求書

（会社名）

御中

私は、貴社が保有する下記個人情報を開示していただきたく請求いたします。
尚、情報開示に係わる実費　　円（通常1,000～3,000円程度）負担を了承いたします。

該当の本人	氏　名	
	住　所	
	生年月日	
開示を請求する情報	居宅介護計画書（時期目途　　） 訪問介護計画書（時期目途　　） サービス提供記録 過去の請求書　　その他（具体的に）	その他 （具体的に）

開示請求者　住　所：
氏　名：
電話番号：
本人との関係：

私は、請求者　　に対して、貴社が上記の内容に沿って情報開示することに同意いたします。

本人（自筆）

例 情報開示回答書

年　　月　　日

様

会社名

担当者

開示請求に関する回答書

本人氏名	
請求情報	

開示請求をいただいておりました上記案件につきまして回答申し上げます。

1. **開示いたします。**

つきましては　　年　　月　　日以降　　年　　月　　日までにお渡しいたします。
受け取り方法につきましてはご相談いたします。
尚、受け渡しの際には別途実費として　　円をご用意下さい。

2. **開示できません。**

理由

（ ） 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ため

（ ） 当社の業務運営に著しい支障を及ぼすおそれがあるため

（ ） 開示することが法令に違反するため

②電話での問い合わせルールについて

電話への問い合わせ対応は、保護法施行の前と後で、最も意識しなければならないことの一つです。

これまでは、利用者の家族というだけで、質問に答えることが自然な対応に近かったかもしれません。しかしながら、利用者本人以外は第三者であり、仮に兄弟だとしても、予め定めた身元引受人でもない限り、本人の同意なくしては、情報提供してはいけません。通常は、「情報開示請求書」等の書面により、請求事実と同意の証拠を備えておくべきでしょう。

ただし、明らかに本人の同意が得られている、または、電話等でも明らかに本人が同意しているような場合には、書面云々のルールのみの優先は、お勧めできません。顧客サービスが劣化しないことも、重要なことです。

例 電話対応ルール（貼り出し用）

電話対応ルール（主に訪問事業所向け／貼り出し）

① 個人情報に関する第三者からの問い合わせについては原則お断りする。
※但し、電話の声やID情報等で身元引受人（家族代表）であることが明確な場合、又は回答の内容のみで個人情報に該当しない場合には例外とする。

② 第三者に個人情報を提供する場合は、書面による開示請求をお願いし、本人の同意を取り付けた後で提供する。

③ 本人からの問い合わせで声やID情報により本人が確認できる場合でも（万が一の思い違いもあるので）、電話ではプライバシーに深く係わる情報には極力応答しない。又、本人の登録してある電話番号に折り返しの対応とする。

④ 緊急の場合、例えば急病で入院した病院から情報を求められた場合、法令の適用外【本人の生命・身体・財産の保護のためであって、本人の同意が得られる状況にない時】と判断しうる時には応答する。
但し、緊急性のない場合や本人が電話口に出られる時には、本人の同意を取った上で応答する。

⑤ その他判断がつきかねる時には、事務局（代表又は副代表）に判断を仰ぐ。

③追加・訂正・削除等

例 **追加・訂正・削除請求書**

年　　月　　日

個人情報の追加・訂正・削除請求書

（会社名）

御中

私は、貴社が保有する下記個人情報について追加・訂正・削除をしていただくよう請求いたします。

該当の本人	氏　名
	住　所
	生年月日
追加・訂正・削除を請求する文書、項目	
上記の内容・部分	

開示請求者　住　所：

氏　名：

電話番号：

本人との関係：

私は、請求者　　に対して、上記の請求に関する一切を委任します。

本人（自筆）

例 追加・訂正・削除回答書

年　　月　　日

様

会社名

担当者

個人情報の追加・訂正・削除に関する回答書

該当の本人	氏　名
	住　所
	生年月日
追加・訂正・削除を請求する文書、項目	
上記の内容・部分	

請求をいただいておりました上記案件につきまして回答申し上げます。

1. 追加 ・ 訂正 ・ 削除　いたします。

なお、　　年　　月　　日付けで措置を講じました。

原本の複写をお求めの場合には別途ご指示ください。
実費　　円を申し受けます。

2. 追加 ・ 訂正 ・ 削除　できません

理由

（ ）利用目的から見て訂正等が必要でないため
（ ）誤りがあるとのご指摘が正しくないため
（ ）訂正要請事項が事実でなく評価であるため
（ ）ご指摘事項について当社では訂正の権限がないため
（ ）その他［　　］

④利用停止等

例 **利用停止・第三者への提供禁止・消去請求書**

年　　月　　日

個人情報の利用停止・第三者への提供禁止・消去請求書

（会社名）

御中

私は、貴社が保有する下記個人情報について利用停止・第三者への提供禁止・消去をしていただくよう請求いたします。

該当の本人	氏　名
	住　所
	生年月日
利用停止・第三者への提供禁止・消去を請求する文書、項目	
上記の内容	
請求の理由	（ ） 利用目的を超えている （ ） 不正な手段によって取得された情報である （ ） その他［　　］

開示請求者

住　所：＿＿＿＿＿＿＿＿＿＿

氏　名：＿＿＿＿＿＿＿＿＿＿

電話番号：＿＿＿＿＿＿＿＿＿＿

本人との関係：＿＿＿＿＿＿＿＿＿＿

私は、請求者＿＿＿＿＿＿＿＿＿＿に対して、上記の請求に関する一切を委任します。

本人（自筆）＿＿＿＿＿＿＿＿＿＿

例 利用停止・第三者への提供禁止・消去回答書

年　　月　　日

様

会社名

担当者

個人情報の利用停止・第三者への提供禁止・消去に関する回答書

本人氏名	
請求文書・項目	
上記の内容	

請求をいただいておりました上記案件につきまして回答申し上げます。

1. 利用停止・第三者への提供禁止・消去　いたします。

なお、　　年　　月　　日付けで措置を講じました。

2. 利用停止・第三者への提供禁止・消去　できません。

理由

（　）利用目的の逸脱が認められない

（　）情報の取得に不正が認められない

（　）その他［　　］

5 保有個人データに関する一定の事項の公表

法令（法第24条）により、個人情報取扱事業者は、以下のような保有個人データに関する一定の事項を利用者に公表しなければなりません。

1）個人情報取扱事業者（居宅サービス事業者）の氏名又は名称
2）保有個人データの利用目的
3）保有個人データに関する諸手続
利用目的の通知を求めるための手続き
a）開示を求めるための手続き
b）訂正等を求めるための手続き
c）利用停止等を求めるための手続き
d）第三者への提供の停止を求めるための手続き
4）保有個人データの適正な取り扱いの確保に関し、必要な事項として、政令で定めるもの（現在は以下の2つ）
a）当該個人情報取扱事業者が行う、保有個人データの取り扱いに関する苦情の申出先（部署名、電話番号、メールアドレス等）
b）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

公表方法としては、「Ⅰ 基礎知識編」でも述べたように、契約を締結する際に、重要事項説明書と一緒に紙面で本人に直接伝えるのが望ましいと考えられます。もちろん、後述する「個人情報保護方針」にこれらの事項を記載しておき、重要事項説明書と一緒に利用者に渡してもかまいません。ただし、現在、居宅サービス事業者が公表している「個人情報保護方針」を見てみると、上記事項の記載漏れが非常に目立ちます。上記事項は必須事項ですので、記入漏れがないように十分気をつけてください。

また、長ったらしい個人情報保護方針を利用者に見せるのが利用者の負担になる心配があるのであれば、次頁のような保護法上通知・公表が義務づけられている部分だけを抜き出した簡易版の個人情報保護方針を作成して、それを利用者に渡す方法をとってもよいと思います。

例 個人情報保護方針簡易版（法第24条対応書式）

平成　　年　　月　　日

【　　】における個人情報の取り扱いについて

＜法令遵守＞

当社は、個人情報保護法・ガイドライン・介護保険法等の法令・諸規範等に基づいて、お客様の個人情報を適切に取り扱います。

＜利用目的＞

当社では、お客様からお預かりした個人情報を、下記の目的で利用します。

① ○○○○○
② ○○○○○
③ ○○○○○

＜第三者提供の制限＞

当社では、お客様からお預かりした個人データを、あらかじめ本人の同意を得ることなく、第三者に提供することはいたしません。ただし、法令等に基づく場合、○○○○○の場合、○○○○○の場合は、この限りではありません。

＜個人データの開示、訂正、利用停止等の請求＞

お客様は、当社が保有しているお客様の個人データについて、いつでもその開示、修正、追加、訂正、利用停止等を請求することができます。請求を希望される方は、下記の手続きに従ってご請求下さい。

①
②
③　（請求先、記入用紙、費用などについて箇条書きで説明）

＜苦情処理＞

当社の個人情報の取り扱いに関する苦情やご質問は、下記までご連絡下さい。

①事業者名、担当者名
②電話番号、Fax番号
③住所、等

6 「個人情報保護方針」の作成・公表

保護法において、通知・公表が義務付けられているのは、法18条の利用目的の特定のところと、前頁で紹介した法第24条関係で掲げられている項目のみです。

しかし、保護法やガイドラインでは、個人情報取扱事業者が、自らの個人情報保護方針について、ホームページ等で公表することを勧めています。そのため、居宅サービス事業者としても、個人情報保護方針を作成して公表しておくことがよいでしょう。

なお、「個人情報保護方針」は、あくまでも、事業者が、自らの個人情報の取り扱い方針を外部に伝えるものであります。ですから、参考書やガイドラインの書式を、そのまま引用するのでは意味がありません。本マニュアル（実践編）の「各義務規定の遵守方針の決定・準備」（37頁～65頁）のところで、個人情報の取り扱い方針を決められたら、その内容を「個人情報保護方針」に記載して、あくまでも、独自の方針を作成するように努力しましょう。

また、介護分野の場合、その方針を伝えなければいけない相手方の多くは、要介護状態にある高齢者ということになります。したがって、どんなに立派な内容の個人情報保護方針であっても、細かい字で長々と書かれていたり、難しい専門用語が多く使われたりしているようなものでは、意味がありません。利用者が読むのに負担にならないような、個人情報保護方針を作成することも非常に大切です。もし、どうしても詳細な内容を含んだ個人情報保護方針を作成・公表したいのであれば、オリジナルと簡易版の2種類を作成して、オリジナルは、ホームページで公表し、簡易版は、利用者に手渡すような工夫をするとよいでしょう。

例 個人情報保護方針

会社・団体名［　　］個人情報保護方針

当社では、良質な介護サービスをご提供させていただくために、お客様のプライバシーに十分配慮した上で、個人情報を適切に取り扱うことを宣言します。

（法令遵守）
当社は、個人情報保護法・ガイドライン・介護保険法等の法令・諸規範を遵守します。

（職員教育）
当社は、個人情報の適切な取り扱いのための職員教育を実施します。

（個人情報の取得・利用）
当社は、お客様やご家族の個人情報の取得にあたり、利用目的を明示しその目的に必要な範囲の個人情報を取得し、利用目的以外に利用しません。
目的にない利用の場合、お客様の同意なしに第三者に情報提供することはいたしません。ただし、法令に定める例外を除きます。

（情報の安全な管理）
当社では、お客様の個人情報を盗難、不正アクセス、紛失、改ざん等から守るために、適切な安全対策を講じます。
また、社員教育・内部統制・システムセキュリティ等の継続的な見直しを図り、お客様の個人情報保護の向上に努めます。

（個人情報の第三者提供）
当社は、お客様やご家族の個人情報をその利用目的の範囲に沿って、第三者（医療関係機関、介護事業者、外部委託事業者）に提供することがあります。
第三者に提供する場合は、利用者やご家族の同意を得ることとします。
また、外部委託事業者に対しては、個人情報を適切に取り扱うよう指導、監督を行います。

（個人情報についての問い合わせ）
お客様又は第三者が個人情報についての情報時開示、修正、追加、削除、利用停止などをご要望される場合には、お客様がご本人であること、あるいはご本人の同意を得た上で、合法的且つ合理的な範囲でご要望に対応させていただきます。

（会社名）＿＿＿＿＿＿＿＿＿＿

（代表者名）＿＿＿＿＿＿＿＿＿＿

7 個人情報保護規程の策定

個人情報保護方針を、羅針盤と例えるなら、個人情報保護規程は、航海図であり、乗組員が守るべき基本ルールです。個別のルールを作成するとき、また迷った際に戻るべき「拠りどころ」です。

2006年度スタートの「介護サービス情報の公表」では、訪問介護事業者への調査項目（予定）の中で、個人情報に関する規程をホームページで公表していることが、確認項目の一つにあがっています（義務ではありません）。

なお、個人情報保護方針と同じく、個人情報保護規程も事業所独自のものでなければ意味がありません。参考書やガイドラインの書式をそのまま引用するのではなく、本マニュアル（実践編）の「各義務規定の遵守方針の決定・準備」（37頁～65頁）の内容を織り込み、事業所独自の「個人情報保護規程」を作成しましょう。

以下、個人情報保護規程を例示します。

例 個人情報保護に関する規定項目

1. 目的
   (1) 目的
   (2) 本規定の対象と守秘義務
   (3) 本規定の事務局
2. 用語の定義
   (1) 個人情報
   (2) 個人情報の利用
   (3) 第三者への情報提供
3. 個人情報の取得
   (1) 利用目的の通知
   (2) 利用目的の変更
4. 個人情報の安全な管理
   (1) 個人情報台帳の設置
   (2) パソコン等によるデーター管理
   (3) 紙ベースのデーター管理
   (4) 外部委託について
   (5) 介護現場における個人情報管理
5. 個人情報の利用
6. 個人情報の第三者への提供
7. 個人情報の開示訂正等
   (1) 個人情報の開示
   (2) 個人情報の訂正・追加・削除
   (3) 個人情報の利用停止
8. 相談、苦情対応
9. 罰則、賠償等
10. 教育・研修
11. その他

例 個人情報保護規程(1/4)

（会社名）[　　社] 個人情報保護に関する規程

1. 目的

(1) 目的

本規程は、当社が取り扱う個人情報の保護のために必要な要件等を定め、法令・ガイドライン等を遵守し、適切に個人情報を取扱うことを目的とする。

(2) 本規程の対象と守秘義務

本規程の対象は、役職員・非常勤・アルバイト等を含む全ての従業者および全ての業務とする。職種の如何を問わず、守秘義務を遵守するものとする。

(3) 事務局

本規程の事務局は、△△△△とする。

2. 用語の定義

(1) 個人情報

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・その他の記述により、個人を識別できるもの。ただし、「ガイドライン」の主旨から、死者情報についても同様に取扱う。

(2) 個人情報の利用

業務の遂行に必要な、個人情報の取扱い全般（個人情報の参照、処理、加工等）をいう。

(3) 第三者への情報提供

当社が保有する個人情報を、第三者に利用可能にすることをいう。ただし、共同利用・委託は、第三者提供に含まない。その他、法令第23条に従うものとする。

3. 個人情報の取得

(1) 利用目的の通知

お客様から個人情報を取得する際には、その利用目的を通知する。

利用については、目的の範囲を超えてはならない。第三者に提供する場合には、あらかじめ本人の同意を得る。ただし、法令の例外規定にあるものは除く。

(2) 利用目的の変更

特定した利用目的を追加・変更する場合には、あらためて通知・公表する。

例 個人情報保護規程(2/4)

4. 個人情報の安全な管理

個人情報台帳を作成し、個人情報の洗い出し、安全な管理、適切な更新、期限切れ情報の破棄を、適時に行う。

(1) パソコン等電磁的・機械的データ管理

① 介護記録等を、コンピュータ等で保存、処理する場合には、処理をする担当を限定し、パスワード・IDによるアクセス制限を行う。

② 通信回路を使用する場合には、漏洩やデータ破損が起きないよう対策を講じる。

③ データ処理の最中、社内、来客を問わず、安易にPC画面が確認出来ないよう配慮（配置）する。

また、PC自体の盗難に対しても対策を講じる。

④ 機械的な故障等によるデータ消失に備えて、バックアップを適時行う。

⑤ バックアップ以外のデータコピーは、原則禁止とする。作業上必要があるときには、事務局（代表者、副代表、等）の了解を取り付ける。

⑥ プリントアウトしたデータは、紙データ管理に従い、厳重に管理する。使用を終えた場合は、速やかに破棄する。（粉砕または焼却処理等）

(2) 紙ベースのデータ管理

① 個人情報データについては、業務終了時に所定の保管場所に収納し、盗難、汚損、消失等に留意する。（ガラス張りでない、極力カギのかかるロッカーで保管する。）

② データは原則持ち出し禁止とする。

業務上必要な場合は、集合的なファイルではなく、個別ごとの情報とする（最小限に抑える）。事務局の了解を必要とするが、日常的に必要な場合は、別途ルールを定める。

③ データに、追加、訂正を加える必要がある場合は、上書きせず、用紙の追加を原則とする。

やむを得ず書きする場合には、訂正日、訂正箇所・内容、担当者を明確にする。

④ 保存期間を過ぎたもの、利用の必要がなくなったものについては、速やかに破棄（粉砕、焼却処理等）する。

例 個人情報保護規程(3/4)

(3) 外部委託について

個人情報の取扱い、保管等を外部委託する場合には、以下に留意して行うものとする。

① 業務上の必要最小限にとどめる。

② 業者の見極め、見直しを行う。(実績、個人情報保護規程があるか等)

③ 賠償責任の所在も含めた取決め(確認)を行う。

(4) 介護現場における個人情報管理

現場における個人情報管理は、「介護現場における個人情報保護は、即ちプライバシー保護である」ことを全職員が認識して業務にあたる。

5. 個人情報の利用

個人情報は、あらかじめ特定通知した利用目的以外には利用してはならない。ただし、法令による例外規定は除く。業務上必要が生じた場合は、事務局と相談、承認の上、利用目的を追加通知する。

6. 個人情報の第三者への提供

個人情報を第三者に提供する場合には、本人の同意を得なくてはならない。原則として、当社は、介護サービス開始時に、個人情報の利用目的通知及び第三者提供の目的を説明し、同意を得ることとする。第三者提供の目的に変更・追加が生じた際は、改めて同意を得るものとする。なお、同意に関する適用除外については、法令に従う。

7. 個人情報の開示、訂正、削除、利用停止

(1) ご利用者本人、家族代表等により、個人情報の開示を求められた場合には、所定の書面を以って行い、担当者、所属長で確認、相談後、事務局がすみやかに対応する。

第三者からの請求の場合には、法令による例外規定を除いて、必ず本人の同意を得る。

ただし、以下のケースと判断される場合には、その理由を明示した上でお断りすることがある。

・本人または第三者の生命・身体・財産その他の権利利益を害する恐れのある場合

・当社業務に著しい支障を及ぼす恐れがある場合

・開示することが法令に違反する場合

例 個人情報保護規程(4/4)

(2) 個人情報の訂正、追加、削除を求められた場合には前記 (1) 同様の対応とする。
ただし、以下のケースと判断される場合には、その理由を明示した上でお断りすることがある。

・本人または第三者の生命・身体・財産その他の権利利益を害する恐れのある場合
・当社業務に著しい支障を及ぼす恐れがある場合
・開示することが法令に違反する場合
・訂正することが正しくないと判断される場合（事実に相違する場合等）
・訂正を求められた事項が「事実」でなく、「評価」に関する場合
・当社に訂正の権限がない場合

(3) 個人情報の利用停止
個人情報の利用停止あるいは第三者への利用停止請求があった場合は、所定の書面によって前記 (1) 同様の速やかな対応により、これを行う。ただし、特別な理由（介護保険請求事務が終了していない等）がある場合は、理由を示した上でお断りすることがある。

8. 相談・苦情
個人情報の取扱いに関する相談・苦情の窓口は、事務局とする。
相談窓口があることを、ご利用者に通知する。

9. 罰則・賠償等
役員、職員（全ての従事者）が、個人情報を故意の重大な過失等、恣意的に漏洩した場合には、損害賠償を負うものとし、解雇を含む処罰の対象とする。
ただし、業務上の過失（ミス）によるものはこの限りでない。

10. 教育・研修
本規程の主旨を役員、職員が理解し遵守できるよう、事務局は、定期的に研修を行う。

11. その他
本規定に定めのない事項は、法令、諸規範に照らして、事務局が判断する。
（この場合は、極力、外部の専門家等の意見も参考にする）

part Ⅲ

資料編

資料1　個人情報管理に関するアンケート調査

調査概要

調査目的

個人情報保護に関する居宅介護事業者の現状をアンケートにより探り、個人情報管理の問題意識および実施における課題を抽出し、その結果をマニュアルに反映する。

調査対象

15大都市を含む都道府県（北海道・宮城県・埼玉県・千葉県・東京都・神奈川県・静岡県・愛知県・京都府・大阪府・兵庫県・広島県・福岡県）の訪問介護事業所のうち、無作為抽出した2,000件

※15大都市：14政令指定都市（札幌市、仙台市、さいたま市、千葉市、川崎市、横浜市、静岡市、名古屋市、京都市、大阪市、神戸市、広島市、北九州市、福岡市）に東京都を加えた都市

調査時期

2005年11月1日～11月22日

調査方法

質問紙による郵送（一部ＦＡＸを併用）

回収数

11月22日までに回収された335事業所（集計率：16.8%）

■発送件数

（事業所）　（%）

都道府県	発送数	回収数	回収率
東京都	355	65	18.3
大阪府	327	56	17.1
神奈川県	202	31	15.3
福岡県	177	24	13.6
兵庫県	159	26	16.4
埼玉県	144	16	11.1
千葉県	136	21	15.4
北海道	129	28	21.7
愛知県	128	23	18.0
広島県	80	12	15.0
宮城県	51	11	21.6
静岡県	71	17	23.9
京都府	41	3	7.3
	2,000	335	16.8

注）地域不明2件

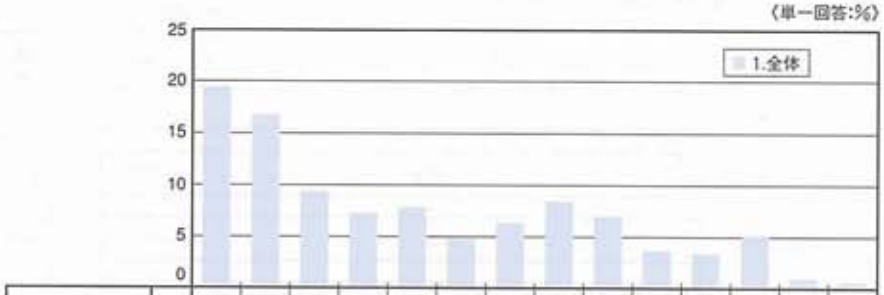
集計結果に関する注意点

本集計結果は、地域別、理解度別についても掲載しているが、区分ごとの件数が少ないため、数字を読み取るにあたって、注意が必要である。

1．回答事業所

■都道府県別回答事業所

〈単一回答:%〉



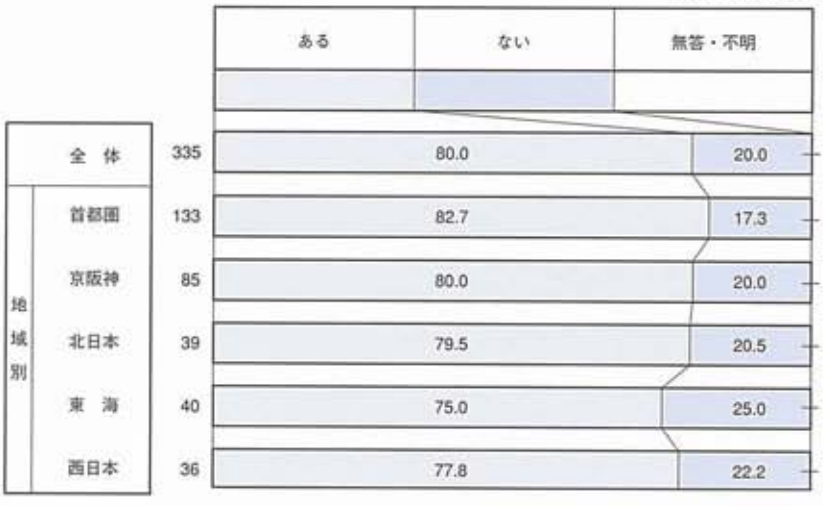
		集計数	東京都	大阪府	神奈川県	福岡県	兵庫県	埼玉県	千葉県	北海道	愛知県	広島県	宮城県	静岡県	京都府	無答・不明
全体		335	19.4	16.7	9.3	7.2	7.8	4.8	6.3	8.4	6.9	3.6	3.3	5.1	0.9	0.6
地域別	首都圏	133	48.9	—	23.3	—	—	12.0	15.8	—	—	—	—	—	—	—
	京阪神	85	—	65.9	—	—	30.6	—	—	—	—	—	—	—	3.5	—
	北日本	39	—	—	—	—	—	—	—	71.8	—	—	28.2	—	—	—
	東　海	40	—	—	—	—	—	—	—	—	57.5	—	—	42.5	—	—
	西日本	36	—	—	—	66.7	—	—	—	—	—	33.3	—		—	—

F

2．個人情報保護法の対応における疑問や苦労

■個人情報保護法の対応における疑問や苦労の有無

＜単一回答：%＞

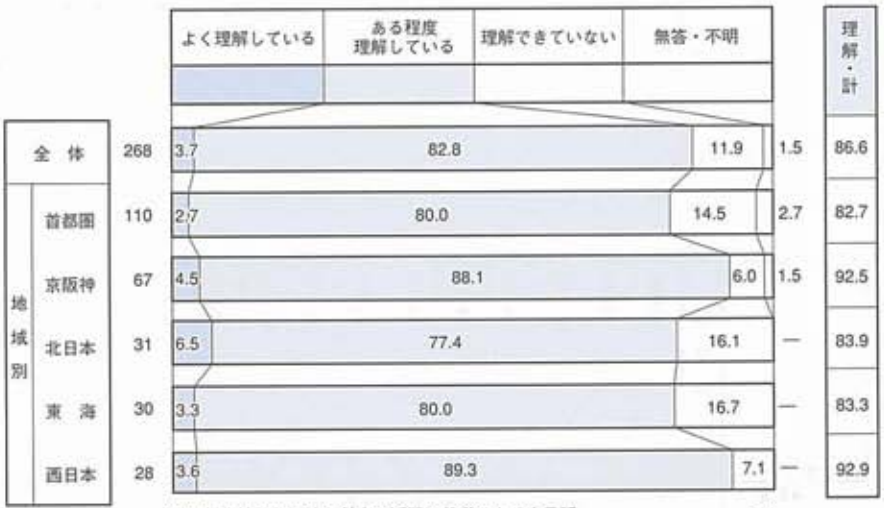


Q1

3．ガイドライン（厚生労働省作成）の内容についての理解

■ガイドライン（厚生労働省作成）の内容についての理解

<単一回答：%>



注）個人情報保護法の対応で疑問や苦労のある事業所　Q2

4．個人情報管理の対策で困っていること

■個人情報管理の対策実施

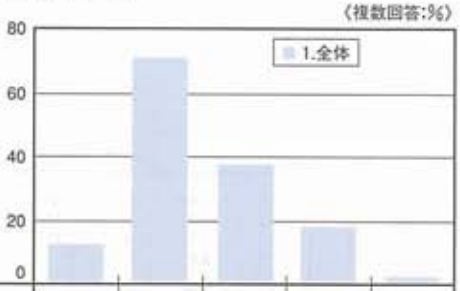
〈単一回答:%〉

集計数　268

注）個人情報保護法の対応で疑問や苦労のある事業所

■個人情報管理の対策で困っていること

〈複数回答:%〉



		集計数	どのような対策を取ればよいか分からない	対策を取っているが、必要なことが適切にできているかよく分からない	対策を取っているが、疑問や不明な点について情報を得る機会がない	対策を取っているが、日々の業務に追われてすべてについて形骸化してきている	無答・不明
全　体		268	13.1	71.3	37.7	17.9	2.2
地域別	首都圏	110	14.5	70.9	38.2	18.2	1.8
	京阪神	67	9.0	68.7	38.8	22.4	4.5
	北日本	31	16.1	77.4	25.8	19.4	—
	東　海	30	16.7	60.0	33.3	10.0	3.3
	西日本	28	10.7	82.1	50.0	14.3	—
理解	よく理解	10	—	30.0	20.0	40.0	20.0
	ある程度理解	222	7.2	74.8	39.6	18.9	1.8
	未理解	32	56.3	56.3	28.1	6.3	—

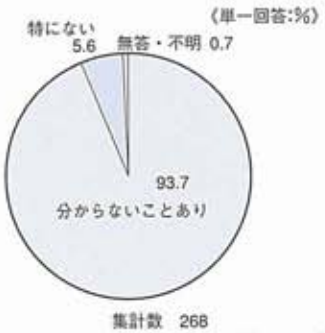
注）個人情報保護法の対応で疑問や苦労のある事業所
「理解」は厚生労働省作成のガイドラインの内容についての理解

Q3

5．事業所の対策・取り組みにおける問題点

①使用目的の特定、通知・公表

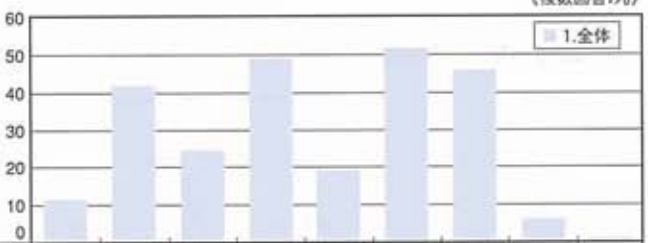
■利用目的の特定、通知・公表



注）個人情報保護法の対応で疑問や苦労のある事業所

■個人情報管理の具体的対策【A.利用目的の特定、通知・公表について】

（複数回答:%）



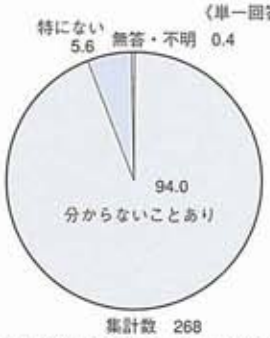
		集計数	利用目的の特定を、どのようにすればよいか分からない	利用目的を特定しているが、必要なことが適切に示されているかよく分からない	利用目的の通知・公表を、どのようにすればよいか分からない	契約時、利用目的を説明しているが、必要なことが適切にできているかよく分からない	掲示物やHP、配布物で利用目的を説明しているが、必要なことが適切にできているかよく分からない	重度の認知症の利用者等に対し、どのように通知・公表すればよいかよく分からない	緊急時に、どのように通知・公表すればよいかよく分からない	分からないことは、特にない	無答・不明
全体		268	11.9	41.8	24.3	48.9	19.0	51.5	45.1	5.6	0.7
地域別	首都圏	110	10.9	53.6	25.5	50.9	20.9	53.6	49.1	3.6	0.9
	京阪神	67	13.4	31.3	23.9	52.2	16.4	55.2	46.3	6.0	1.5
	北日本	31	12.9	35.5	32.3	45.2	12.9	45.2	48.4	9.7	—
	東海	30	10.0	36.7	10.0	43.3	13.3	50.0	40.0	—	—
	西日本	28	14.3	32.1	28.6	39.3	28.6	46.4	32.1	3.6	—
理解	よく理解	10	—	40.0	10.0	50.0	20.0	30.0	30.0	20.0	—
	ある程度理解	222	7.7	41.4	23.0	48.6	20.3	53.2	44.1	4.5	0.9
	未理解	32	46.9	40.6	37.5	53.1	12.5	50.0	59.4	—	—

注）個人情報保護法の対応で疑問や苦労のある事業所
「理解」は厚生労働省作成のガイドラインの内容についての理解

Q4 A

②個人情報の安全管理対策

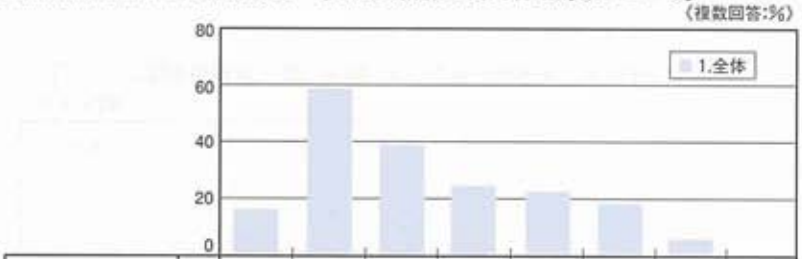
■個人情報の安全管理対策



注）個人情報保護法の対応で疑問や苦労のある事業所

■個人情報管理の具体的対策　【B.個人情報の安全管理対策について】

〈複数回答:%〉



		集計数	安全管理対策を、どのようにすればよいか分からない	安全管理対策を取っているが、必要なことが適切にできているかよく分からない	利用者情報が入ったパソコン等に、どのような対策を取ればよいかよく分からない	利用者記録やメモ等の紙媒体を、どのように保管・管理すればよいかよく分からない	従業員や実習生、ボランティアへの指導が、十分にできていない	従業員や実習生、ボランティアの教育・研修を、どのように行えばよいかよく分からない	分からないことは、特にない	無答・不明
全　体		268	16.8	59.7	39.6	25.0	23.9	19.0	5.6	0.4
地域別	首都圏	110	14.5	62.7	44.5	29.1	26.4	18.2	5.5	0.9
	京阪神	67	25.4	56.7	37.3	23.9	22.4	19.4	6.0	—
	北日本	31	16.1	64.5	35.5	22.6	19.4	19.4	6.5	—
	東　海	30	13.3	43.3	43.3	26.7	23.3	23.3	3.3	—
	西日本	28	10.7	64.3	28.6	14.3	25.0	17.9	—	—
理解	よく理解	10	20.0	40.0	40.0	30.0	10.0	10.0	30.0	—
	ある程度理解	222	10.8	64.4	37.4	23.0	24.8	18.0	4.5	—
	未理解	32	53.1	37.5	50.0	37.5	21.9	28.1	—	3.1

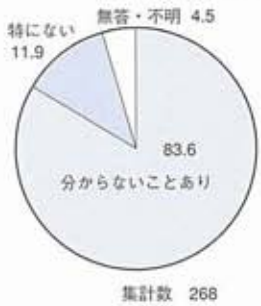
注）個人情報保護法の対応で疑問や苦労のある事業所
「理解」は厚生労働省作成のガイドラインの内容についての理解

Q4B

③個人情報の第三者提供制限

■個人情報の第三者提供制限

〈単一回答:%〉



集計数 268

注）個人情報保護法の対応で疑問や苦労のある事業所

■個人情報管理の具体的対策【C.個人情報の第三者提供制限について】

〈複数回答:%〉

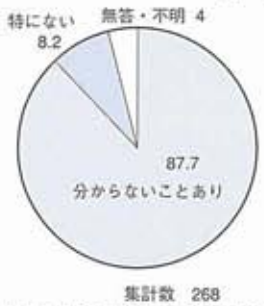
		集計数	「第三者提供制限」の規定（例外や本人への再確認等）が、何かよく分からない	誰が「第三者」に該当するのかよく分からない	重度の認知症の利用者等、本人の同意を得るのが困難な時の対応方法がよく分からない	分からないことは、特にない	無答・不明
全体		268	40.7	34.0	49.6	12.7	4.5
地域別	首都圏	110	45.5	40.0	53.6	7.3	2.7
	京阪神	67	46.3	40.3	47.8	13.4	1.5
	北日本	31	35.5	32.3	38.7	19.4	9.7
	東海	30	33.3	20.0	50.0	10.0	3.3
	西日本	28	25.0	14.3	53.6	21.4	7.1
理解	よく理解	10	20.0	20.0	40.0	30.0	10.0
	ある程度理解	222	36.9	31.5	50.0	12.6	4.5
	未理解	32	65.6	53.1	53.1	3.1	3.1

注）個人情報保護法の対応で疑問や苦労のある事業所
「理解」は厚生労働省作成のガイドラインの内容についての理解　Q4C

④プライバシーポリシーの作成・公表

■プライバシーポリシーの作成・公表

〈単一回答:%〉

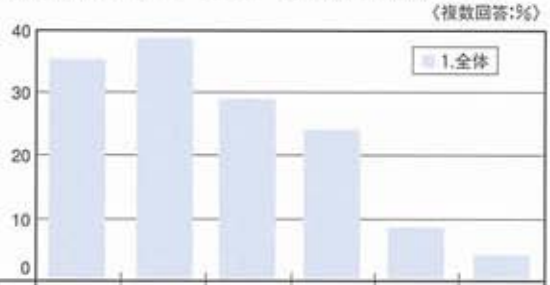


集計数　268

注）個人情報保護法の対応で疑問や苦労のある事業所

■個人情報管理の具体的対策【D.プライバシーポリシーの作成・公表について】

〈複数回答:%〉



		集計数	「プライバシーポリシー」が、何かよく分からない	どのような事項を記載すればよいかよく分からない	作成をしているが、必要なことが適切に示されているかよく分からない	通知・公表を、どのようにすればよいか分からない	分からないことは、特にない	無答・不明
全　体		268	35.4	38.8	29.1	23.9	8.6	4.1
地域別	首都圏	110	41.8	40.0	31.8	26.4	6.4	1.8
	京阪神	67	32.8	40.3	28.4	25.4	9.0	1.5
	北日本	31	32.3	41.9	16.1	25.8	19.4	6.5
	東　海	30	36.7	36.7	26.7	13.3	6.7	10.0
	西日本	28	21.4	32.1	39.3	21.4	3.6	3.6
理解	よく理解	10	10.0	—	40.0	10.0	40.0	10.0
	ある程度理解	222	31.1	37.4	30.6	23.4	8.1	4.5
	未理解	32	68.8	62.5	18.8	34.4	—	—

注）個人情報保護法の対応で疑問や苦労のある事業所
「理解」は厚生労働省作成のガイドラインの内容についての理解　　Q4D

資料２　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(抜粋)

厚生労働省

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、「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６条第３項及び第８条の規定に基づき、法の対象となる病院、診療所、薬局、介護保険法に規定する居宅サービス事業を行う者等の事業者等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ガイドラインとして定めるものであり、厚生労働大臣が法を執行する際の基準となるものである。

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、法第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、各医療機関等における積極的な取組が求められている。また、介護分野においても、介護関係事業者は、多数の利用者やその家族について、他人が容易には知り得ないような個人情報を詳細に知りうる立場にあり、医療分野と同様に個人情報の適正な取扱いが求められる分野と考えられる。このことを踏まえ、本ガイドラインでは、法の趣旨を踏まえ医療・介護関係事業者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、各医療・介護関係事業者においては、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、医療・介護関係事業者は、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。

3．本ガイドラインの対象となる「医療・介護関係事業者」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、①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（以下「医療機関等」という。）、②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険施設を経営する事業、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経営する事業その他高齢者福祉サービス事業を行う者（以下「介護関係事業者」という。）であり、いずれについても、個人情報保護に関する他の法律や条例が適用される、国、地方公共団体、独立行政法人等が設置するものを除く。ただし、医療・介護分野における個人情報保護の精神は同一であることから、これらの事業者も本ガイドラインに十分配慮することが望ましい。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、業務の委託に当たり、本ガイドラインの趣旨を理解し、本ガイドライン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。また、法令上、「個人情報取扱事業者」としての義務等を負うのは医療・介護関係事業者のうち、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、医療・介護関係事業者は、個人情報を提供して医療・介護関係事業者からサービスを受ける患者・利用者等から、その規模等によらず良質かつ適切な医療・介護サービスの提供が期待されていること、そのため、良質かつ適切な医療・介護サービスの提供のために最善の努力を行う必要があること、また、患者・利用者の立場からは、どの医療・介護関係事業者が法令上の義務を負う個人情報取扱事業者に該当するかが分かりにくいこと等から、本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・介護関係事業者にも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、医療・介護関係事業者が保有する生存する個人に関する情報のうち、医療・介護関係の情報を対象とするものであり、また、診療録等の形態に整理されていない場合でも個人情報に該当する。なお、当該患者・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する。

５．大臣の権限行使との関係等

本ガイドライン中、【法の規定により遵守すべき事項等】に記載された内容のうち、医療・介護関係事業者の義務とされている内容を個人情報取扱事業者としての義務を負う医療・介護関係事業者が遵守しない場合、厚生労働大臣は、法第３４条の規定に基づき、「勧告」及び「命令」を行うことがある。また、法の適用除外とされている小規模事業者については、努力義務として本ガイドラインの遵守が求められる。また、法第５１条及び「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。以下「令」という。）第１１条において、法第３２条から第３４条に規定する主務大臣の権限に属する事務は、個人情報取扱事業者が行う事業であって当該主務大臣が所管するものについての報告の徴収、検査、勧告等に係る権限に属する事務の全部又は一部が、他の法令の規定により地方公共団体の長その他の執行機関が行うこととされているときは、当該地方公共団体の長等が法に基づく報告の徴収、助言、勧告及び命令を行うことがある。

６．医療・介護関係事業者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。医療・介護関係事業者は、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、患者等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、迅速に情報提供を行う等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、医療・介護関係事業者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及び本ガイドライン等を遵守すること等、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。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医療・介護関係事業者で個人情報が利用される意義について患者・利用者等の理解を得ること。②医

療・介護関係事業者において、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。

7．責任体制の明確化と患者・利用者窓口の設置等

医療・介護関係事業者は、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、患者・利用者等に対しては、受付時、利用開始時に個人情報の利用目的を説明するなど、必要に応じて分かりやすい説明を行う必要があるが、加えて、患者・利用者等が疑問に感じた内容を、いつでも、気軽に問い合わせできる窓口機能等を確保することが重要である。また、患者・利用者等の相談は、医療・介護サービスの内容とも関連している場合が多いことから、個人情報の取扱いに関し患者・利用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するとともに、その窓口がサービスの提供に関する相談機能とも有機的に連携した対応が行える体制とするなど、患者・利用者等の立場に立った対応を行う必要がある。なお、個人情報の利用目的の説明や窓口機能等の整備、開示の求めを受け付ける方法を定める場合等に当たっては、障害のある患者・利用者等にも配慮する必要がある。

8．遺族への診療情報の提供の取扱い

法は、ＯＥＣＤ８原則の趣旨を踏まえ、生存する個人の情報を適用対象とし、個人情報の目的外利用や第三者提供に当たっては本人の同意を得ることを原則としており、死者の情報は原則として個人情報とならないことから、法及び本ガイドラインの対象とはならない。しかし、患者・利用者が死亡した際に、遺族から診療経過、診療情報や介護関係の諸記録について照会が行われた場合、医療・介護関係事業者は、患者・利用者本人の生前の意思、名誉等を十分に尊重しつつ、特段の配慮が求められる。このため、患者・利用者が死亡した際の遺族に対する診療情報の提供については、「診療情報の提供等に関する指針」（「診療情報の提供等に関する指針の策定について」（平成１５ 年９月１２日医政発第0912001 号））の９において定められている取扱いに従って、医療・介護関係事業者は、同指針の規定により遺族に対して診療情報・介護関係の記録の提供を行うものとする。

9．個人情報が研究に活用される場合の取扱い

近年の科学技術の高度化に伴い、研究において個人の診療情報等や要介護認定情報等を利用する場合が増加しているほか、患者・利用者への診療や介護と平行して研究が進められる場合もある。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本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おり、これに当たっては、医学研究分野の関連指針（別表５参照）とともに本ガイドラインの内容についても留意することが期待される。なお、治験及び市販後臨床試験における個人情報の取扱いについては、本ガイドラインのほか、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年厚生省令第２８号）等）の規定や、関係団体等が定める指針に従うものとする。また、医療機関等が企業から研究を受託して又は共同で実施する場合における個人情報の取扱いについては、本ガイドラインのほか、別表５に掲げる指針や、関係団体等が定める指針に従うものとする。

10. 遺伝情報を診療に活用する場合の取扱い

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６参照）、別表５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、医療機関等が、遺伝学的検査を行う場合には、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を実施するなど、本人及び家族等の心理社会的支援を行う必要がある。

11. 他の法令等との関係

医療・介護関係事業者は、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、介護保険法等）の規定を遵守しなければならない。また、病院等の管理者の監督義務（医療法第１５条）や業務委託（医療法第１５条の２等）に係る規定、介護関係事業者における個人情報保護に係る規定等を遵守しなければならない。また、医療分野については、すでに「診療情報の提供等に関する指針」が定められている。これは、インフォームド・コンセントの理念等を踏まえ、医療従事者等が診療情報を積極的に提供することにより、医療従事者と患者等とのより良い信頼関係を構築することを目的としており、この目的のため、患者等からの求めにより個人情報である診療情報を開示する場合は、同指針の内容に従うものとする。

12. 認定個人情報保護団体における取組

法第３７条においては、個人情報取扱事業者の個人情報の適正な取扱いの確保を目的とする業務を行う法人等は主務大臣の認定を受けて認定個人情報保護団体となることができることとされている。認定個人情報保護団体となる医療・介護関係の団体等は、傘下の医療・介護関係事業者を対象に、個人情報保護に係る普及・啓発を推進するほか、法の趣旨に沿った指針等を自主的なルールとして定めたり、個人情報の取扱いに関する患者・利用者等のための相談窓口を開設するなど、積極的な取組を行うことが期待されている。

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。また、例えば診療録には、患者について客観的な検査をしたデータもあれば、それに対して医師が行った判断や評価も書かれている。これら全体が患者個人に関する情報に当たるものであるが、あわせて、当該診療録を作成した医師の側からみると、自分が行った判断や評価を書いているものであるので、医師個人に関する情報とも言うことができる。したがって、診療

録等に記載されている情報の中には、患者と医師等双方の個人情報という二面性を持っている部分もあることに留意が必要である。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、医療・介護関係事業者が保有する医療・介護関係個人情報を対象とするものであり、診療録等の形態に整理されていない場合でも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。（医療・介護関係法令において医療・介護関係事業者に作成・保存が義務づけられている記録例は別表１参照）

○医療機関等における個人情報の例診療録、処方せん、手術記録、助産録、看護記録、検査所見記録、エックス線写真、紹介状、退院した患者に係る入院期間中の診療経過の要約、調剤録等

○介護関係事業者における個人情報の例ケアプラン、介護サービス提供にかかる計画、提供したサービス内容等の記録、事故の状況等の記録等

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。顔写真については、一般的には目の部分にマスキングすることで特定の個人を識別できないと考えられる。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、事業者内で医療・介護関係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患者・利用者等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り、あわせて、本人の同意を得るなどの対応も考慮する必要がある。また、特定の患者・利用者の症例や事例を学会で発表したり、学会誌で報告したりする場合等は、氏名、生年月日、住所等を消去することで匿名化されると考えられるが、症例や事例により十分な匿名化が困難な場合は、本人の同意を得なければならない。なお、当該発表等が研究の一環として行われる場合にはＩ９．に示す取扱いによるものとする。

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。診療録等の診療記録や介護関係記録については、媒体の如何にかかわらず個人データに該当する。また、検査等の目的で、患者から血液等の検体を採取した場合、それら

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）等の対象となることから、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り扱ってはならない。また、これらの検査結果については、診療録等と同様に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、第三者提供（Ⅲ５．参照）や開示（Ⅲ７．参照）の対象となる。

４．本人の同意

法は、個人情報の目的外利用や個人データの第三者提供の場合には、原則として本人の同意を得ることを求めている。これは、法の基本となるＯＥＣＤ８原則のうち、利用制限の原則の考え方の現れであるが、医療機関等については、患者に適切な医療サービスを提供する目的のために、当該医療機関等において、通常必要と考えられる個人情報の利用範囲を施設内への掲示（院内掲示）により明らかにしておき、患者側から特段明確な反対・留保の意思表示がない場合には、これらの範囲内での個人情報の利用について同意が得られているものと考えられる。（Ⅲ５．（３）（４）参照）また、患者・利用者が、意識不明ではないものの、本人の意思を明確に確認できない状態の場合については、意識の回復にあわせて、速やかに本人への説明を行い本人の同意を得るものとする。なお、これらの場合において患者・利用者の理解力、判断力などに応じて、可能な限り患者・利用者本人に通知し、同意を得るよう努めることが重要である。

５．家族等への病状説明

法においては、個人データを第三者提供する場合には、あらかじめ本人の同意を得ることを原則としている。一方、病態によっては、治療等を進めるに当たり、本人だけでなく家族等の同意を得る必要がある場合もある。家族等への病状説明については、「患者（利用者）への医療（介護）の提供に必要な利用目的（Ⅲ１．（１）参照）と考えられるが、本人以外の者に病状説明を行う場合は、本人に対し、あらかじめ病状説明を行う家族等の対象者を確認し、同意を得ることが望ましい。この際、本人から申出がある場合には、治療の実施等に支障の生じない範囲において、現実に患者（利用者）の世話をしている親族及びこれに準ずる者を説明を行う対象に加えたり、家族の特定の人を限定するなどの取扱いとすることができる。一方、意識不明の患者の病状や重度の認知症の高齢者の状況を家族等に説明する場合は、本人の同意を得ずに第三者提供できる場合と考えられる（Ⅲ５．（２）②参照）。この場合、医療・介護関係事業者において、本人の家族等であることを確認した上で、治療等を行うに当たり必要な範囲で、情報提供を行うとともに、本人の過去の病歴、治療歴等について情報の取得を行う。本人の意識が回復した際には、速やかに、提供及び取得した個人情報の内容とその相手について本人に説明するとともに、本人からの申出があった場合、取得した個人情報の内容の訂正等、病状の説明を行う家族等の対象者の変更等を行う。なお、患者の判断能力に疑義がある場合は、意識不明の患者と同様の対応を行うとともに、判断能力の回復にあわせて、速やかに本人への説明を行い本人の同意を得るものとする。

Ⅲ 医療・介護関係事業者の義務等

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

医療・介護関係事業者が医療・介護サービスを希望する患者・利用者から個人情報を取得する場合、当該個人情報を患者・利用者に対する医療・介護サービスの提供、医療・介護保険事務、入退院等の病棟管理などで利用することは患者・利用者にとって明らかと考えられる。これら以外で個人情報を利用する場合は、患者・利用者にとって必ずしも明らかな利用目的とはいえない。この場合は、個人情報を取得するに当たって明確に当該利用目的の公表等の措置が講じられなければならない。（Ⅲ２．参照）医療・介護関係事業者の通常の業務で想定される利用目的は別表２に例示されるものであり、医療・介護関係事業者は、これらを参考として、自らの業務に照らして通常必要とされるものを特定して公表（院内掲示等）しなければならない。（Ⅲ２．参照）また、別表２に掲げる利用目的の範囲については、法第１５条第２項に定める利用目的の変更を行うことができると考えられる。ただし、変更された利用目的については、本人へ通知又は公表しなければならない。（Ⅲ２．参照）

（2）利用目的による制限の例外

医療・介護関係事業者は、あらかじめ本人の同意を得ないで法第１５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が（法第１６条第１項）、同条第３項に掲げる場合については、本人の同意を得る必要はない。具体的な例としては以下のとおりである。

①法令に基づく場合

医療法に基づく立入検査、介護保険法に基づく不正受給者に係る市町村への通知、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り、医療・介護関係事業者の通常の業務で想定される主な事例は別表３のとおりである。根拠となる法令の規定としては、一般に刑事訴訟法第２１８条（令状による捜査）、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）等が考えられる。これらの法令は強制力を伴って回答が義務づけられるため、医療・介護関係事業者は捜査等が行われた場合、回答する義務が生じる。また、刑事訴訟法第１９７条第２項（捜査に必要な取調べ）等については、法の例外規定の対象であるが、当該法令において任意協力とされており、医療・介護関係事業者は取調べ等が行われた場合、回答するか否かについて個別の事例ごとに判断する必要

がある。この場合、本人の同意を得ずに個人情報の提供を行ったとしても、法第１６条違反とはならないが、場合によっては、当該本人からの民法に基づく損害賠償請求等を求められるおそれがある。

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

(例)・意識不明で身元不明の患者について、関係機関へ照会する場合・意識不明の患者の病状や重度の認知症の高齢者の状況を家族等に説明する場合

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等】

・医療・介護関係事業者は、個人情報を取り扱うに当たって、その利用目的をできる限り特定しなければならない。

・医療・介護関係事業者は、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。・医療・介護関係事業者は、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(同意を得るために患者・利用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。

・医療・介護関係事業者は、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。

(利用目的を変更する場合の取扱いについてはⅢ２．を参照)

【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。

・患者が未成年者等の場合、法定代理人等の同意を得ることで足りるが、一定の判断能力を有す

る未成年者等については、法定代理人等の同意にあわせて本人の同意を得る。
・意識不明の患者や重度の認知症の高齢者などで法定代理人がいない場合で、緊急に診療が必要な場合については、上記（２）②に該当し、当該本人の個人情報を取り扱うことができる。

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】

・医療・介護関係事業者は、個人情報を取得するに当たって、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、院内や事業所内等に掲示するとともに、可能な場合には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。
・医療・介護関係事業者は、受付で患者に保険証を提出してもらう場合や問診票の記入を求める場合など、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、その利用目的を院内掲示等により明示しなければならない。ただし、救急の患者で緊急の処置が必要な場合等は、この限りでない。
・医療・介護関係事業者は、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。
・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など利用目的の通知等の例外に該当する場合は、上記内容は適用しない。（「利用目的が明らか」な場合についてはⅢ１．（１）を参照）

【その他の事項】

・利用目的が、本規定の例外である「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」に該当する場合であっても、患者・利用者等に利用目的をわかりやすく示す観点から、利用目的の公表に当たっては、当該利用目的についても併せて記載する。
・院内や事業所内等への掲示に当たっては、受付の近くに当該内容を説明した表示を行い、初回の患者・利用者等に対しては、受付時や利用開始時において当該掲示についての注意を促す。
・初診時や入院・入所時等における説明だけでは、個人情報について十分な理解ができない患者・利用者も想定されることから、患者・利用者が落ち着いた時期に改めて説明を行ったり、診療計画書、療養生活の手引き、訪問介護計画等のサービス提供に係る計画等に個人情報に関する取扱いを記載するなど、患者・利用者が個人情報の利用目的を理解できるよう配慮する。
・患者・利用者等の希望がある場合、詳細の説明や当該内容を記載した書面の交付を行う。

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】

・医療・介護関係事業者は、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。
・診療等のために必要な過去の受診歴等については、真に必要な範囲について、本人から直接取得するほか、第三者提供について本人の同意を得た者（Ⅲ５．（３）により本人の黙示の同意が得られていると考えられる者を含む）から取得することを原則とする。ただし、本人以外の家族等から取得することが診療上又は適切な介護サービスの提供上やむを得ない場合はこの限りでない。
・親の同意なく、十分な判断能力を有していない子どもから家族の個人情報を取得してはならない。ただし、当該子どもの診療上、家族等の個人情報の取得が必要な場合で、当該家族等から個人情報を取得することが困難な場合はこの限りではない。
・医療・介護関係事業者は、適正な医療・介護サービスを提供する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】

・第三者提供により他の医療・介護関係事業者から個人情報を取得したとき、当該個人情報の内容に疑義が生じた場合には、記載内容の事実に関して本人又は情報の提供を行った者に確認をとる。
・医療・介護関係事業者は、個人データの内容の正確性、最新性を確保するため、Ⅲ４．（２）②に示す委員会等において、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）医療・介護関係事業者が講ずるべき安全管理措置

①安全管理措置

医療・介護関係事業者は、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、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

医療・介護関係事業者は、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、医療資格者のみならず、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、雇用関係のある者のみならず、理事、派遣労働者等も含むものである。医療法第１５条では、病院等の管理者は、その病院等に勤務する医師等の従業者の監督義務が課せられている。（薬局や介護関係事業者についても、薬事法や介護保険法に基づく「指定居宅サービス等の事業の人員、設備及び運営に関する基準」、「指定居宅介護支援等の事業の人員及び運営に関する基準」、「指定介護老人福祉施設の人員、設備及び運営に関する基準」、「介護老人保健施設の人員、施設及び設備並びに運営に関する基準」及び「指定介護療養型医療施設の人員、設備及び運営に関する基準」（以下「指定基準」という。）等に同様の規定あり。）

（２）安全管理措置として考えられる事項

医療・介護関係事業者は、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を参考に、必要な措置を行うものとする。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

・医療・介護関係事業者は、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、苦情への対応を行う体制も含めて、院内や事業所内等への掲示やホームページへの掲載を行うなど、患者・利用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、具体的な取組を進めるため、医療における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。

・医療・介護関係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

・１）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。（Ⅲ１０．参照）

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、医師等の医療資格者や介護サービスの従業者については、刑法、関係資格法又は介護保険法に基づく指定基準により守秘義務規定等が設けられており（別表４）、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）業務を委託する場合の取扱い

①委託先の監督

医療・介護関係事業者は、検査や診療報酬又は介護報酬の請求に係る事務等個人データの取扱い

の全部又は一部を委託する場合、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である事業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、業務が再委託された場合で、再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・介護関係事業者や再委託した事業者が責めを負うこともあり得る。

②業務を委託する場合の留意事項

医療・介護関係事業者は、個人データの取扱いの全部又は一部を委託する場合、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委託することを予定している場合は、再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（患者・利用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

＊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）医療情報システムの導入及びそれに伴う情報の外部保存を行う場合の取扱い

医療機関等において、医療情報システムを導入したり、診療情報の外部保存を行う場合には、厚生労働省が別途定める指針によることとし、各医療機関等において運営及び委託等の取扱いについて安全性が確保されるよう規程を定め、実施するものとする。

（５）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。

（６）その他

受付での呼び出しや、病室における患者の名札の掲示などについては、患者の取り違え防止など業務を適切に実施する上で必要と考えられるが、医療におけるプライバシー保護の重要性にかんがみ、患者の希望に応じて一定の配慮をすることが望ましい。

【法の規定により遵守すべき事項等】

・医療・介護関係事業者は、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。

・医療・介護関係事業者は、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。