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。）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。

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、苦情処理体制も含めて、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定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、苦情処理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３）、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。

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。

－個人情報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）

－個人情報データに対するアクセス記録の保存

－個人情報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、元の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）電子カルテ等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、電子カルテ等を導入したり、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）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。
・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】
・医療・介護関係事業者は、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

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、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、次のような場合には、本人の同意を得る必要がある。

（例）

・民間保険会社からの照会
・職場からの照会
・学校からの照会

（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、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、医療機関等の通常の業務で想定される主な事例は別表2のとおりである。

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

（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痴呆性の高齢者の状況を家族に説明する場合

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
・児童虐待事例についての関係機関との情報交換

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

（3）本人の同意が得られていると考えられる場合

医療機関等については、第三者への情報の提供のうち、以下に掲げる場合については、黙示による同意が得られていると考えられる。

①患者への医療の提供のために通常必要な範囲の利用目的について、院内掲示等で公表しておくことによりあらかじめ包括的な同意を得る場合

医療機関の受付等で、診療を希望する患者から個人情報を取得した場合、それらが患者自身の医療サービスの提供のために利用されることは明らかである。このため、院内掲示等により公表して、患者に提供する医療サービスに関する利用目的について患者から明示的に留保の意思表示がなければ、患者の黙示による同意があったものと考えられる。（Ⅲ２．参照）

また、

(ｱ)患者への医療の提供のため、他の医療機関等との連携を図ること

(ｲ)患者への医療の提供のため、外部の医師等の意見・助言を求めること

(ｳ)患者への医療の提供のため、他の医療機関等からの照会があった場合にこれに応じること

(ｴ)患者への医療の提供に際して、家族等への病状の説明を行うこと

等が利用目的として特定されている場合は、これらについても患者の同意があったものと考えられる。

②この場合であっても、黙示の同意があったと考えられる範囲は、患者のための医療サービスの提供に必要な利用の範囲であり、別表１の「患者への医療の提供に必要な利用目的」に示された利用目的に限られるものとする。

なお、院内掲示等においては、

(ｱ)患者は、医療機関が示す利用目的の中で同意しがたいものがある場合には、その事項について、あらかじめ本人の明確な同意を得るよう医療機関に求めることができること。

(ｲ)患者が、(ｱ)の意思表示を行わない場合は、公表された利用目的について患者の同意が得られたものとすること。

(ｳ)同意及び留保は、その後、患者からの申出により、いつでも変更することが可能であること。

をあわせて掲示するものとする。

※上記①の(ｱ)～(ｴ)の具体例

（事例１）他の医療機関宛に発行した紹介状等を本人が持参する場合

医療機関等において他の医療機関等への紹介状、処方せん等を発行し、当該書面を本人が他の医療機関等に持参した場合、当該第三者提供については、本人の同意があったものと考えられ、当該書面の内容に関し、医療機関等との間での情報交換を行うことについて同意が得られたものと考えられる。

例えば、薬局の薬剤師が、処方せんの内容に疑義が生じたため、処方せんを交付した医師に照会を行う場合がこれに該当する。

（事例２）他の医療機関等からの照会に回答する場合

診療所Ａを過去に受診したことのある患者が、病院Ｂにおいて現に受診中の場合で、病院Ｂから診療所Ａに対し過去の診察結果等について照会があった場合、病院Ｂの担当医師等が受診中の患者から同意を得ていることが確認できれば、診療所Ａ

は自らが保有する診療情報の病院Ｂへの提供について、患者の同意が得られたものと考えられる。

（事例３）家族等への説明

病態等について、本人と家族に対し同時に説明を行う場合には、明示的に本人の同意を得なくても、家族等に対する診療情報の提供について、本人の同意が得られたものと考えられる。

③医療機関等が、労働安全衛生法第６６条、健康保険法第１５０条、国民健康保険法第８２条又は老人保健法第２０条により、事業者、保険者又は市町村が行う健康診断等を受託した場合、その結果である労働者等の個人データを当該事業者等に対して提供することについて、本人の同意が得られていると考えられる。

④介護関係事業者については、介護保険法に基づく指定基準において、サービス担当者会議等で利用者の個人情報を用いる場合には利用者の同意を、利用者の家族の個人情報を用いる場合には家族の同意を、あらかじめ文書により得ておかなければならないとされていることを踏まえ、事業所内への掲示によるのではなく、サービス利用開始時に適切に利用者から文書により同意を得ておくことが必要である。

（４）「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。医療・介護関係事業者における具体的事例は以下のとおりである。

・検査等の業務を委託する場合
・外部監査機関への情報提供（（財）日本医療機能評価機構が行う病院機能評価等）
・個人データを特定の者との間で共同して利用するとして、あらかじめ本人に通知等している場合

※個人データの共同での利用における留意事項

病院と訪問看護ステーションが共同で医療サービスを提供している場合など、あらかじめ個人データを特定の者との間で共同して利用することが予定されている場合、(ｱ)共同して利用される個人データの項目、(ｲ)共同利用者の範囲（個別列挙されているか、本人から見てその範囲が明確となるように特定されている必要がある）、(ｳ)利用する者の利用目的、(ｴ)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、をあらかじめ本人に通知し、又は本人が容易に知り得る状態においておくとともに、共同して利用することを明らかにしている場合には、当該共同利用者は第三者に該当しない。

この場合、(ｱ)、(ｲ)については変更することができず、(ｳ)、(ｴ)については、本人が想定することが困難でない範囲内で変更することができ、変更後、本人

に通知又は本人の容易に知り得る状態におかなければならない。

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。医療・介護関係事業者における具体的事例は以下のとおりである。

・病院内の他の診療科との連携など当該医療・介護関係事業者内部における情報の交換
・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（特定し、公表した利用目的との関係で、目的外利用として所要の措置を行う必要があり得る）
・当該事業者内で経営分析を行うための情報の交換

このうち、医療・介護関係事業者内部の研修でカルテや介護関係記録等を利用する場合には、具体的な利用方法を含め、あらためて本人の同意を得るか、個人が特定されないよう匿名化する。

（5）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

第三者提供を行う場合のほか、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。

（適切ではない例）

・医師及び薬剤師が製薬企業のMR（医薬品情報担当者）、医薬品卸業者のMS（医薬品販売担当者）等との間で医薬品の投薬効果などについて情報交換を行う場合に、必要でない氏名等の情報を削除せずに提供すること。

【法の規定により遵守すべき事項等】

・医療・介護関係事業者においては、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。なお、医療機関等については、（2）の本人の同意を得る必要がない場合に該当する場合には、本人の同意を得る必要はない。

【その他の事項】

・第三者提供に該当しない情報提供が行われる場合であっても、院内や事業所内等への掲示、ホームページ等により情報提供先をできるだけ明らかにするとともに、患者等からの問い合わせがあった場合に回答できる体制を確保する。

・例えば、業務委託の場合、当該医療・介護関係事業者において委託している業務の内容、委託先事業者、委託先事業者との間での個人情報の取扱いに関する取り決めの内容等について公開することが考えられる。
・個人情報の第三者提供について本人の同意があった場合で、その後、本人から第三者提供の範囲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、本人の同意のあった範囲に限定して取り扱うものとする。