個人情報保護に関する規程・細則等

〔目　　次〕

令和８年２月 13 日現在

公益社団法人日本医業経営コンサルタント協会

個人情報保護規程

第１章　本規程の目的

（目的）

第１条　公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）が自らの事業の用に供する個人情報について、本協会の事業や業務における個人情報の取扱いの各局面（取得、利用、委託、第三者提供、保管・バックアップ、消去・廃棄など）における①個人情報の漏えい、滅失又は毀損、②関連する法令・国が定める指針その他の規範に対する違反、③想定される経済的な不利益及び社会的な信用の失墜、④本人の権利利益の侵害など、種々の個人情報保護リスクを適切にマネジメントすると共に、最小化することを目的とする。

第２章　定義

（定義）

第２条　本規程において、次の各項に掲げる用語の定義は、当該各項に定めるところによる。

１　個人情報とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

（１）　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（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をいう。 次項第２号において同じ。）で 作られる記録をいう。 以下同じ 。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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。)

（２）　個人識別符号が含まれるもの

２　個人識別符号とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、個人情報の保護に関する法律施行令（以下「政令」という 。） 第１条で定めるものをいう。

（１）　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

（２）　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

３　要配慮個人情報とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、 偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令第２条で定める記述等が含まれる個人情報をいう。

４　個人情報データベース等とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除

く）をいう。

（1） 特定の個人情報を電子計算機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もの

（2） 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

5　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。

6　保有個人データとは、本協会が、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利を有する個人データであって、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として政令で定めるもの以外のものをいう。

7　本人とは、個人情報によって識別される特定の個人をいう。

8　個人情報保護管理者とは、本規程の構築及び維持・管理に関する責任及び権限を持つ者をいう。

9　個人情報保護部門管理者とは、各支部における本規程の維持・管理に関する責任及び権限を持つ者をいう。

10　個人情報取扱担当者とは、個人情報のコンピュータへの入力・出力、台帳・申込書等の個人情報を記載した書類を保管・管理する責任及び権限を持つ者をいう。

11　担当者とは、日常の業務で個人情報及び個人データを取り扱う担当者をいう。

12　監査責任者とは、公平かつ客観的な立場にあり、監査の実施及び報告を行う責任及び権限を持つ者をいう。

13　本人の同意とは、本人の個人情報が、本協会によって示された取扱方法で取扱われることを承諾する旨の当該本人の意思表示をいう。

14　提供とは、個人データ、保有個人データを、自己以外の者が利用可能な状態に置くことをいう。

15　委託とは、契約の形態・種類を問わず、本協会が他の者に個人データの全部又は一部の取扱いを行わせることをいう。

16　共同利用とは、特定の者との間で個人データを共同して利用する場合、次の各号の情報をあらかじめ本人に通知、又は本人が容易に知り得る状態に置いて、当該特定の者に個人データを提供し、利用することをいう。

① 共同利用をする旨

② 共同して利用される個人データの項目

③ 共同して利用する者の範囲

④ 利用する者の利用目的

⑤ 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及び住所並びに法人にあっては、その代表者の氏名

17　役員等とは、会長、副会長、専務理事、理事、監事をいい、常勤、非常勤を問わない。

18　職員等とは、職員、契約社員、アルバイト等を含めた本協会の業務に従事する者をいう。

19　従業者とは、役員等及び職員等をいう。

20　漏えいとは、個人データが外部に流出することをいう。

21　滅失とは、個人データの内容が失われることをいう。
22　毀損とは、個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となることをいう。

第３章　本規程の適用範囲

（適用範囲）

第３条　本協会が事業の用に供するすべての個人情報について適用する。
２　本規定は、個人情報を取扱う従業者すべてに適用する。

第４章　個人情報の利用目的に関する措置

（利用目的の特定）

第４条　本協会は、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。）をできる限り特定する。
２　協会は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲内で行なうものとする。

（利用目的による制限）

第５条　本協会は、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、個人情報を取り扱わないものとする。
２　前項の規定は、次に掲げる場合については、適用しない。
（１）　法令に基づく場合
（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
（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　本協会は、違法又は不当な行為を助長し、又は誘発するおそれがある方法による個人情報の利用は行わない。

第５章　個人情報の取得に関する措置

（取得方法の制限）

第６条　本協会は、適法かつ公正な手段によって個人情報の取得を行うものとする。
２　本協会は、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、要配慮個人情報を取得しない。
（１）　法令に基づく場合
（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
（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
（５） 当該要配慮個人情報が、本人、国の機関、地方公共団体、放送機関、新聞社、通信社その他の報道機関、大学その他の学術研究を目的とする機関等、宗教団体、政治団体 、その他著述を業として行う者、個人情報の保護に関する法律施行規則（以下「個人情報保護委員会規則」という。） で定める者（外国政府等）により公開されている場合
（６） 本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合
（７） 委託、事業承継又は共同利用に伴って個人データの提供を受ける場合おいて、個人データである要配慮個人情報の提供を受けるとき

（取得に際しての利用目的の通知等）

第７条　本協会は、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、又は公表する。

２　本協会は、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（電磁的記録を含む。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する。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　本協会は、利用目的を変更した場合には、変更された利用目的について、本人に通知、又は公表する。

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。

（１） 利用目的を本人に通知、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
（２） 利用目的を本人に通知し、又は公表することにより本協会の権利又は正当な利益を害するおそれがある場合
（３） 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
（４） 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

第６章　データの安全・適正な管理

（データ内容の正確性の確保等）

第８条　本協会は、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とともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めるものとする。

（データの安全性の確保）

第９条　本協会は、その取り扱う個人データの漏えい、滅失又は毀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ずるものとする。

２　本協会は、前項に規定する必要かつ適切な措置に関して、「情報システム管理規程」、「個人情報の安全管理に関する取扱細則」、「個人データ取扱マニュアル」に定め、適用する。

（従業者の監督）

第 10 条　本協会は、個人情報の取得、利用、提供、保管又は廃棄に従事する従業者に個人データを取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、当該従業者に対し必要かつ適切な監督を行うものとする。

２　従業者は、法令の規定又は本規程若しくは個人情報保護管理者又は個人情報保護部門管理者が指示した事項に従い、個人情報の秘密の保持に十分な注意を払いつつその業務を行うものとする。

３　従業者が従業者でなくなった場合、従事している間に取得した個人情報は、上位の従業者の指示に従って返却、廃棄等の処理を行なうものとする。

（委託先の監督）

第 11 条　本協会は、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うものとする。

２　前項に係る監督は、「個人情報取扱いの外部委託細則」の規定に従い行うものとする。

第７章　個人データの提供に関する措置

（第三者提供の制限）

第 12 条　本協会は、次に掲げる場合に限り、個人データを第三者に提供する。

（１）　あらかじめ本人の同意を得た場合

（２）　法令に基づく場合

（３）　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

（４）　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

（５）　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

（６）　本協会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ことに伴って当該個人データが提供される場合

（７）　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

（８）　特定の者との間で共同利用される個人データが当該特定の者に提供される場合

2　前項第１号において、あらかじめ得た同意の範囲を超えて個人データの提供を行う場合、本人に対して書面又はこれに代わる方法により、事前に通知し、本人より同意を得た後に提供を行うものとする 。

（共同利用）

第 13 条　本協会は、特定の者との間で共同して利用される個人データを特定の者に提供する場合には、共同利用する旨並びに共同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並びに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、住所並びに会長名について、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くものとする。

2　前項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又は名称、住所並びに会長名を変更するときは遅滞なく、共同して利用する者の利用目的又は当該責任を有する者を変更しようとするときはあらかじめ、変更する内容について、本人に通知し、又は本人が容易に知り得る状態に置くものとする。

（第三者提供に係る記録）

第 14 条　本協会は、個人データを第三者（国の機関、地方公共団体、独立行政法人等、地方独立行政法人を除く。）に提供したときは、次に掲げる事項に関する記録を作成する。ただし、当該個人データの提供が第 12 条第１項第２号から第８号のいずれかに該当する場合は、この限りでない。

（１）　当該個人データを提供した年月日

（２）　本人より第三者提供の同意を得ている旨

（３）　当該第三者の氏名又は名称及び住所並びに法人にあっては代表者の氏名

（４）　当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項

（５）　当該個人データの項目

2　前項の記録は、個人データを第三者に提供した都度、速やかに作成するものとする。ただし、当該第三者に対し個人データを継続的若しくは反復して提供したとき、又は当該第三者に対し個人データを継続的に若しくは反復して提供することが確実であると見込まれるときの記録は、一括して作成することも可能とする。

3　本協会は、前項の記録を、当該記録を作成した日から３年間保存するものとする。

（第三者提供を受ける際の確認等）

第 15 条　本協会は、第三者から個人データの提供を受けるに際しては、次に掲げる事項の確認を行うものとする。ただし、当該個人データの提供が第 12 条第２号から第８号のいずれかに該当する場合は、この限りでない。

（１）　当該第三者の氏名又は名称及び住所並びに法人にあってはその代表者名

（２）　当該第三者による当該データの取得の経緯

2　前項の規定による確認を行ったときは、次に掲げる事項に関する記録を作成する。

（１） 当該個人データの提供を受けた年月日
（２） 当該本人の同意を得ている旨
（３） 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者名
（４） 当該第三者による当該個人データの取得の経緯
（５） 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
（６） 当該個人データの項目

３　前項の記録は、個人データを第三者から提供を受けた都度、速やかに作成するものとする。ただし、当該第三者から継続的に若しくは反復して個人データの提供を受けたとき、又は当該第三者から継続的に若しくは反復して個人データの提供を受けることが確実であると見込まれるときの記録は、一括して作成することも可能とする。

４　本協会は、前項の記録を、当該記録を作成した日から３年間保存するものとする。

第８章　本人関与の仕組み等

（保有個人データに関する事項の公表等）

第 16 条　本協会は、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。）に置くものとする。

（１） 本協会の名称及び住所並びに会長名
（２） 全ての保有個人データの利用目的
（３） 次項の規定による求め又は次条第１項、第 18 条第１項又は第 19 条第１項、第２項若しくは第３項の規定による請求に応じる手続（第 22 条第２項（手数料）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。）
（４） 保有個人データの安全管理のために講じた措置
（５） 保有個人データの取扱に関する苦情の申出先

２　本協会は、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、これを通知する。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。

（１） 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
（２） 第７条第４項第１号から第３号のいずれかに該当する場合

３　本協会は、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、その旨を通知する。

（個人情報の開示等）

第 17 条　本協会は、本人から、当該本人が識別される保有個人データの電磁的記録の提供による方法その他の個人情報保護委員会規則で定める方法により開示請求を受けたときは、本人に対し、当該本人が請求した方法（当該方法による開示に多額の費用を要する場合その他当該方法による開示が困難である場合にあっては、書面の交付による方法）により、遅滞なく、当該保有個人データの開示に応じるものとする。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、その全部若しくは一部について開示しないものとする。

（１） 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
（２） 本協会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
（３） 他の法令に違反することとなる場合

2　本協会は、前項の規定による請求に係る保有個人データの全部若しくは一部について開示しない旨の決定をしたとき、当該保有個人データが存在しないとき、又は同項の規定により本人が請求した方法による開示が困難であるときは、本人に対し、遅滞なく、その旨を通知する。

3　他の法令の規定により、本人に対し第１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また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、第１項の規定は、適用しない。

4　第１項から第２項までの規定は、当該本人が識別される個人データに係る第 14 条第１項及び第 15 条第２項の記録（その存否が明らかになる事により公益その他の利益が害されるものとして政令で定めるものを除く。第 21 条第２項において「第三者提供記録」という。）について準用する。

5　前各項に係る対応はすべて「個人情報の開示等に関する細則」第３章開示等対応手続きの規定に従い行うものとする。

（個人情報の訂正等）

第 18 条　本協会は、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の事由により、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。）の請求を受けた場合には、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きが定められている場合を除き、利用目的の達成の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うものとする。

2　本協会は、前項の規定による請求に係る保有個人データの内容の全部も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（訂正等を行ったきは、その内容を含む。）を通知する。

3　第１項及び第２項に係る対応はすべて「個人情報の開示等に関する細則」第３章開示等対応手続きの規定に従い行うものとする。

4　第１項の訂正等の請求のうち、本協会の事業に係る登録事項の訂正手続きについては、本協会が定める各種登録手続きによるものとする。

（利用停止等）

第 19 条　本協会は、本人から、当該本人が識別される保有個人データが第５条第１項若しくは第３項の規定に違反して取り扱われているとき、又は第６条の規定に違反して取得されたものであるとして、当該保有個人データの利用の停止または消去（以下この条において「利用停止等」という。）の請求を受けた場合であって、その請求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う。

2　本協会は、本人から、当該本人が識別される保有個人データが第 12 条第１項の規定に違反して第三者に提供されているとして、当該保有個人データの第三者提供の停止の請求を受け

た場合、その請求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提供を停止する。

3　本協会は、本人から、当該本人が識別される保有個人データを本協会が利用する必要がなくなったとして、又は当該本人が識別される保有個人データに係る第 24 条第１項に規定する事態が生じた場合、その他の当該本人が識別される保有個人データの取扱いにより当該本人の権利または正当な利益が害されるおそれがあるとして、当該保有個人テータの利用停止等又は第三者への提供の停止の請求を受けた場合であって、その請求に理由があることが判明したときは、本人の権利利益の侵害を防止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又は第三者への提供を停止する。

4　第１項から第３項について、当該保有個人データの利用停止等又は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利用停止等又は第三者への提供の停止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、適用しない 。

5　本協会は、第１項から第３項の規定による請求に係る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、又は第２項若しくは第３項の規定による請求に係る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、その旨を通知するものとする。

6　前第１項から第５項に係る対応は、すべて「個人情報の開示等に関する細則」第３章開示等対応手続きの規定に従い行うものとする。

（理由の説明）

第 20 条　本協会は、第 16 条第３項、第 17 条第２項、第 18 条第２項又は第 19 条第５項の規定により、本人から求められ、又は請求さ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には、本人に対し、その理由を説明するよう努めるものとする。

（開示等の請求等に応じる手続）

第 21 条　本協会は、第 16 条第２項による求め又は第 17 条第１項　（同条第４項において準用する場合を含む。次条第１項において同じ）、第 18 条第１項若しくは第 19 条第１項、第２項若しくは第３項の規定による請求（以下この条において「開示等の請求等」という。）は、「個人情報の開示等に関する細則」第４条の定めにより受け付ける。

2　本協会は、本人に対し、開示等の請求等に関し、その対象となる保有個人データ又は第三者提供記録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、本協会は、本人が容易かつ的確に開示等の請求等をすることができるよう、当該保有個人データ又は第三者提供記録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るものとする。

3　開示等の請求等は、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ものとする。

4　本協会は、前３項の規定に基づき開示等の請求等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するものとする。

（手数料）

第 22 条 本協会は、第 16 条第２項の規定による利用目的の通知を求められたとき又は第 17 条第１項の規定による開示の請求を受けたときは、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　本協会は、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る。

（苦情の処理）

第 23 条　本協会は、個人情報の取扱いに関する苦情が生じた場合には、適切かつ迅速に処理する。

2　本協会は、前項の目的を達成するために個人情報保護苦情・相談窓口を設置する。

第９章　個人データ事故報告・対応

（漏えい等の報告・対応）

第 24 条　本協会は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして「個人情報保護委員会規則」で定めるもの（以下「事故」という。）が生じたときは、「個人情報事故細則」で定めるところより、当該事態が生じた旨を個人情報保護委員会に報告するものとする。

2　本協会は、前項に規定する事故が生じたときは、本人に対し、「個人情報保護委員会規則」で定めるところにより、当該事故が生じた旨を通知するものとする。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するために必要なこれに代わるべき措置をとるときは除く。

3 第１項の事故に関して、個人情報保護委員会に報告を要しない事故の発生を確認した場合又は発生したと思料される場合には、これを知った者は、ただちに「個人情報事故細則」「別表１個人情報に関する事故情報連絡順序」に基づき直属の上司に報告するものとする。

4 前項の事故対応は、「個人情報事故細則」の規定に従い、速やかに対応を行うものとする。

第 10 章　組織及び実施責任

（個人情報保護管理者及び監査責任者の選任）

第 25 条　会長は、本規程の内容を理解し実践する能力のある者を本協会内から１名指名し、理事会の承認を得た上で個人情報保護管理者としての業務を行わせるものとする。

2　個人情報保護管理者は、本規程の内容を理解し公平かつ客観的立場にある者を本協会内から１名指名し、会長の承認を得た上で、監査責任者としての業務を行わせるものとする。

（個人情報保護管理者の責務）

第 26 条　個人情報保護管理者は、本規程に定められた事項を理解し、遵守するとともに、個人

情報の取得、利用、又は提供に従事する者にこれを理解させ、遵守させるための教育訓練、安全対策の実施並びに周知徹底等の措置を実施する責任を負うものとする。

2　個人情報保護管理者は、個人情報に関する教育訓練を実施するため個人情報の教育担当者を本協会内部から指名し、その責務を行わせるものとする。

3　個人情報保護管理者は、個人情報保護苦情・相談窓口を設置し、個人情報に関する苦情又は相談に対応させるものとする。

4　個人情報保護管理者は、個人情報保護に関する当該事業年度の教育計画、内部監査計画、規程類の見直し等の計画を取り纏めて理事会へ報告する責任を負うものとする。

5　個人情報保護管理者は、当該事業年度に実施した個人情報保護に関する教育、内部監査、規程類の見直し、監視・測定の結果等を取り纏めて理事会へ報告する責任を負うものとする。

（個人情報保護部門管理者の責務）

第 27 条　個人情報保護部門管理者は、支部長又は支部長によって指名された者とし、本規程に定められた事項を理解し、遵守するとともに、個人情報の取得、利用、又は提供に従事する者にこれを理解させ、かつ遵守させるため、安全対策の実施並びに周知徹底等の措置を実施する責任を負うものとする。

2　個人情報保護部門管理者は支部に所属する者の中から、必要な人数の個人情報取扱担当者を選任することができる。

3　個人情報保護部門管理者は、個人情報保護管理者又は監査責任者が行う業務に協力するものとする。

（個人情報の教育担当者の責務）

第 28 条　個人情報の教育担当者は、本規程に定められた事項を理解し、遵守するとともに、役員等及び職員等に本規程を遵守させるための教育訓練を企画・運営する責任を負うものとする。

（個人情報保護苦情・相談窓口の責務）

第 29 条　個人情報保護苦情・相談窓口（以下「窓口」という。）を担当する者は、本人からの個人情報に関する問い合わせ、相談又は苦情（以下「相談等」という。）に応じる。

2　窓口を担当する者は、相談等につき、法令、ガイドライン、本規程、その他の規則の内容、趣旨に沿って回答するとともに、必要に応じて本協会の担当部署に相談等を回付する。

3　窓口を担当する者は、個々の相談等につき相談記録を作成し、保管する。

4　窓口を公表する項目は以下のとおりとする。

（1）　住所

（2）　電話番号

（3）　窓口

（監査責任者の責務）

第 30 条　監査責任者は、本規程に定められた事項を理解し、遵守するとともに、定期的に本規

程が適切かつ有効に実施されているかを評価し、確認する責任を負うものとする。なお、本協会外の第三者に監査業務を委託することを妨げない。

第 11 章　教育

（教育の実施）

第 31 条　本協会は、個人データを取り扱う従業者に対し、その取扱う個人情報の質及び量に応じた必要な研修を行うものとする。

2　研修の内容及び日程は、事業年度毎に教育担当者が定める。

第 12 章　監査

（監査の実施）

第 32 条　監査責任者は、原則として年１回、「個人情報保護に関する監査基本計画書」（以下「基本計画書」という。）を策定の上、個人情報保護管理者に提出し、会長の承認を得なければならない。

2　基本計画書に記載された個別の監査については、「個人情報保護に関する監査個別計画書」（以下「個別計画書」という。）を作成するものとし、個別計画書は監査責任者の承認を得なければならない。

3　監査責任者は、個別計画書に従って監査を行い、「個人情報保護に関する監査報告書」（以下「監査報告書」という。）を作成し、個人情報保護管理者に提出し、会長に報告する。

4　監査報告書に改善勧告が含まれていた場合、会長又は個人情報保護管理者は被監査部門に対し「個人情報保護に関する改善計画書」（以下「改善計画書」という。）の提出を命じるものとする。

5　改善計画書の提出を求められた被監査部門は、改善計画書を作成して会長及び個人情報保護管理者の承認を受け、改善計画書に従って改善活動を行わなければならない。

6　監査責任者は、改善計画書の作成支援、改善活動の見直しを行うとともに、改善状況を会長及び個人情報保護管理者に報告する。

7　監査責任者は、会長又は個人情報保護管理者が必要と認めた場合、前各項に基づき、臨時監査を行うことができる。

第 13 章　罰則

（罰　則）

第 33 条　本規程に故意に違反した者、あるいは自らの職務を適正に遂行していれば違反を知り得たすべての役員等は、定款に基づく解任の対象となる。

2　本規程に故意に違反した者、あるいは自らの職務を適正に遂行していれば違反を知り得たすべての職員等は、就業規則に基づく解雇を含む懲戒の対象となる。

第 14 章　雑則

（適用除外）

第 34 条　本協会は、個人情報の保護に関する法律第 24 条　外国にある第三者への提供の制限、

第35条の２　仮名加工情報取扱事業者の義務及び第２節　匿名加工情報取扱事業者等の義務は何れも該当する取扱いがないことから適用しない。当該取扱いが生じた場合には、あらためて規定するものとする。

（細　則）

第35条　本規程の運用に必要な細則は別に定める。

（改　廃）

第36条　本規程の改廃は、理事会の承認を得なければならない。

（附　則）

本規程は、平成18年1月18日から適用する。

（附　則）

本規程は、令和４年４月１日から適用する。

（附　則）

本規程は、令和８年２月13日から適用する。

情報システム管理規程

第１章　総　則

（目的）

第１条　本規程は、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）における情報システムの適正な管理並びに効率的かつ円滑な運用を図るとともに、保有する個人データを適正に管理するため、これらの利用及び管理のあり方を定めることを目的とする。

（用語の定義）

第２条　本規程において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）　情報システム

業務の情報化・効率化を推進するために構築されたソフトウェア、データベース等のシステム及びネットワークに接続された情報処理機器並びにこれらに関連するマニュアル、作成・記録されたドキュメントを含めた総体をいう。

（２）　情報処理機器

ファイルサーバ、業務サーバ、クライアントパソコン、それらの周辺機器及びネットワークをいう。

（３）　データ

情報システムに入力された情報であって、情報処理に適するように形式化されたもの及び情報システムから記録媒体に保存又は出力されたものをいう。

（４）個人情報　　個人情報保護規程第２条第１項をいう。

（５）個人データ　　個人情報保護規程第２条第５項をいう。

（６）情報の安全性　情報の機密性、安全性及びコンピュータウィルス対策をいう。

（７）利用者　　本協会の情報システムを利用する者をいう。

第２章　情報システムの管理

（総括管理者）

第３条　本協会に情報システム総括管理者（以下「総括管理者」という。）を置く。

２　総括管理者は、事務局長とする。

３　総括管理者は、情報システムの効率的な運用及び適正な管理並びに安全性を確保するための運用の総括に当たるものとする。

４　総括管理者は、情報システムの利用者に対し、情報システムの利用を制限し、又は禁止することができる。

５　総括管理者は、情報システムの円滑な運用及び管理を図るため、必要があると認められるときは、情報システムの利用状況等を調査することができる。

６　総括管理者は、情報システムに他の情報システムを接続することができる。ただし、Application Service Provider(ASP)又はSoftware as a Service(SaaS)等外部のアプリケーションサービスを情報システムに接続する場合は、接続前に本協会の定める評価を行い、接

続の承認をしなければならない。
7　総括管理者は、情報システムに接続した他の情報システムを接続することを制限し、又は禁止することができる。
8　総括管理者は、第４項及び第７項の規定に基づき、必要に応じて制約事項を定めることができる。
9　総括管理者は、本規程に定める情報システム運用管理者（以下、「運用管理者」という。）が、情報システムの管理、情報システムの利用者の指導及び監督その他の職務を怠っていると認められるときは、その改善を命ずることができる。
10　総括管理者は、情報システムにおいて本協会が保有する情報資産に係る情報の安全性を確保するための具体的な実施手順を定め、運用管理者及び情報システムの利用者に対する周知徹底を図らなければならない。

（運用管理者）

第４条　本協会に運用管理者を置く。
2　運用管理者は、総務部長とする。
3　運用管理者は、総括管理者を補佐し、次に掲げる業務を行う。
（1）　情報システムの運用、管理、保全に関すること。
（2）　情報システムの利用に関する利用者への指導及び監督に関すること。
（3）　配備したソフトウェア及び情報処理機器の閲覧、貸出し並びに情報処理機器等の利用に必要な消耗品の管理に関すること。
（4）　利用者が管理する情報処理機器等において発生した障害及びコンピュータウィルス対策への対応に関すること。
（5）　利用者が管理するＰＣに標準的に搭載しているアプリケーション以外のアプリケーションをインストールする場合は審査、承認すること。
4　運用管理者は、本協会が保有する情報システムのデータの漏えい、滅失、毀損等を防止し、データの適正な管理を図らなければならない。
5　運用管理者は、その職務のうち、保守及び運用に係る一部を外部業者に委託することができる。
6　前項の規定により外部業者に委託する場合、運用管理者は総括管理者を経由して、理事会の承認を得なければならない。
7　前項の規定により外部業者に委託した場合、運用管理者はその外部業者を適切に管理しなければならない。

第３章　個人情報の管理

（個人情報の管理）

第５条　個人情報は、個人情報保護規程及び同規程に関連する細則等に基づき取扱わなければならない。
2　利用者は、個人情報が記録されたデータを情報システムに保有しようとするときは、あらかじめ、データの管理に必要な事項を定め、運用管理者に届け出なければならない。

3 前項の届出があった場合、運用管理者は個人情報保護規程第２条第８項に定める個人情報保護管理者又は第９項に定める個人情報保護部門管理者に通知しなければならない。
4 利用者は、個人情報の保護に関する関係法規及び個人情報保護規程並びに同規程に関連する細則等を遵守し、会員情報の適正な管理、漏えい等の防止に努めなければならない。

第４章　情報システムの運用

（運用時間）

第６条　情報処理機器のうち、特段の定めがない各種サーバは、無停止で運用するものとする。
２　前項の規定にかかわらず、運用管理者は、次に掲げるときは、情報システムの運用の一部又は全部を停止若しくは利用を制限することができる。
（１）　情報システムに障害が発生した場合
（２）　第４条第３項第１号の規定により、データの保全又は復元を行う場合
（３）　その他、情報システムの管理上の理由から、運用管理者が必要と認めた場合

（利用者）

第７条　運用管理者は、総括管理者の承認を受けた者以外の者に情報システムを利用させてはならない。
２　運用管理者は、利用者がその資格を喪失するときは、その旨を速やかに総括管理者に届け出なければならない。

（会員及び職員以外の利用）

第８条　運用管理者は、業務の処理等を行うため、会員及び職員以外の者に情報システムを利用させる必要があるときは、総括管理者の許可を得なければならない。
２　総括管理者は、前項の規定により運用管理者に許可を与えるときは、利用に関する条件を付することができる。

（利用の管理）

第９条　会員の個人情報等、情報セキュリティが必要なデータの参照（閲覧）及び更新は、総括管理者があらかじめ指定した者でないとできない。
２　運用管理者は、利用者に対し、利用者ＩＤ等を付与するものとする。
３　利用者は、自己のパスワードについて、第三者に知られないように厳重に管理するとともに、必要に応じて変更する等の措置を講じなければならない。
４　利用者は、他者のパスワードを知ったときは、第三者に知らせてはならない。

（利用者の責務）

第 10 条　利用者は、情報システムの効率的かつ適正な利用、事故及び障害の回避並びにデータの漏えい、滅失及び毀損等の防止に努めるとともに、業務等に関連しない利用及び社会常識に反する利用を行ってはならない。
２　利用者は、個人を単位として設置された情報処理機器等を自らの責任で管理しなければな

らない。
3　利用者は、第３条第４項の規定に基づき総括管理者が定める制約事項並びにこれに基づく運用管理者の指示に従わなければならない。
4　利用者は、情報システムに異常を認めたときは、その旨を速やかに運用管理者に報告しなければならない。
5　利用者は、個人を単位として設置された情報処理機器等を外部へ持出して使用する必要が生じたときは、別に定める誓約書を添えて所属部課長を経由し、総括管理者の承認を得なければならない。支部においては、個人情報保護規程第２条第９項に定める個人情報保護部門管理者の承認をもって総括管理者の承認に代えることができる。
6　利用者は、その職務において、長期間若しくは連続的な持出しが必要なときは、総括管理者の許可を得なければならない。支部においては、個人情報保護規程第２条第９項に定める個人情報保護部門管理者の承認をもって総括管理者の承認に代えることができる。

（利用者ＩＤ等の付与等）

第 11 条　運用管理者は、新たに利用者となる会員及び職員並びに第８条第１項の規定により、総括管理者から情報システムの利用の承認を受けた者について、総括管理者に利用者ＩＤ等の付与を申請しなければならない。
2　運用管理者は、第９条第２項の規定に基づき利用者ごとに有効な利用者ＩＤ、電子メールアドレス及び仮パスワードを付与する。
3　運用管理者は、前項の規定に基づき、利用者に仮パスワードを付与した際には、当該利用者に対し、速やかに仮パスワードの変更を行うよう指示をしなければならない。
4 電子メールアドレスは利用者の氏名に基づき付与することとする。ただし、利用者が旧姓を日常生活において利用する等の理由により氏名の表記以外の電子メールアドレスを希望したときは、別の表記による電子メールアドレスの付与を運用管理者に申請する。
5　利用者は、婚姻等により氏名の表記が変更になったときは、運用管理者に氏名変更の届出を行わなければならない。
6　運用管理者は、第７条第２項の規定により、利用者でなくなった者に係る届出を受け取った場合は、該当する利用者ＩＤ等を速やかに失効しなければならない。
7　運用管理者は、個人を単位として設置された情報処理機器等を外部へ持出して使用する利用者に、生体認証の設定を指示しなければならない。

（利用者ＩＤ等の被付与者の責務）

第 12 条　前条第１項の規定により新たに利用者ＩＤ等を付与された利用者は、運用に関する規定の習得、情報セキュリティ及び個人情報の適正な管理に努めなければならない。

（特殊電子メールアドレス）

第 13 条　利用者は、業務上インターネットを介して、公に意見を求める場合等において、利用者の電子メールアドレスを公開することが適当ではないと判断したとき又は特定のグループ内で効率的に電子メールを回付するためにメーリングリスト化し、グルーピングするときは、

運用管理者に、利用期間を限定し、利用者の電子メールアドレスと異なる電子メールアドレス（この条においては「特殊電子メールアドレス」という。）を申請することができる。

2　運用管理者は、前項に規定する申請を承認したときは、速やかに特殊電子メールアドレスを発行しなければならない。

3　運用管理者は、第１項の規定により特殊電子メールアドレスの発行を許可するとき、条件を付すことができる。

（パスワードの管理）

第 14 条　利用者は、パスワードの厳重な管理を実施するため、次に掲げる措置を講じなければならない。

（１）　パスワードのメモ等の放置又はクライアントパソコンにパスワードを記憶してはならない。

（２）　パスワードの長さは６文字以上としなければならない。

（３）　利用者ＩＤ、氏名等第三者に容易に推察できる文字列をパスワードとして使用してはならない。

（４）　仮のパスワードは、最初の利用時に変更しなければならない。

2　利用者は、クライアントパソコンを外部へ持出して使用するときは、運用管理者の指示に従い、生体認証の設定を行わなければならない。

（利用者の異動）

第 15 条　利用者に異動等があった場合、その事務を担当する職員は異動状況等について、速やかに運用管理者に届出なければならない。

2　運用管理者は、前項に規定する届出を受け取ったときは、当該情報に基づいて、速やかに情報システムにおける利用者の設定の更新等必要な措置を講じなければならない。

（情報処理機器の移動）

第 16 条　利用者は、クライアントパソコンの台数を増設する必要が生じたときは、その旨を速やかに運用管理者に申請しなければならない。

2　利用者は、不要なクライアントパソコンが生じたときは、速やかに当該クライアントパソコンを運用管理者に返納しなければならない。

3　座席の配置の変更等の理由により、情報処理機器の移動等を行う必要が生じたときは、その旨を速やかに運用管理者に申請しなければならない。

（利用者の情報処理機器に関する義務）

第 17 条　利用者は、利用者個人に配備されたクライアントパソコン等については、自ら管理し、適切な利用を心がけなければならない。

2　利用者は、利用者個人に配備されたクライアントパソコンが第三者に使用又は許可なくデータの閲覧等が行われないよう、長時間、離席する際は、必要な措置を講じなければならない。

3　利用者は、利用者個人に配備されたクライアントパソコンに搭載されたソフトウェアの各種更新を適用し、最新版を使用しなければならない。

（禁止事項）

第 18 条　利用者は、情報システムの安全性を確保する等の理由により、次に掲げる行為を行ってはならない。

（1）　情報処理機器に搭載されているソフトウェアの複写、改変等の著作権の侵害及び使用許諾契約に違反する行為並びにその削除
（2）　利用者に認められていない権限による情報システムの利用
（3）　情報処理機器への他の通信回線の接続
（4）　情報処理機器へのハードウェアの接続及びソフトウェアの搭載
（5）　事務局に配備された情報処理機器以外からの情報システムの利用
（6）　情報処理機器への事務局から貸与されている電子記録媒体以外の接続

（利用の制限）

第 19 条　総括管理者は、利用者が本規程に違反したときは、当該利用者に対し、情報システムの利用の制限又は禁止若しくは利用者ＩＤの削除等の措置を講じなければならない。

第５章　緊急時における対応

（障害発生時の対応）

第 20 条　利用者は、情報システムに異常を認めたときは、直ちに運用管理者にその旨を報告しなければならない。

2　前項にいう異常には、コンピュータウィルスによる被害を含むものとする。

3　運用管理者は、第１項に規定する報告を受けたとき又は自ら情報システムに異常を認めたときは、その旨を速やかに総括管理者に報告し、必要な措置を講じなければならない。

4　利用者が故意又は過失により次に掲げる事項を発生させたときは、当該利用者は、その故意又は過失の程度に応じ、報告書等の提出及び修理又は弁償に要した費用を負担しなければならない。

（1）　第 17 条に違反した場合
（2）　外部から情報システムへ不正侵入された場合
（3）　情報システムに障害を発生させた場合
（4）　情報システムにコンピュータウィルスを侵入させた場合
（5）　情報処理機器を亡失若しくは破損させた場合
（6）　情報システムを利用し他の情報システムに障害等を発生させた場合

（不正侵入の防止）

第 21 条　運用管理者は、情報システムへの不正侵入を防止するため、必要な措置を講じなければならない。

（運用管理者が実施するコンピュータウィルス対策）

第 22 条　運用管理者は、コンピュータウィルスが情報システムに被害を与えないよう、また、二次感染しないよう注意するとともに、次に掲げる措置を講じなければならない。

（１）　情報システムのコンピュータに、セキュリティソフトウェアの導入を実施すること。

（２）　定期的又は必要に応じて随時、コンピュータウィルスに関する情報収集及び利用者に対して注意を喚起すること。

（３）　重要な情報システムの設定に係るファイルに対し、定期的にコンピュータウィルスの有無を確認すること。

（４）　情報システムにおけるコンピュータウィルスの被害の確認及び被害発生時における復旧その他必要な措置を講ずること。

（利用者が実施するコンピュータウィルス対策）

第 23 条　利用者は、コンピュータウィルスが情報システムに被害を与えないよう、また、二次感染しないよう注意するとともに、次に掲げる措置を講じなければならない。

（１）　取り外し可能な電子記録媒体及び情報システム以外から送信された電子メールに添付されたファイルを情報処理機器で開封するとき並びにインターネットを介し、外部からデータを情報処理機器に取り込むときのコンピュータウィルスの確認

（２）　情報システム以外に電子メールで送信する際、添付するファイルに対するコンピュータウィルスの確認

（３）　運用管理者が提供するコンピュータウィルス情報の確認

２　利用者は、差出人が不明又は不自然な電子メールを受信した際は、当該電子メールを速やかに削除しなければならない。

第６章　電子メールの利用

（電子メール）

第 24 条　利用者は、利用者個人の責任において電子メールの送信を行うものとし、業務に関連のない内容及び社会常識に反する内容の電子メールを送信してはならない。

２　利用者は、運用管理者が別に定めるファイルの容量を超える電子メールを送信してはならない。

３　利用者は、運用管理者の許可を得ずに利用者個人のプライベートアドレスに個人データが含まれるメールを送信、又は許可されていない外部のストレージにアップロードしてはならない。

第７章　個別システムとの接続等

（インターネットの利用等）

第 25 条　利用者は、情報システムを介してインターネットを利用することができる。

２　利用者は、前項の規定によりインターネットを利用して情報の収集・交換等を行うに当たっては、業務に関連のない利用及び社会常識に反する利用を行ってはならない。

３　運用管理者は、前項の規定に関し、情報システム上の機能において、一部のホームページ

の閲覧を制限することができる。
4　利用者は、前項の規定により閲覧を制限されたホームページについて、業務上閲覧が必要な場合は、運用管理者に申請を行わなければならない。
5　運用管理者は、前項の規定による申請を承認したときは、速やかに総括管理者に報告しなければならない。
6　運用管理者は、インターネットの利用等について、制約事項を定めることができる。

（個別システムの接続）

第 26 条　運用管理者は、利用者から情報処理機器へのハードウェアの接続又はソフトウェアの搭載若しくは情報システムに他の情報システムの接続（この条において「個別システムの接続等」という。）等の申請があったときは、情報システムの運用に影響を及ぼすことがないと判断した場合に限り個別システムの接続等を承認することができる。
2　運用管理者は、個別システムの接続等を許可するとき、条件を付すことができる。
3　個別システムの接続等を行った利用者は、当該接続したハードウェア及び搭載したソフトウェアの管理を行うものとする。
4　運用管理者は、個別システムとの接続等を行った利用者に当該個別情報システムの接続等について報告を求め、必要な指示を与えることができる。

第８章　その他

（補　足）

第 27 条　本規程に定めるもののほか、本規程の実施に関し必要な事項は、別に定める。

（改　廃）

第 28 条　本規程の改廃は、理事会の承認を得なければならない。

（附　則）

本規程は、平成 22 年２月１日から施行する。
本規程は、平成 24 年４月１日から施行する。
本規定は、平成 26 年４月１日から施行する。
本規定は、令和４年４月１日から施行する。

特定個人情報等取扱規程

第１章　総　則

（目的）

第１条　本規程は、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び個人情報保護委員会が定める「特定個人情報の取扱いに関するガイドライン（事業者編）」に基づき、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）の事務局職員等（職員、契約社員、アルバイト等を含めた本協会の業務に従事する者。以下同じ。）及び各支部の特定個人情報の事務取扱担当者が遵守すべき個人番号及び特定個人情報（以下「特定個人情報等」という。）の適正な取扱いの確保について、必要な事項を定めることを目的とする。

（定義）

第２条　本規程における特定個人情報等とは、個人番号（個人番号に対応し、その個人番号に代わって用いられる番号、記号、その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

（適用）

第３条　本規程は本協会の事務局職員等及び各支部の特定個人情報の事務取扱担当者に適用する。

２　本規程は、本協会が取り扱う特定個人情報等を対象とする。

（特定個人情報等基本方針）

第４条　本協会は、本協会における特定個人情報等の適正な取扱いを確保するため、次の事項を含む特定個人情報等の適正な取扱いに関する基本方針（以下、「基本方針」という。）を定める。

（１）　関係法令・ガイドライン等の遵守

（２）　利用目的

（３）　安全管理措置に関する対応

（４）　質問及び苦情処理等の窓口

２　本協会は、基本方針を、事務局職員等及び各支部の特定個人情報の事務取扱担当者に周知する。

第２章　利用制限

（取扱い事務の範囲）

第５条　本協会において個人番号等を取り扱う事務（以下「個人番号関係事務」という。）は、次に掲げる事務に限定する。

（１）　事務局職員等の所得税法等に係る税務関連の届け出事務

（２） 社会保険及び労働保険関連の届け出事務
（３） 報酬・料金等の支払調書作成事務
（４） 前各号のほか関係法令において特定個人情報等を利用することができる等と定められた事務
（５） 前各号の事務に付随して行う行政機関への届け出事務
２　本協会は、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、本人の同意があり、又は本人の同意を得ることが困難であるときは、保有している個人番号について、人の生命、身体又は財産を保護するために利用することができる。

（個人番号の利用）
第６条　本協会は、前条に規定する事務を処理するために必要な場合に限り、個人番号を利用するものとする。なお、前条第２項の場合を除き、たとえ本人の同意があったとしても、利用目的を超えて個人番号を利用してはならない。

（特定個人情報ファイルの作成の制限）
第７条　本協会は、第５条に規定する事務を処理するために必要な場合に限り、特定個人情報ファイルを作成するものとする。
２　特定個人情報ファイルには、パスワードを付与する等の保護措置を講じたうえで適切に保存する。

第３章　安全管理措置等

第１節　組織的安全管理措置

（事務取扱担当部門）
第８条　本協会は、次の部門ごとに特定個人情報等に関する事務を行うものとする。
（１） 本協会の事務局職員等及び第５条に関係する者（以下「関係者等」という。）に係る個人番号関係事務に関する事務部門
（２） 支部の関係者等に係る個人番号関係事務に関する事務部門

（特定個人情報保護責任者）
第９条　本協会は、特定個人情報等の取扱いに関して総括的な責任を有する特定個人情報保護責任者を設置するものとし、その責任者は事務局長とする。
２　特定個人情報保護責任者は、次の各号に掲げる事項その他事務局における特定個人情報等に関する全ての権限と責務を有する。
（１） 第４条に規定する基本方針の策定、事務局職員等への周知、一般への公表
（２） 本規程に基づき特定個人情報等の取扱いを管理する上で必要とされる事案の承認
（３） 特定個人情報等に関する安全対策の策定・推進
（４） 特定個人情報等の適正な取扱いの維持・推進等を目的とした諸施策の策定・実施
（５） 「個人情報保護委員会規則」で定めるところにより、特定個人情報等の漏えい、滅失又

は毀損（以下「漏えい等」という。）、及びその他の特定個人情報等の安全の確保に重大な事態（漏えい等を合わせ、以下「事故」という。）発生時の対応策・実施

（特定個人情報保護部門管理者）

第 10 条　本協会は、各支部の特定個人情報等の取扱に関して責任を有する特定個人情報保護部門管理者を設置するものとし、その責任者は各支部の個人情報保護部門管理者とする。

２　特定個人情報保護部門管理者は、次の各号に掲げる事項その他支部における特定個人情報等に関する全ての権限と責務を有する。

（１）　第４条に規定する基本方針及び本規程等の支部内への周知

（２）　支部における特定個人情報等の事務取扱担当者の監督

（３）　支部における特定個人情報等の管理状況に関する本部への報告

（４）　事故発生時の初期対応と特定個人情報保護責任者等への報告・相談

（事務取扱担当者）

第 11 条　本協会における特定個人情報等を取り扱う事務については、第８条に規定する部門ごとに事務取扱担当者を明確にするものとする。

２　事務取扱担当者は、次の各号に掲げる方法により特定個人情報等を取り扱う。

（１）　事務取扱担当部門ごとに取得した特定個人情報等を含む書類等（磁気媒体及び電子媒体（以下「磁気媒体等」という。）を含む。）は、当該部門において安全に管理する。

（２）　取得した特定個人情報等に基づき特定個人情報ファイルを作成する。

（３）　関係者等の特定個人情報等を取り扱う事務取扱担当者は、源泉徴収票又は支払調書等を作成し、行政機関等に提出するとともに、関係者等に交付する。

（４）　支部の関係者等の特定個人情報等を取り扱う事務取扱担当者は、支払調書等を作成し、行政機関等に提出するとともに、関係者等に交付する。

３　事務取扱担当者は、特定個人情報等を取り扱う情報システム及び機器等を適切に管理し、利用権限のない者には使用させてはならない。

４　事務取扱担当者は、特定個人情報等の取扱状況を明確にするため、執務記録を作成し、適宜記録する。

５　事務取扱担当者は、徹底した守秘義務の中で業務を遂行しなければならない。

（特定個人情報等の取扱状況の確認）

第 12 条　特定個人情報保護責任者は、本協会における特定個人情報等の取扱いが関係法令、本規程等に基づき適正に運用されていることを定期的に確認する。

２　特定個人情報保護責任者は、執務記録の内容を定期的に確認する。

（苦情等への対応）

第 13 条　本協会における特定個人情報等の取扱いに関する苦情等があったときは、これに適切に対応する。

2　特定個人情報保護責任者は、前項の目的を達成するために必要な体制の整備を行うものとする。

（体制の見直し）

第 14 条　本協会は、必要に応じて特定個人情報等の取扱いに関する安全対策に関する諸施策について見直しを行い、改善を図るものとする。

第２節　人的安全管理措置

（職員等の監督）

第 15 条　本協会は、事務局職員等が特定個人情報等を取り扱うに当たり、必要かつ適切な監督を行う。

（職員等の教育）

第 16 条　本協会は、事務局職員等に対して定期的な研修の実施又は情報提供等を行い、特定個人情報等の適正な取扱いを図るものとする。

第３節　物理的安全管理措置

（管理区域及び取扱区）

第 17 条　本協会は、漏えい等を防止するため、第８条に規定する部門ごとに特定個人情報ファイルを取り扱う情報システム（サーバ等）を管理する区域（以下、「管理区域」という。）、及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、事務取扱担当者以外の者が特定個人情報等を容易に閲覧等できないようにする。

2　管理区域とは、特定個人情報ファイルを取り扱う情報システム及び特定個人情報ファイルを管理するキャビネット等のある区域とし、他の区域との間仕切りの設置及びキャビネット等の施錠等の安全管理措置を講じることとする。

3　取扱区域とは、事務取扱担当者の机周辺とし、他の区域との間仕切りの設置及び座席配置等による安全管理措置を講じることとする。

（特定個人情報等の持出し等）

第 18 条　本協会において保有する特定個人情報等を持ち出すときは、次に掲げる方法により管理する。

（１）　特定個人情報等を含む書類を持ち出すときは、外部から容易に閲覧されないよう封筒に入れる等の措置を講じる。

（２）　特定個人情報等を含む書類を郵送等により発送するときは、簡易書留等の追跡可能な移送手段等を利用する。

（３）　特定個人情報ファイルを磁気媒体等又は機器にて持ち出すときは、ファイルへのパスワードの付与等又はパスワードを付与できる機器の利用等の措置を講じる。

2　特定個人情報等を事務局へ持ち帰る場合についても前項に準じた安全管理措置を講じる。

（特定個人情報等の削除及び廃棄）

第 19 条　本協会は、個人番号関係事務を行う必要がなくなった場合で、第 24 条第１項に規定する保管期間を経過した場合には、次の通り速やかに削除又は廃棄する。

（１）　特定個人情報等を含む書類は、焼却又は溶解等の復元不可能な手法により廃棄する。

（２）　特定個人情報ファイルは、完全削除ソフトウェア等により完全に消去する。

（３）　特定個人情報等を含む機器及び磁気媒体等は、破壊等により廃棄する。

（４）　特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合は、容易に復元できない手法により削除する。

（廃棄の記録）

第 20 条　本協会は、特定個人情報等を削除又は廃棄したときは、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。

第４節　技術的安全管理措置

（情報システムの管理）

第 21 条　本協会において使用する情報システムにおいて特定個人情報等を取り扱うときは、次に掲げる方法により管理する。

（１）　特定個人情報保護責任者及び特定個人情報保護部門管理者は、情報システムを使用して個人番号を取り扱う事務を処理するときは、ユーザーID に付与されるアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

（２）　事務取扱担当者は、情報システムを取り扱う上で、正当なアクセス権を有する者であることを確認するため、ユーザーID、パスワード等により認証する。

（３）　情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するため、情報システム及び機器にセキュリティ対策ソフトウェア等を導入する。

（４）　特定個人情報等をインターネット等により外部に送信するときは、通信経路における情報漏えい等を防止するため、通信経路の暗号化等の措置を講じる。

第４章　提供制限等

（個人番号の提供の要求の制限）

第 22 条　本協会は、第５条に規定する事務を処理するために必要がある場合に限り、本人又は他の個人番号関係事務実施者若しくは個人番号利用事務実施者（社会保障、税及び災害対策に関する特定の事務において保有している個人情報の検索、管理のために個人番号を利用して事務を処理する者で、主として、行政機関等。）に対して、利用目的を通知したうえで個人番号の提供を求めることができるものとする。

２　個人番号の提供を求める時期は、原則として個人番号を取り扱う事務が発生したときとす

る。

（特定個人情報等の提供）

第 23 条　本協会にて保有する特定個人情報等の提供は、第５条に規定する事務に限るものとする。

（保管）

第 24 条　本協会は、第５条に規定する事務が終了するまでの間、特定個人情報等を保管する。ただし、所管法令等により保存期間が定められているものについては、当該期間を経過するまでの間、特定個人情報等を保管する。

２　特定個人情報等を取り扱う機器、磁気媒体等及び書類等は、漏えい等の防止その他の安全管理の確保のため、次に掲げる方法により保管又は管理する。

（１）　特定個人情報等を取り扱う機器は、施錠できるキャビネット等に保管するか、又は盗難防止用のセキュリティワイヤー等により固定する。

（２）　特定個人情報等を含む書類及び磁気媒体等は、施錠できるキャビネット等に保管する。

（３）　特定個人情報ファイルは、パスワードを付与する等の保護措置を講じたうえでこれを保存し、当該パスワードを適切に管理する。

（４）　特定個人情報等を取り扱う磁気媒体等は、漏えい等を防止するために、事務取扱担当者が扱うパソコンやネットワーク上の共有フォルダ等に保存しないものとする。

（５）　特定個人情報等を含む書類であって、法定保存期間を有するものは、期間経過後速やかに廃棄することを念頭に保管する。

（開示及び訂正）

第 25 条　本協会は、本協会にて保有する特定個人情報等については、適法かつ合理的な範囲に限り開示することとし、特定個人情報等の本人より訂正の申出があったときは、速やかに対応する。

（本人確認）

第 26 条　本協会は、本人又は代理人から個人番号の提供を受けたときは、関係法令等に基づき本人確認を行うこととする。

２　書面の送付により個人番号の提供を受けるときは、併せて本人確認に必要な書面又はその写し（以下「本人確認書類」という。）の提出を求めるものとする。

（本人確認書類の保存）

第 27 条　提出された本人確認書類は、当該個人番号を利用する事務が終了するまでの間又は第 24 条第１項に規定する期間が経過するまでの間、これを適切に保管することができる。

第５章　第三者提供の停止に関する取扱い

（第三者提供の停止）

第 28 条　特定個人情報等が違法に第三者に提供されていることを知った本人からその提供の停止が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、遅滞なく第三者への提供を停止する。

第６章　その他

（所管官庁等への報告）

第 29 条　特定個人情報保護責任者は、事故が生じたときは、個人情報保護委員会及び所管官庁に報告するものとする。

（罰　則）

第 30 条　本協会は、本規程に違反した職員等に対して、就業規則、契約又は法令に照らして処分を決定する。

（規程の改廃）

第 31 条　本規程の改廃は、理事会の承認を得なければならない。

（附　則）

本規程は、平成 27 年 12 月１日から施行する。

（附　則）

本規程は、令和４年４月１日から施行する。

個人情報の安全管理に関する取扱細則

第１章　総　則

（目的）

第１条　本細則は、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）が個人情報の取扱いに関し適切な利用と保護を行うにあたり、個人情報保護委員会が定めた個人情報保護ガイドライン、本協会の個人情報保護規程第９条及び情報システム管理規程第 27 条に基づき、個人情報の管理に関し遵守すべき事項及び規律を定めるものである。

（定義）

第２条　本細則で用いる用語の定義は、本協会の個人情報保護規程第２条及び情報システム管理規程第２条に定めるものの他、以下に定めるものを含むものとする。

・保　　管：使用頻度が高い記録媒体等を随時使用できるように業務スペース室内（情報を取扱うセキュリティが確保された領域）に置くこと

・保　　存：電子データの記録媒体等への保存及び使用頻度が下がった紙媒体等を必要な期限を満たすまで倉庫等業務スペース室内以外の場所に置くこと

（適用範囲）

第３条　本細則は、個人情報を取扱う役員等及び職員等に適用する。

２　本細則は、個人情報及び個人情報に係る全てのシステム・機器類・記録媒体等について適用する。

３　本協会は、外部委託先社員等や派遣社員等、本協会と直接雇用契約がない者に対しても、誓約書の徴求等又は守秘義務契約等の締結により、本細則に準拠した行動を求めるものとする。

（遵守）

第４条　個人情報を取扱う役員等及び職員等は、個人情報の取扱いに関し適切な利用と保護を行うために、個人情報保護規程、特定個人情報等取扱規程、情報システム管理規程、本細則、個人データ取扱マニュアル等の本協会規定（以下「協会規定」という。）に従わなければならない。

２　役員等及び職員等は、他の者に対して協会規定に違反する行為を誘動、命令してはならない。

３　役員等及び職員等は、違反行為や漏えい、滅失、毀損その他の個人データの安全の確保に係る事案（以下「漏えい等」という。）又はその発生の兆候等を発見した場合には、速やかに個人情報保護管理者等の適切な権限者に報告し、その指示に従わなければならない。

（個人情報等の安全管理の取扱いに関する規定の整備）

第５条　本協会は、個人情報の取扱いに係る安全管理措置、役員等及び職員等の役割・権限・責任等を第２章安全管理措置に規定する。

２　個人情報保護管理者は、本協会における個人情報の取扱状況や情報通信技術の動向等を踏ま

えて、原則として年１回、必要な場合は都度、本取扱細則の見直しを行う。

３　本取扱細則は、本協会事務局内イントラネット上に常時掲示し、閲覧可能な状態に維持するとともに、改定した場合にはその旨を役員等及び職員等に通知する。

第２章　安全管理措置

第１節　組織的安全管理措置

（組織体制）

第６条　本協会は、組織的安全管理措置として、次に掲げる措置を講じるものとする。

（１）　組織体制の整備について本条に定め、実施する。

（２）　個人データの取扱いに係る規律に沿った運用について第 14 条に定め、実施する。

（３）　個人データの取扱状況を確認する手段の整備について第７条に定め、実施する。

（４）　漏えい等に対する体制の整備について、個人情報事故細則に定め、実施する。

（５）　取扱状況の把握及び安全管理措置の見直しについて、自己点検、内部監査を実施する。

２　個人情報保護管理者は、個人情報管理に係る諸施策の推進状況、個人情報の安全管理に係る管理の状況、個人情報保護法対応状況、個人情報管理に関する各種規程類の制定・改廃等について、年に１回以上点検し、理事会に報告する。

３　個人情報保護管理者の下で、総務部を個人情報管理統括部門とし、個人情報安全管理全般に関する企画立案及び推進を行い、適切な個人情報の安全管理の実施を図る。

４　総務部は、以下の管理を行う。

（１）　個人情報を取扱う部門（以下「個人情報取扱部門」という。）における、個人情報の収集・入力、利用・加工、保管・保存、移送・送信、消去・廃棄の流れに沿った取扱いの実態の確認及び必要な見直しの指示

（２）　個人情報の保護に係る規程等の整備及び維持状況の確認、その評価・見直し又はその指示

（３）　本細則と異なる取扱いを行う場合の当該個人情報取扱部門との協議、その目的と必要性の確認及び必要な対応の指示

（４）　理事会等への報告連絡体制の整備

５　職員等の役割・責任

（１）　職員等は、プライバシーポリシー、協会規定に沿って、本協会の個人情報を業務上必要な範囲に限定して取扱う。

（２）　職員等は、個人情報の収集・入力、利用・加工、保管・保存、移送・送信、消去・廃棄の取扱いにあたっては、本細則を遵守するとともに、以下の事項に留意のうえ、情報の取扱いについて必要な場合は見直しを行う。

①　個人情報の取扱い（複写、保存等を含む）の目的とその必要性を確認できなかった場合には、原則として当該取扱いを廃止する。

②　利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認を実施し、誤りを発見した場合には訂正等を速やかに実施する。また、記録は定められた保存期間中、個人データを正確かつ最新の内容に保つよう努める。

③　個人データを扱う各情報システムは情報システム管理規程に基づき管理し、不正アクセスの防止や、権限のない者のアクセスの拒否、個人データの流出防止等を徹底するとともに、システムの維持を行う。

６　監査責任者は、個人情報の管理に係る本細則等の遵守状況について内部監査の対象とする。

また、個人情報保護委員会への届出に該当する重大な事故が発生した場合は、是正処置が終了後に臨時監査を行う。

（個人データの取扱状況を確認する手段）

第７条　本協会は、個人情報が記録された台帳（以下「個人情報台帳」という。）を整備することにより、個人データの適正な取扱状況を維持する。

（１）　個人情報保護管理者は、業務上取扱う個人データの安全管理措置を講じるため、職員等が取扱う個人データに関する個人情報台帳を作成させる。

（２）　個人情報台帳は、主な個人データの種類、名称、個人データの項目、責任者・取扱部門、利用目的、概数、アクセス権を有する者、保管方法など、個人データの各段階に応じたものとする。

（３）　特定個人情報の取扱状況を確認するため、個人情報台帳において特定個人情報を含むものとする。

（４）　個人情報台帳は、年に一度は定期的に見直すほか、新たに個人データが追加された場合は、その都度更新する。

（匿名化した個人データの取扱い体制）

第８条　本協会は、無料経営相談に係る個人情報に関して、相談者及び回答者の個人情報を削除し、匿名化した個人データを本協会ホームページに公開する場合がある。公開する情報は匿名化した個人データではあるが、復元可能な情報であり個人データとして管理する。

２　前項の個人データを取扱う担当者は、匿名化した個人データのホームページの公開にあたっては、相談者氏名及び回答者氏名等を削除する他、相談項目等に特定の個人を識別できる情報が含まれている場合は一般化したうえで、公開する。

３　本協会は、匿名加工情報データベースを構成する検索可能な匿名加工データは作成しない。

第２節　人的安全管理措置

（人的安全管理体制の整備）

第９条　本協会は、役員等及び職員等による本協会の個人データの漏えい等や不適切な利用等を未然に防止するため、役員等及び職員等に対して必要かつ適切な監督を実施する。

２　本協会は、職員等に対する監督として以下の事を行う。

（１）　個々の職員等との間で、採用時等において、業務上知り得た秘密等に関する守秘義務を含む非開示契約又は誓約書（以下「誓約書等」という。）の締結・取得・管理・保管を行う。誓約書等には、職員等でなくなった後においても、非開示義務を遵守する旨の内容を含むものとする。

（２）　就業規則等において、業務上知り得た秘密等に関する守秘義務や、個人情報保護に係る関係法令等や協会規定に違反した場合に適用されうる処分を定める。

（３）　本協会は、誓約書等の提出にあたっては、職員等に対して内容を十分に説明する。

（４）　外部委託先社員等や派遣社員等、本協会と直接雇用契約がない者を情報の取扱いに係る業務に従事させる場合には、外部委託契約や派遣契約に守秘義務を規定する。

３　役員等及び職員等の役割・責任等の明確化

（１）　本協会は、各管理段階における情報の取扱いに関する役員等及び職員等の役割・責任の明確化及びアクセス権限の設定を実施する。

（2） 本協会は、職員等の雇用終了時に、保有していた本協会の資産を全て返却させるとともに、直ちに個人データ及び情報処理施設へのアクセス権の削除を実施する。

4 教育・研修

（1） 個人情報の教育担当者は、個人データを取扱う全ての役員等及び職員等に対して、個人情報管理に係る関係法令等や協会規定の周知と個人情報保護に対する意識の向上を図るための教育・研修を行うための体制を整備する。

（2） 個人情報の教育担当者は、個人情報取扱部門と協働して役員等及び職員等に対する個人情報の保護に関する教育・研修の計画を年度ごとに策定する。個人情報取扱部門は、当該計画に沿って教育・研修を実施するとともに、教育・研修が効果的であることを確実にするために、教育・研修の評価及び見直しを行う。

5 懲戒等

本協会は、就業規則等において、個人情報の取扱いに関する役員等及び職員等の役割・責任、及び情報管理に係る関係法令等や協会規定への違反時には懲戒処分を行うことがある旨を定めて役員等及び職員等に周知するとともに、違反行為を行った役員等及び職員等及び当該違反行為に関係した職員等に対し、関係法令等や就業規則等に照らして懲戒等の処分や損害賠償の請求等を行うことがある。

第3節 物理的安全管理措置

（物理的安全管理措置の設定）

第 10 条 本協会は、正当なアクセス権限を有しない者による本協会の個人データへのアクセスや、漏えい等を防ぐため、以下のとおり、適切な物理的安全管理措置を講じる。

1 建物内の各領域のセキュリティ要求事項の設定

本協会は、建物内の各領域のセキュリティ要求事項の設定として、以下の対策を実施する。

（1） 建物内の各領域のセキュリティ境界及びセキュリティ要求事項の設定

職員等が利用する建物内の全ての領域について、実施される業務内容や取り扱われる個人情報、システム・機器類の有無等に応じて、セキュリティ管理上の境界を定め、以下の対策を実施する。

① 各エリアの管理区分として、以下の通りセキュリティ管理上の境界を設定する。

(a)非セキュリティエリア: 暗証扉外のエリア（エレベータ前）

(b)セキュリティエリア：各フロア暗証扉内のエリア（高セキュリティエリアを含む）

(c)高セキュリティエリア：本協会内において内部情報管理等の観点から高度な配慮を必要とするエリア（個人番号取扱いエリア）

② 総務部長は、本協会が直接使用する全てのセキュリティ境界につき、セキュリティ要求事項を設定する。

(a)非セキュリティエリア要求事項

a. 内線電話を設置し、応対する者が応対するまで待機させる。

b. 不審者の有無を黙視する。

(b)セキュリティエリア要求事項

a. セキュリティエリアは、職員等は識別証の着用をする。

b. セキュリティエリア内に職員等以外の者が入る場合は、応対する職員等は必ず付き添うか、又は入出記録を残す。

c. 入退館・入退室の電子錠の設置と開錠、施錠の記録を自動作成する。

d. セキュリティエリア（執務室）の最終退出者は、退出記録に氏名、時間を記載する。

(c) 高セキュリティエリア要求事項

特定個人情報等を取り扱う業務に関するエリアとして、特定個人情報を取り扱うシステムを管理する区域（管理区域）及び特定個人情報等を取り扱う事務を実施する区域（取扱区域）を明確化し、特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的安全管理措置を講じる。

（2）各領域のセキュリティ要求事項の遵守状況確認

セキュリティエリアの管理責任者は定められたセキュリティ要求事項が遵守されているか定期的に確認し、必要な場合には改善措置を実施する。

2　電子機器及び電子媒体の盗難防止策

本協会は、電子機器及び電子媒体の盗難防止策として、以下の対策を実施する。

（1）防犯設備の設置等

犯罪の未然防止と発生時の対応のため、建物の構造等に応じ、以下の防犯対策を実施する。

① 入居するフロアの階段扉の施錠装置の設置
② オフィス入口ドアの施錠装置の設置
③ 休日出勤等に利用する場合は、事前に上長に承認を得る。

（2）個人情報の保護管理策の実施

個人データの盗難、紛失等への対応のため、以下の対策を実施する。

① 重要な個人データを記載した紙媒体、記録媒体は、施錠保管管理を行う。
② 離席時に個人データを記した紙媒体、記録媒体、携帯可能な機器類の机上放置の禁止又は代替の安全管理措置を実施する。

3　電子媒体を持ち運ぶ場合の漏えい等防止策

本協会は、媒体移動時の漏えい等防止策として、以下の対策を実施する。

（1） 漏えい等への備え

（2） 権限の無い者のアクセス防止

前項に対する管理策として、以下のことを実施する。

① 個人データが保管されている PC を外部持ち出しする場合は、生体認証設定を行い、本人以外にアクセスできないよう制御する。
② バックアップ媒体は、倉庫に移動する際は専用のケースに格納し、担当者が施錠をして保管業者と授受を行う。
③ 個人データが保管された USB メモリー等記録媒体を外部に持ち出す場合は、事前に上長に持ち出しの承認を得て持ち出す。また、持ち出す媒体にロックをかけるか、パスワード設定をする。

4　個人データの削除及び電子機器・電子媒体の廃棄

本協会は、個人データの削除及び電子機器・電子媒体の廃棄時の漏えい防止策として、以下の対策を実施する。

（1）個人データの削除・廃棄による漏えい等の防止

個人データの削除・廃棄による漏えい等の防止を図るため、以下の対策を実施する。

① 個人データが記録された書類は、保管期限を定め、期限到来後速やかに廃棄する。

② 廃棄書類の廃棄は、他の者の立ち合いのうえ、シュレッダーで裁断、又は廃棄業者に委託して溶解廃棄する。溶解廃棄の場合は溶解証明をとる。

（2）不完全な消去・未消去による漏えいの防止

不完全な消去又は未消去によって個人データが漏えいすることを避けるため、以下のことを実施する。

① 個人データが記録された電子媒体の廃棄方法については、適切なデータ消去ツールを使用してハードデスク等の記録媒体を完全消去するか、記録媒体を物理的に破壊する。

② 電子機器がリース等による貸与者の資産の場合には、返却前に適切なデータ消去ツールを使用してハードデスク等の記録媒体を完全消去するか、返却後に貸与業者により記録媒体を完全消去することを依頼し、消去後に消去証明を入手する。

③ 複合機がリースアップにより返却される場合には、返却前に複合機内のハードデスク等の記録媒体を完全消去するか、返却後にメーカーで録媒体を完全消去することを依頼し、消去後に消去証明を入手する。

第4節　技術的安全管理措置

（技術的安全管理）

第11条　本協会は、個人データの適正な稼動等を確保するため、以下のとおり、適切な技術的安全管理措置を講じる。

1　個人情報の利用者の識別及び認証

本協会は「個人情報の利用者の識別及び認証」として、以下の対策を実施する。

（1）　本人確認機能の整備

個人情報の利用者が正当な権限を保有した本人かどうかの正当性を確認（以下「本人確認」という。）する機能を整備する。具体的には、以下の対策を実施する。

① 職員等が使用するPCは原則指紋認証などの生体認証設定とし、本人識別を行う。

② 生体認証設定ができない場合の措置としてIDとパスワードを使用し、本人識別を行う。

（2）　本人確認に関する情報の不正使用防止機能の整備

本人確認に関する情報の不正使用防止として、以下の対策を実施する。

① 第三者による悪用を抑止するため、指紋などの生体認証により本人認証する。

② 生体認証が通らない場合には、情報システム担当者がIDとパスワードとの仕組みを有効にし、以後IDとパスワードで本人認証する。

③ 個人データが保管されている共有サーバへのアクセスは、使用するPCのキッティング（初期設定）時にアクセス権限を付与し、本協会事務局内のイントラネット環境下で接続した場合に本人認証する。

④ ネットバンキングシステム、PX 給与システム等高い安全性が求められるシステムについてはIDとパスワードを設定し、本人認証する。

⑤ パスワードは本人が自ら設定し、パスワードを忘れて再設定する場合は、システム担当者より初期のパスワードの発行を受けて、自ら変更する。

（3）　本人確認に関する情報が他人に知られないための対策

本人確認に関する情報が他人に知られることを防止するため、以下の対策を実施する。

① 情報システム管理規程第14条の規定に従い実施する。

2　情報のアクセス権限の管理

職員等がアクセスできる個人情報データベース等の範囲を限定するため、適切なアクセス制御を以下のとおり実施する。

（１） アクセス権の設定

① 個人データを取り扱う情報システムを使用する職員等が、正当なアクセス権を有する者であることを、生体認証又はユーザーID、パスワード等により認証する。

② 個人情報が保管されるサーバへのアクセス権限は、本部事務局員へ貸与する PC アクセス権を付与し、本部の LAN 接続下でのみアクセスできるよう設定する。

③ 職員等に付与するアクセス権限を必要最小限に限定する。

④ 支部及び研修団体が本協会の情報にアクセスする場合は、ユーザーID、パスワードにより認証し、研修管理システムにアクセスできるよう設定する。

⑤ 会員がホームページの会員専用ページにアクセスする場合は、ユーザーID、パスワードにより認証する。

（２） アクセス権限の付与を明確に確実にするため、以下のことを実施する。

① アクセス権限の設定作業は情報システム管理規程第４条に規定された運営管理者に指示された者（以下「情報システム担当者」という。）が行う。

② 情報システム担当者は、アクセス権限の登録、変更、抹消は職員等の異動に伴い速やかに行うとともに、異動処理の時点で、職員等に付与されたアクセス権が必要最低限で付与されていることを確認する。

３ 情報システム利用に伴う個人情報の漏えい等防止策

個人情報の漏えい等防止策として、情報の保護策を実施する。

（１） 個人情報の保護策

情報の漏えい等防止策として、以下の対策を実施する。

① 保管データの漏えい等防止策

② 移送・伝送データの漏えい等防止策

③ コンピュータウイルス等不正プログラムへの防御対策

（２） 保護策の詳細

① 保管データの漏えい等防止策の詳細策

ファイルの不正コピーや盗難等による漏えい等を防止するため、以下の事項に留意し実施する。

(a) 個人情報を取り扱うシステム・機器について、紛失や権限外の者がアクセスするリスクを考慮して設置する。

(b) 保管・バックアップに外部記録媒体を用いる場合は、不正コピー・盗難があった際の対策として、記録媒体にロックをかけるかパスワードを設定する。

(c) 不正アクセスや目的外利用を防止するため、USB メモリーや CD-ROM 等の記録媒体を情報システムに接続する場合は、事務局から貸与された電子記録媒体のみ使用し、接続時にウイルスチェックを行う。

(d) USB メモリー等の記録媒体等は、業務上の必要性が認められる場合以外は、利用・加工段階における外部への持ち出しを禁止する。

(e) USB メモリーの紛失の際に、個人データの漏えい等を防止するため、個人情報のデータ保存目的で使用する場合以外、利用目的が終了した都度 USB メモリー内のデータを消去し、保管する。

② 伝送データの漏えい等防止策

個人情報の移送・伝送時に盗聴等による漏えい等を防止するため、データの移送・伝送時に盗聴された場合にもデータの内容がわからないようにする等の対策を実施する。

(a) 個人情報を通信（例：本人及び職員等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など）する場合には、個人情報が記録されたファイルへのパスワードの設定又は暗号化を実施する。

(b) パスワードの伝達方法はメール以外の手段を原則とし、やむをえずメールで伝達する場合は、誤送信リスクを十分認識し、細心の注意を払って実施する。

(c) バックアップ媒体の移送時は、移送専用ケースに入れて、移送する者が施錠・解錠する。施錠・解鍵用の鍵は移送する者が自ら保管する。

③ コンピュータウイルス等不正プログラムへの防御対策

コンピュータウイルス等不正プログラムへの防御対策として、以下の事項に留意し、コンピュータウイルスの侵入や不正アクセスによるプログラムの改ざんがなされないための対策を実施する。

(a) 使用する PC 等についてはセキュリティソフトウエアの導入を実施する。

(b) 差出人が不明又は不自然な電子メールを受信した場合は、不用意に添付ファイルは開かずに、当該電子メールを速やかに削除する。また、必要と判断した場合は、情報システム担当者に報告する。

(c) 不正ソフトウェアか否かにかかわらず、無認可のソフトウェアの導入・使用を禁止する。また、内部監査等を通じて定期的及び必要な場合には随時、システム及び機器内の無認可ソフトウェアの有無を確認する。

(d) 利用者が、システムやサービスのセキュリティの弱点又はそれらへの脅威に気づいた場合、若しくは疑いを持った場合には自らの判断のみで対処することなく、直ちに、情報システム担当者及び部門責任者に報告し、その後の対応については、関係各部又は個人情報保護管理者の指示に従う。

(e) オペレーションシステム（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）は速やかに適用する。

(f) 不正ソフトウェア対策の有効性・安定性を確認する（例：パターンファイル、修正ソフトウェアの更新の確認など）。自動更新の場合、適用する全機器の更新状況を確認する等、仕組みの実効性を確保する。

4　情報システムの開発・運用時の脆弱性への対応策

（1）情報システムの開発時の脆弱性への対応

① 本協会は、情報システムを開発する際には、開発目的、実現機能、システムの構成、セキュリティの確保、障害対策、既存他のシステムの連携等を充分に検証し、開発にあたるものとする。

② セキュリティの確保に関しては、情報システム自体のセキュリティ確保は勿論として、本協会のイントラネットに接続した環境下でのセキュリティの確保を含めて検証し、開発する。

（2） 情報システムの運用時の脆弱性への対応

① 本協会は、協会の外側（インターネット）からの脅威に対処し、セキュリティの確保を確実にするため、信頼できる専門の事業者により構築されているセキュリティサービスを受けることによって、協会の内側（イントラネット）に係るセキュリティを確保する。

② 本協会は、マルウエア等により不正通信が発生した場合には、①の事業者よりアラートが発せられることから、アラートを受け取り次第速やかに検証し、必要な対応をとる。

③　本協会は、サーバが通常の稼働と異なる事象が発生した場合には、以下の対応をとる。
(a) 情報システム担当者はログの分析により、不正アクセス等を調査する。
(b) 本協会は、Web サーバに対して不正アクセスがあった場合には、Web サーバの運営を行う者より通知を受け、アクセスを検証し、必要な対策を実施する。
(c) 本協会は、本協会内に設置しているサーバは①に規定する専門の事業者により構築されているセキュリティサービスを受けることによって、イントラネットに係るセキュリティを確保する。また、マルウエアやスパイウェアの脅威に対しては、サーバにウイルスソフトを組み込むことによって常時脅威を監視し、脅威に対処する。
(d) 本協会内部に設置している会員データベースへのアクセスは、データベースにアクセスした PC に付された個別の番号によってアクセスログを収集する。アクセスログの確認が必要な事態が生じたときは、PC に付された個別の番号と紐づけされている個人を特定し、必要な検証と分析を行う。アクセスログは、サーバ内に自動保存され一定期間保持される。その後、情報システム担当者が保存用ファイルへ移行し保存する。
④　e ラーニング等のシステムのアクセスログは、適正に受講しているか研修視聴時間ログを、その e ラーニング等の担当者が必要に応じて抽出して確認する。
⑤　アクセスログの定期確認は、自己点検時と内部監査時に実施する。
⑥　本協会は、自然災害，悪意のある攻撃又は事故に対する物理的な保護を目的として、サーバ等に保存しているデータは自動的に日々バックアップ行う。
　また、火災や盗難等のリスクに対応するため、下記のデータは１ヶ月に１度データをバック媒体にバックアップをとり、外部倉庫で保管する。外部で保管するときの安全確保については、本条第３項（２）②(c)による。
(a) 会員データベース等が稼働するサーバのデータ
(b) 共有データが保存される NAS のデータ
(c) 人事データが保存される PX4 クラウドのデータ
(d) 人事関連のデータ

（３）　障害発生時の技術的対応・復旧手続の整備
本協会は、障害発生時の技術的対応・復旧手続として、以下の対策を実施する。
①　データバックアップの環境を整備する。
②　業務で共有して使用するデータの保存はファイルサーバに保存する。
③　利用者個人で使用するデータは PC 内に保存するとともに、利用者に割り当てられた利用者専用の One Drive for Business（Microsoft 社）に同期をとる。ただし、データに個人情報が含まれる場合は、データ又はフォルダにパスワードを設定するか、若しくは One Drive for Business に二段階認証を設定するか、何れかを選択し、なりすましの防止を行うものとする。
④　コンピュータウイルス等不正プログラムによる被害時には、バックアップ媒体からデータを復元処理する。

（リモートアクセス管理）

第 12 条　本協会は、リモートワーク等により外からネットワークにアクセスする場合の情報の保護策として、以下のとおり、適切な安全管理措置を講じる。

（１）リモートアクセスの保護策として、以下の対策を実施する。
①　端末に対する対策
(a) 本人が執務室で使用している PC を使用する。

(b) 端末等の紛失・盗難に備え、PC は遠隔でデータを消去できる機能を設定する。
(c) 不正侵入・不正利用対策として、生体認証での本人確認を行う。

② 通信経路における対策
(a) 共有サーバにアクセスする場合は、VPN を使用する。
(b) インターネット等の利用時にフリーWi-Fi を利用する場合は、使用する Wi-Fi の信頼性を判断し、慎重に利用する。(例えば、ホテルが提供する Wi-Fi と個人の飲食店が提供する Wi-Fi ではセキュリティ確保のレベルが異なる場合が想定される。)

③ 協会内システムにおける対策
(a) ウィルス・ワーム防止策をとる。
(b) 不正侵入・不正利用の監視を行う。

第５節　外的環境の把握

(個人情報を取り巻く環境の把握)

第 13 条　本協会は、個人情報の保護に係る関連法令、情報セキュリティ技術、インフォメーションテクノロジー、情報通信等の環境変化について注視する。

２　個人情報保護管理者は、上記の個人情報を取り巻く環境の変化が本協会の個人情報保護の体制に重大な影響を与えると判断した場合には、理事会に報告し、対応する。

第３章　個人情報の取扱いの各局面における安全管理

(個人情報の取扱いの各局面における安全管理に係る取扱い)

第 14 条　本協会は、本協会の個人情報の取扱いの各局面において、個人データを記録した媒体等の性質等に応じた適切な安全管理措置を講じることとし、具体的な方法等を以下に規定する。

また、個人データの取扱い（複写、保存等を含む）の目的とその必要性を確認できなかった場合には、原則として当該取扱いを廃止する。

（１） 個人情報の取扱いの各局面における安全な取扱い規律の整備

本協会は、収集、利用（入力・加工)、保管・保存、提供（委託・移送)、廃棄・削除の各局面における個人データの安全な取扱いを行うため、情報の種別に応じた業務マニュアル（以下「個人データ取扱マニュアル」という。）を整備し、個人データの取扱いは個人データ取扱マニュアルに準拠する。

個人データ取扱マニュアルは下記の三種別とする。

① 会員等外部関係者に係る個人データの取扱マニュアル
② 職員等に係る個人データの取扱マニュアル
③ 支部における個人データの取扱マニュアル

（２） 個人情報保護法及び第１号で規定した規律違反が起きたときの報告体制

職員等は、個人情報保護法や本協会が整備している協会規定に違反している事実又は兆候を把握した場合には、速やかに個人情報保護管理者に報告するものとする。

① 報告を受けた個人情報保護管理者は、速やかに事実の確認を行う。
② 確認の結果、違反している事実又は兆候を把握した場合には、所管部長に速やかに処置を行うよう指示する。
③ 指示を受けた所管部長は、速やかに処置を行う。

（３） 個人データ取扱マニュアルでは、以下の事項を明確にする。

なお、下記の②取扱いの詳細(a)から(e)の規定は、個人データの取扱状況及び記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とする。

① 対象個人情報

(a) 対象個人情報

(b) 対象個人情報台帳番号

(c) 対象とする業務

(d) 使用システム

(e) 使用電子媒体

② 取扱いの詳細

(a)収集段階における取扱いに関して、以下の事項を定める。

a. 取扱責任者

b. 収集部門

c. 収集目的

d. 収集する個人情報

e. 収集時の安全管理措置上の実施事項

(b)利用（入力・加工）段階における取扱いに関して、以下の事項を定める。

a. 取扱責任者

b. 利用部門

c. 利用業務

d. 利用個人情報

e. 利用時の安全管理措置上の実施事項

(c)保管・保存段階における取扱いに関して、以下の事項を定める。

a. 取扱責任者

b. 保管・保存部門

c. 保管・保存の業務

d. 保管・保存方法

e. 保管・保存時の安全管理措置上の実施事項

(d)提供（委託・移送を含む）段階における取扱いに関して、以下の事項を定める。

a. 取扱責任者

b. 提供部門

c. 提供・委託等の業務

d. 提供個人情報

e. 提供時の安全管理措置上の実施事項

(e)廃棄・削除段階における取扱に関して、以下の事項を定める。

a. 取扱責任者

b. 廃棄・削除部門

c. 廃棄・削除の対象となる業務

d. 保管期間

e. 廃棄・削除時の安全管理措置上の実施事項

第４章 支部での適用

（支部での適用）

第 15 条　本細則を支部で適用する際は、支部における個人データ等の取扱マニュアルに定めるものとする。

第５章　雑　則

（改廃）

第 16 条　本取扱細則の制定及び改廃は、理事会の承認を得なければならない。

（附則）

第 17 条　本取扱細則は令和４年４月１日から適用する。

個人情報事故細則

第１章　総則

（目的）

第１条　本細則は、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）における個人情報の取扱いについて漏えい、滅失、毀損又はそのおそれのある事案、及び個人情報保護規程第４条に規定する目的外利用の事案（以下「漏えい等事案」という。）が発覚した場合に、個人情報保護規程第 24 条又は特定個人情報取扱規程第 29 条に基づき取るべき措置を明確にするとともに、被害を最小にすることを目的とする。

第２章　定義

（定義）

第２条　本細則で用いる用語の定義は、本協会の個人情報保護規程第２条に定めるものとする。

第３章　緊急事態対応

（緊急事態の対応）

第３条　個人情報に係わる漏えい等事案を認識した者は、別表１「個人情報に関する事故情報連絡順序」に示す順序で事故情報を伝達する。

２　個人情報保護管理者は、事故報告を受領後速やかに別表１－２「個人情報に関する事故対応体制」に基づき、事故対応体制をとるものとする。

３　前項に基づき事故対応を所管する組織として、個人情報事故調査委員会（以下「事故調査委員会」という。）を設置する場合には、会長、副会長、個人情報保護管理者、監査責任者、総務部長、及び該当する場合（支部における事故の場合）は当該地区協議会代表並びに当該個人情報保護部門管理者によって構成し、事実調査を行い、当該事故を所管する。

４　事故調査委員会の所管に該当しない個人情報事故は別表１－２の一類、二類の事故を所管する組織が、事実調査を行い、当該事故を所管する。

５　事故発生部門の責任者は、別紙１「個人情報漏えい等事故対応記録」を作成し、必要に応じて資料等を添付し、個人情報保護管理者に提出する。

（漏えい等事案が発覚した場合に講ずべく措置）

第４条　本協会は、本協会が保有する個人情報（特定個人情報を含む）の漏えい等事案が発覚した場合は、漏えい等事案の内容に応じて次に掲げる事項について必要な措置を講ずる。

（１）　本協会内部における報告及び被害の拡大防止

別表１「個人情報に関する事故情報連絡順序」に規定する責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

（２）　事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

（３） 影響範囲の特定

上記（２）で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。

（４） 再発防止策の検討及び実施

上記（２）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。

（５） 個人情報保護委員会への報告及び本人への通知

第６条に該当する漏えい等事案の場合は個人情報保護委員会へ速やかに報告及び本人へ通知し、又は本人が容易に知り得る状態に置く。

（ガイドライン 3-5-2）

（委託先で個人データの漏えい等事案が発覚した場合に講ずべく措置）

第５条　個人情報保護管理者は、個人情報の取扱いを委託した委託先から委託している個人情報の漏えい等の事故発覚の報告を受けた場合には、次に記載する事項について必要な措置を実施する。

（１） 委託先から事故の概要と、影響度を速やかに報告させる。

（２） 漏えい等の事故内容が、第６条第１項（１）又は（２）に該当する場合には、原則として個人情報保護委員会への報告を委託元と委託先の双方で行うか、委託元及び委託先の連名で報告するかを守秘義務契約等に基づき委託先の代表者と協議する。

（３） 個人情報保護委員会への報告対象の漏えい等の事故の場合は、第６条第２項（１）に基づき速やかに個人情報保護委員会に対して報告を行う。

（４） 本人に対して、漏えい等の事故発生について通知又は公表を行う。

（５） 事故に対する処置及び是正処置を入手し、処置を評価する。

（６） 前（３）に該当する漏えい等の事故である場合は、前項の是正処置の評価結果を踏まえて、個人情報保護委員会に対して第６条第２項（２）に従って詳細報告を行う。

（７） 委託先には、是正処置の評価を踏まえて、必要な場合には改善策の実施状況を報告させるか、監査を行う。

（個人情報保護委員会への報告）

第６条　個人情報保護管理者は、取り扱う個人データの漏えい等その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定める以下の事態が生じたときは、当該事態が生じた旨を個人情報保護委員会に報告する。

（１） 個人情報

① 要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。）の漏えい等が発生し、又は発生のおそれがある事態（個人情報の保護に関する法律施行規則第６条の二 １）

② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（個人情報の保護に関する法律施行規則第６条の二 ２）

③ 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（個人情報の保護に関する法律施行規則第６条の二 ３）

④ 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある

事態（個人情報の保護に関する法律施行規則第６条の二 ４）

（２） 特定個人情報

次に掲げる特定個人情報が漏えい等した事態

① 次に掲げる特定個人情報に係る本人の数が百人を超える事態（特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則第２条２）

(a) 漏えい等した特定個人情報

(b) 行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第９条の規定に反して利用された個人番号を含む特定個人情報

(c) 番号法第 19 条の規定に反して提供された特定個人情報

② 本協会が保有する特定個人情報ファイルに記録された特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ、その特定個人情報が閲覧された事態（特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則第２条３）

③ 不正の目的をもって、本協会が保有する特定個人情報ファイルに記録された特定個人情報を利用し、又は提供した者がいる事態（特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則第２条４）

２ 個人情報保護委員会に対する報告は、当該事態を知った日より下記の日数内に行う。

報告事項は、第３項に規定する内容とする。ただし、報告時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる。

（１） 速報：速やかに（当該事態を知った時点から概ね３日から５日以内）

（２） 確報：当該事態を知った日から 30 日以内（不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態 60 日以内）

（個人情報の保護に関する法律施行規則第６条の３第１項、第２項）

３ 個人情報保護委員会に対する報告事項

（１） 概要

（２） 漏えい等が発生し、又は発生したおそれがある個人データの項目

（３） 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数

（４） 原因

（５） 二次被害又はそのおそれの有無及びその内容

（６） 本人への対応の実施状況

（７） 公表の実施状況

（８） 再発防止のための措置

（９） その他参考となる事項

特定個人情報の報告の場合は、上記報告事項（２）の個人データは特定個人情報と読み替え、（３）の個人データに係る本人の数は特定個人情報の数と読み替える。

４ 個人情報保護委員会に対する報告は、報告すべき情報が個人情報又は特定個人情報かにより、指定されたフォームを選択して報告する。

（１） 個人データの場合「漏えい等の対応（個人データ）」の漏えい等の報告フォーム

（ https://roueihoukoku.ppc.go.jp/?top=kojindata ）

（２） 特定個人情報の場合「特定個人情報の漏えい等の対応について」の漏えい等の報告フォーム
（ https://roueihoukoku.ppc.go.jp/?top=mynumber ）

５ 重大な影響が生じると判断された事案、公表事案等の急を要する報告は、指定フォームでの報告の前に、個人情報保護委員会の個人データ漏えい等報告窓口に速やかに報告する。
個人情報保護委員会 TEL．０３－６４５７－９６８５

６ 個人情報保護委員会への報告を要しない事案
第１項に該当する事態が生じた場合であっても、次の（１）又は（２）に該当するときは、個人情報保護委員会への報告を要しない。

（１） 個人データの漏えい等事案で、次の①又は②のいずれかに該当する場合
① 実質的に個人データが外部に漏えいしていないと判断される場合
(a) 漏えい等事案に係る個人データについて高度な暗号化等の秘匿化がされている場合
(b) 漏えい等事案に係る個人データを第三者に閲覧されないうちに全てを回収した場合
(c) 漏えい等事案に係る個人データによって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合（ただし、漏えい等事案に係る個人データのみで、本人に被害が生じるおそれのある情報が漏えい等した場合を除く。）
(d) 個人データの滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データを閲覧することが合理的に予測できない場合
(e) 上記(a)～(d)のほか、外部に漏えいしていないと合理的に判断できる場合
② FAX 若しくはメール誤送信、又は荷物の誤配等のうち軽微なものの場合
（平成 29 年個人情報保護委員会告示第１号３．（２））

（２）特定個人情報の漏えい等事案で、下記に該当する場合
本協会の従業員の数が 100 人以下であって、次の全てに当てはまる場合は、個人情報保護委員会への報告を要しない（ただし、個人番号の利用制限違反等の番号法固有の規定に関する事案等の場合を除く。）。
① 影響を受ける可能性のある本人全てに連絡した場合（本人への連絡が困難な場合には、本人が容易に知り得る状態に置くことを含む。）
② 実質的に外部に漏えいしていないと判断される場合
③ 事実関係の調査を了し、再発防止策を決定している場合
④ 「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」（平成 27 年 特定個人情報保護委員会規則第５号）第２条に規定する特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態に該当しない場合
（平成 27 年特定個人情報保護委員会告示第２号２．（２））

（本人への通知）

第７条 個人情報保護管理者は、第６条に該当する個人情報の漏えい等が発生した場合は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態（以下「通知対象事態」という。）が生じた旨を通知する。ただし、本人への通知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。

【本人への通知が困難な場合に該当する事例】

事例１）保有する個人データの中に本人の連絡先が含まれていない場合

事例２）連絡先が古いために通知を行う時点で本人へ連絡できない場合

【代替措置に該当する事例】

事例１）事案の公表

事例２）問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにすること

（ガイドライン 3-5-4-5）

２　本協会は、第６条に該当する通知対象事態を知ったときは、当該事態の状況に応じて速やかに、本人への通知を行うものとする。「当該事態の状況に応じて速やかに」とは、速やかに通知を行うことが求められるものであるが、具体的に通知を行う時点は、個別の事案において、その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断するものとする。

（ガイドライン 3-5-4-2）

３　本人へ通知すべき事項は、第６条第３項（１）、（２）、（４）、（５）、（９）とする。なお、これらの事項が全て判明する前であっても、判明した一部のみでも前項に従って通知する必要があると本協会が判断した場合には、当該一部を本人に通知するものとする。また当初、通知対象事態に該当すると判断したものの、その後、通知対象事態に該当していなかったことが判明した場合には、本人への通知は不要とする。

（ガイドライン 3-5-4-3）

４「本人への通知」とは、本人に直接知らしめることをいい、事業の性質及び個人データの取扱状況に応じ、通知すべき内容が本人に認識される合理的かつ適切な方法によるものとする。

（ガイドライン 3-5-4-4）

（マスコミへの対応）

第８条　マスコミへの対応が必要な場合は、公表文書を作成し、理事会の承認を得て公表する。

（是正処置）

第９条　個人情報保護管理者は、漏えい等の事故処理が終了した後、事故再発防止策として、事故を起こした部門の責任者に対して、再発防止策を策定させ、別紙２「個人情報の漏えい等事故に関する是正処置報告書」を理事会に上程させる。

２　前項の部門の責任者は「個人情報の漏えい等事故に関する是正処置報告書」が理事会において承認された後、再発防止策を実施する。

３　個人情報保護管理者は、当該部門において再発防止策が実施された後、再発防止策の効果の確認を行う。効果の確認結果は理事会に報告する。

（対応記録の保管）

第 10 条　個人情報保護管理者は、「個人情報漏えい等事故対応記録」及び「個人情報の漏えい等事故に関する是正処置報告書」を保管する。「個人情報漏えい等事故対応記録」及び「個人情報の漏え

い等事故に関する是正処置報告書」には、漏えい等を起こした職員等の懲戒記録を含む。

第４章　支部での適用

（支部での適用）

第 11 条　本細則は、支部で適用する際には、支部における個人データ等の取扱マニュアルに定めるものとする。

第５章　雑則

（制定及び改廃）

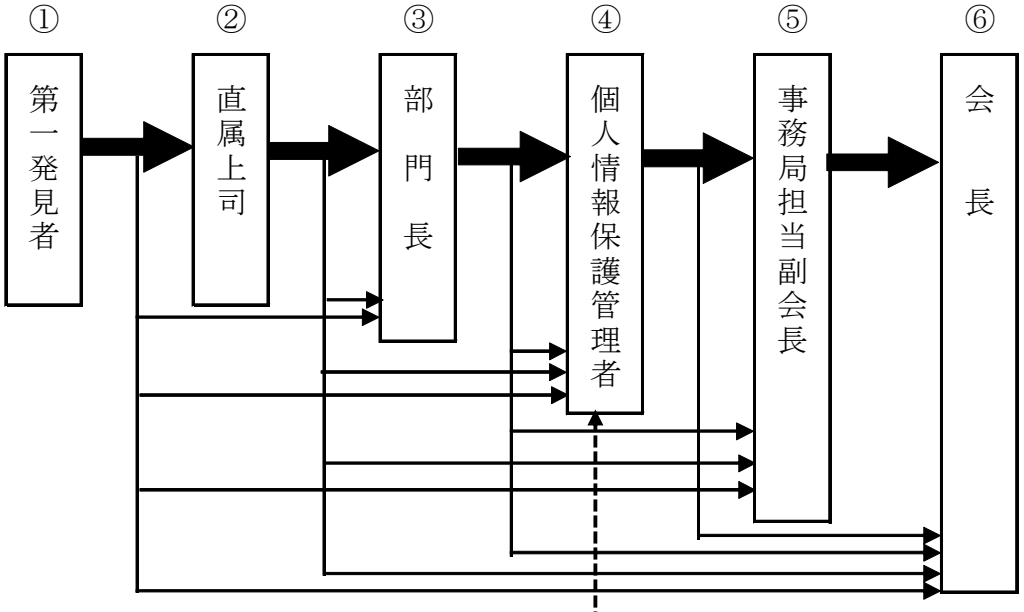
第 12 条　本細則の制定及び改廃は、理事会の承認を得なければならない。

（附則）

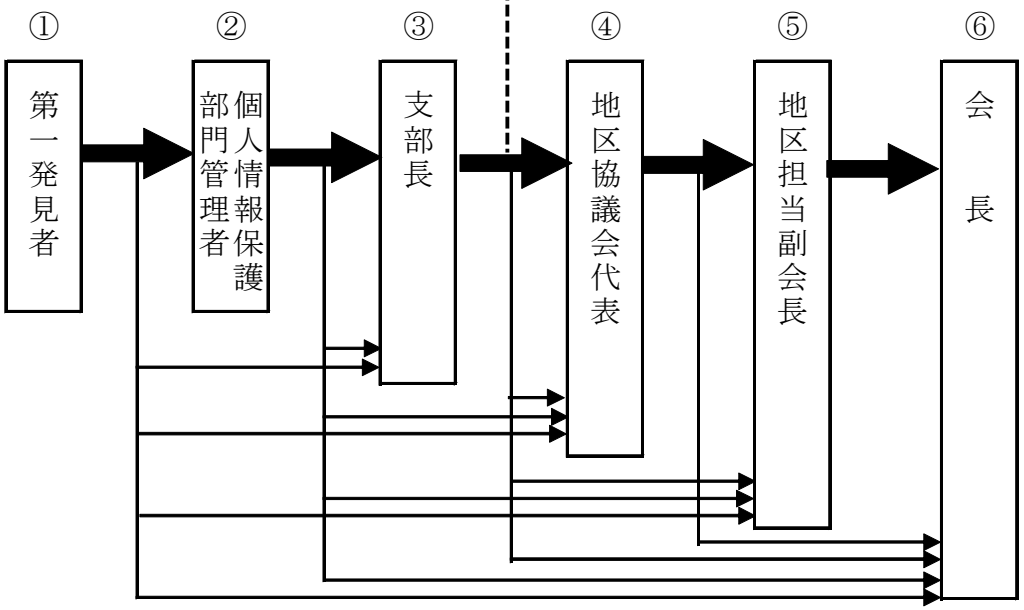
本細則は、令和４年４月１日から施行する。

別表１ 個人情報に関する事故情報連絡順序

連絡順序１．本部



連絡順序２．支部



注１　第一発見者は、把握した事故情報を上記連絡順序に従い、伝達すること。（本部・支部共通）
注２　連絡先が不在、又は連絡ができない場合、次の連絡先へ伝達すること。（本部・支部共通）
注３　支部での事故は、支部長より個人情報保護管理者に伝達すること。

別表１－２　個人情報に関する事故対応体制

個人情報保護管理者は、部門長より事故の報告を受けて、速やかに次の報告者に対して、第一報を入れるとともに、事故対応体制を下記の基準に従い構築する。

事故対応体制構築基準１（本部）

区分	事故形態	事故件数	事故所管組織
一類	1. 郵便局、宅配便等配送段階での誤配 2. 保存データの誤消去	単数又は １桁内	個人情報保護管理者
二類	1. 一類の範疇の事故で、事故件数が一類を超える 2. 郵便物の誤封入、誤送付 3. 電子メール、FAX の誤送信 4. 組織内での個人情報の紛失、誤廃棄、誤消去等	該当なし	個人情報保護管理者 事務局担当副会長
三類	一類、二類に属さない事故全て 例1. 本細則第５条第１項に該当する場合 例2. 外出先で個人情報を紛失した場合 例3. 委託先が個人情報事故を起こした場合 例4. 漏えい等した個人情報が特定できず、公表する場合等	該当なし	事故調査委員会

事故対応体制構築基準２（支部）

区分	事故形態	事故件数	事故所管組織
一類	1. 郵便局、宅配便等配送段階での誤配 2. 保存データの誤消去	単数又は １桁内	個人情報保護部門管理者 個人情報保護管理者
二類	1. 一類の範疇の事故で、事故件数が一類を超える 2. 郵便物の誤封入、誤送付 3. 電子メール、FAX の誤送信 4. 組織内での個人情報の紛失、誤廃棄、誤消去等	該当なし	支部長 個人情報保護部門管理者 個人情報保護管理者 地区協議会代表 地区担当副会長
三類	一類、二類に属さない事故全て 例1. 本細則第５条第１項に該当する場合 例2. 外出先で個人情報を紛失した場合 例3. 委託先が個人情報事故を起こした場合 例4. 漏えい等した個人情報が特定できず、公表する場合等	該当なし	事故調査委員会

別紙１

個人情報漏えい等事故対応記録

作成者
作成日　　年　　月　　日

事故発生年月日		委員会報告	**要**	**不要**
項　目	記　　事			
漏えい等事故の概要 （原因・その他の状況）				
初期対応処置 （日時、対応者）				
対応処置 （日時、対応者）				
対応結果				
今後の考慮すべき事項				
通知・公表の概要				
その他				

※ 必要に応じて資料を添付する。
※ 保管期間　３年

別紙２

個人情報の漏えい等事故に関する是正処置報告書

「個人情報の漏えい等事故に関する是正処置報告書」は第９条に規定する再発防止のための処置に用いる。再発防止とは、個人情報の漏えい等の事故処置が終了した後、事故が生じた原因を分析し、その原因を取り除き、再発を防止するための活動をいう。

報告者:
作成日:　　年　　月　　日

<table>
<tr><td colspan="4">１．事故に対する是正処置内容</td></tr>
<tr><td>事故の種類</td><td colspan="3">☑緊急事態</td></tr>
<tr><td>事故の内容

【報告者】</td><td colspan="3"></td></tr>
<tr><td>事故の原因
【報告者】</td><td colspan="3"></td></tr>
<tr><td rowspan="3">是正処置計画
【期限を含む】

(対応部署)</td><td rowspan="3">上記処置は　月　日までに完結する。</td><td colspan="2">是正処置計画</td></tr>
<tr><td>当該部署部長　又は
個人情報保護部門管理者</td><td>会長</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="4">２．是正処置を講じて取り組んだ結果に対する評価</td></tr>
<tr><td>是正処置の結果
【是正処置
計画の実施】

(対応部署)</td><td colspan="3"></td></tr>
<tr><td rowspan="3">実施結果に対する有効性のレビュー
(報告者:個人情報保護管理者)</td><td rowspan="3">効果の確認は　月　日までに実施する。</td><td colspan="2">是正処置結果</td></tr>
<tr><td>個人情報保護管理者</td><td>会長</td></tr>
<tr><td></td><td></td></tr>
</table>

個人情報の開示等に関する細則

第１章　総　則

（目的）

第１条　本細則は、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）が、本協会の個人情報保護規程（以下「個人情報保護規程」という。）に基づき、本協会の本人から利用目的の通知、開示、訂正等、利用停止等(以下「開示等」という。)の請求及び保有個人データの公表等の求めがあった場合に、本協会が対応を適切に行うことを目的とする。

第２章　定義

（定義）

第２条　本細則で用いる用語の定義は、本協会の個人情報保護規程第２条に定めるものとする。

第３章　開示対応手続き

（保有個人データの開示方法）

第３条　本協会は、本人から本人が識別される保有個人データの電磁的記録による方法その他の個人情報保護委員会規則に定める方法により開示を求められた場合は、本人であることを確認のうえ、求められた方法により開示する。

ただし、当該方法による開示に多額の費用を要する場合その他当該方法による開示が困難である場合にあっては、書面による方法により、遅滞なく、当該保有個人データの開示を行う。

２　本人から開示の方法について特に指定がなく、本協会が提示した方法に対して異議を述べなかった場合は、本協会が提示した方法（書面による方法）で開示を行う。

３　第１項のただし書きに規定する方法による場合の判断は個人情報保護管理者が行う。

（開示等の請求に応じる方法）

第４条　本協会は、開示等の請求に応じる方法として、本人より、請求目的に応じていずれかの依頼書を提出させることとする。

（１）　個人情報保護規程第 16 条第２項による保有個人データの利用目的の通知の求めによる場合は、「個人データ利用目的通知依頼書」による。

（２）　個人情報保護規程第 17 条第１項(同条第４項において準用する場合を含む)の規定による保有個人データの開示の請求の場合は、「個人データ開示依頼書」による。

（３）　個人情報保護規程第 18 条第１項の規定による保有個人でデータの訂正等の請求若しくは第 19 条第１項、第２項若しくは第３項の規定による利用停止等の請求の場合は、「個人データ訂正等依頼書」による。

（手数料）

第５条　本協会は、個人情報保護規程第 22 条の規定による手数料の額は　1,000 円（消費税込み）とする。

（受付）

第６条　開示等の請求があった場合は総務部が一元的に受け付ける。

（開示等の請求受け付け手順）

第７条　開示等の請求に関する受付手順は以下のとおりとする。

（１）　開示等の請求に関する照会があった場合、照会を受けた者は総務部を案内する。

（２）　総務部は、開示等の請求に関する照会を受けた場合、「開示等請求手続」を案内する。案内にあたって、総務部は本人から開示等に当たって求められた方法がある場合には原則として求められた方法により開示することになるため、第３条に規定する開示方法について本人に説明し、開示方法について本人の同意を得るものとする。同意を得た開示方法は「個人データに関する開示等請求対応管理表」に記録する。

（３）　総務部は、開示等の請求手続に則った請求を受付した場合、必要書類、必要事項の確認、手数料の徴求（開示請求・利用目的の通知請求の場合のみ）を確認のうえ、請求を受領する。

（４）　総務部は、当該請求にかかる個人情報の内容を確認し、当該個人情報を所管する部を所管部として決定し、第２号に定める「個人データに関する開示等請求管理表」を引き継ぐものとする。

（５）　総務部は、請求内容を所管部に対して、必要に応じて個人情報の内容確認等を指示することができる。

（開示等の請求に対する対応方針の決定）

第８条　開示等に対する対応方針の決定は以下のとおり行う。

（１）　所管部は、総務部と協議のうえ、対応方針を決定し、決定した対応方針は「個人データに関する開示等請求対応管理表」に記録を残す。

（２）　対応方針は以下の基準に基づき決定する。

①　開示の請求

(a) 個人情報保護規程第 17 条第１項に該当する場合を除き、開示を行う方針とする。

(b) 前記、いずれかに該当する場合の判断は理事会が行う。

②　利用目的の通知の請求

(a) 個人情報保護規程第７条第４項に該当する場合を除き、通知を行う方針とする。

(b) 前記、いずれかに該当する場合の判断は理事会が行う。

③　内容の訂正等の請求

(a) 個人情報保護規程第 18 条第１項に規定する請求を受けた場合は、総務部は遅滞なく所管部に対して必要な調査を指示する。調査の結果、請求に理由があることが判明した場合は、訂正等に応じる方針とする。

(b) 保有個人データが誤りである旨の指摘が正しくない等により、訂正等を行わない場合の判断は個人情報保護管理者が行う。

④ 利用停止等の請求

(a) 個人情報保護規程第 19 条第１項及び第３項に規定する利用停止の請求を受けた場合は、総務部は遅滞なく所管部に対して必要な調査を指示する。調査の結果、請求に理由があることが判明した場合は、遅滞なく利用停止等に応じる方針とする。ただし、個人情報保護規程第 19 条第４項に該当する場合は、利用停止を行う必要はない。

(b) 前記、ただし書きの判断は理事会が行う。

⑤ 第三者への提供の停止の請求

(a) 個人情報保護規程第 19 条第２項及び第３項に規定する第三者提供の停止の請求を受けた場合は、総務部は遅滞なく所管部に対して必要な調査を指示する。調査の結果、請求に理由があることが判明した場合は、遅滞なく利用停止等若しくは第三者への提供の停止に応じる方針とする。ただし、個人情報保護規程第 19 条第４項に該当する場合は、利用停止等又は第三者への提供停止を行わない。

(b) 前記のただし書きの判断は理事会が行う。

（請求に対する対応の実施）

第９条　請求に対する対応は以下のとおり行う。

（１） 開示及び利用目的の通知についての請求に関して、全部若しくは一部について対応する方針とした場合、所管部は総務部に対し、開示対象の個人データ又は通知対象の利用目的を報告する。

（２） 訂正等、利用停止等、第三者への提供の停止についての請求に関して、全部若しくは一部について対応する方針とした場合、所管部は当該対応を実施し、対応が完了した後、対応内容を記載した書面を添付し、総務部に報告する。

（３） 第１号及び第２号の請求があった日から２週間以内に当該措置が完了しない場合、所管部は理由を付して総務部に報告し、善後策を協議する。

（請求者への通知）

第 10 条　請求者への通知は以下のとおり行う。

（１） 利用目的の通知の請求

① 利用目的の通知の請求があった場合には、総務部は所管部からの報告を受領後、本人通知書面を作成し、請求者に対して遅滞なく通知する。

② 利用目的の通知の請求に関して、保有個人データの利用目的を通知しない方針とした場合、総務部は本人通知書面を作成し、請求者に対して遅滞なく通知する。その際には、対応しない方針とした理由を説明するよう努めるものとする。

（２） 開示の請求

① 開示の請求に関して、全部若しくは一部について対応する方針とした場合、総務部は所管部からの報告を受領後、本人通知書面を作成し、請求者に対して遅滞なく通知する。なお、開示の請求に基づく個人データの通知方法は本人と合意した方法によって通知するものとする。

② 開示の請求に関して対応しない方針とした場合、当該保有個人データが存在しないとき、又は本人が請求した方法による開示が困難であるときは、総務部は本人通知書面を作成し、請求者に対して遅滞なく通知する。その際には、対応しない方針とした理由を説明するよう努めるものとする。

（３） 訂正等の請求

① 訂正等の請求に関して、全部若しくは一部について訂正等を行ったとき、総務部は所管部からの報告を受領後、訂正を行った内容を含む本人通知書面を作成し、請求者に対して遅滞なく通知する。

② 訂正等の請求に関して対応しない方針とした場合、総務部は本人通知書面を作成し、請求者に対して遅滞なく通知する。その際には、対応しない方針とした理由を説明するよう努めるものとする。

（４） 利用停止等又は第三者への提供の停止の請求

① 利用停止等又は第三者への提供の停止の請求に関して、全部若しくは一部について利用停止等又は第三者への提供を停止したとき、総務部は所管部からの報告を受領後、本人通知書面を作成し、本人に対して遅滞なく通知する。

② 利用停止等又は第三者への提供の停止の請求に関して、全部若しくは一部について利用停止等又は第三者への提供を停止しない方針とした場合、総務部は所管部からの報告を受領後、本人通知書面を作成し、本人に対して遅滞なく通知する。その際には、対応しない方針とした理由を説明するよう努めるものとする。

（５） 本人通知書面は本人限定受取郵便にて郵送する。

第４章　保有個人データの公表等

（保有個人データの公表等）

第 11 条　個人情報保護管理者は、本人より本協会が保有する個人データに関し、個人情報保護規程第 16 条に規定する事項について公表を求められた場合は、速やかに「保有個人データの公表等」の書面を本人に送付するものとする。

第５章　支部での適用

（支部での適用）

第 12 条　本細則を支部で適用する際には、支部における個人データ等の取扱いマニュアルに定めるものとする。

第６章　雑　則

（制定及び改廃）

第 13 条　本細則の制定及び改廃は、理事会の承認を得なければならない。

（附則）

本細則は、令和４年４月１日から施行する。

個人情報取扱いの外部委託細則

第１章　総　則

（目的）

第１条　本細則は、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）が個人情報を本協会以外の者（以下「外部事業者」という。）に取扱いを行なわせる場合に、個人情報保護規程第 11 条の規定に基づき、本協会が個人情報の取扱いの外部委託を適切に行うことを目的としている。

第２章　定義

（定義）

第２条　本細則で用いる用語の定義は、個人情報保護規程第２条に定めるものとする。

２　委託元とは、個人情報保護規程第２条第 15 項に定める委託を行う者をいう。

３　委託先とは、個人情報保護規程第２条第 15 項に定める委託を受ける者をいう。

（適用範囲）

第３条　本細則は、本協会の個人情報の取扱いを外部事業者に委託する場合に適用する。

２　前項における Software as a Service（SaaS）等の外部設備の利用が個人情報の取扱いの委託に該当するかどうかの判定にあたって、委託する業務の内容に応じて、別表１（委託の範疇等に関する経済産業省 Q&A(旧)、個人情報保護委員会 FAQ）を参照して、個人情報の取扱いの委託に該当するか否かを判断し、該当する場合は委託として適用する。

第３章　委託措置

（委託にあたって取るべき措置）

第４条　委託にあたっては、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい、滅失、毀損その他の個人データの安全確保に係る事案（以下「漏えい等」という。）が発生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、委託する事業の規模及び性質、個人データの取扱い状況等に起因するリスクに応じて、次に掲げる事項について必要かつ適切な措置を講じるものとする。

（１）適切な委託先の選定

（２）委託契約の締結

（３）委託先における個人データの取扱い状況の把握

（委託先選定基準）

第５条　個人データの取扱いを外部事業者に委託するにあたっては、個人情報保護規程第 11 条第１項の定めにより、十分な個人データの保護水準を満たしている委託先を選定することが求められることから、個人情報保護委員会による個人情報の保護に関する法律についてのガイドライン（通則編）「８（(別添）講ずべき安全管理措置の内容)」に沿って、個人データの安

全管理の分野に関して「個人情報管理体制に関するアンケート」(以下「アンケート」という。)及びサービスの持続性の分野に関して「個人情報委託先評価表」(以下「評価表」という。)を選定基準として定める。

2　アンケート及び評価表の策定は、個人情報保護管理者が行う。

3　アンケート及び評価表の項目は、以下の構成とする。

（1）　個人情報に関する公的認証の取得の有無又は国家資格による守秘義務の有無

（2）　個人情報管理体制について

① 個人情報の安全管理に係る基本方針の整備

② 個人データの取扱いに関する規律の整備

③ 組織的安全管理措置に係る取扱規程に基づく運用状況

④ 人的安全管理措置に係る取扱規程に基づく運用状況

⑤ 物理的安全管理措置に係る取扱規程に基づく運用状況

⑥ 技術的安全管理措置に係る取扱規程に基づく運用状況

⑦ 特定個人情報の取扱いに係る安全管理措置の運用状況

（3）　個人情報取扱委託先評価表

① 経営の健全性

② 工程の健全性

③ 安全性

4　個人情報保護管理者は委託先選定基準を適宜、見直すものとする。

第４章　委託先の監督

（適切な委託先の選定）

第６条　個人情報の取扱いを外部事業者に委託する場合の責任者（以下「委託責任者」という。）は、個人情報の取扱いを外部事業者に委託する前に、前条に定めるアンケート及び評価表により、委託先の調査を実施し、評価する。

2　委託先が委託可能な水準に達していると認められるためには、次の条件を満たさなければならない。

（1）　アンケート

①「チェック項目」のうち、１から３の設問の全てを満たすことを必須条件とする。

②「チェック項目」のうち、１から 18 までの設問に対して○の割合が７割を達成していること。

③ 特定個人情報の取扱いの委託の場合には、設問 19 から 27 までのすべてが○であること。

（2）　評価表

①　評価点平均が 2.0 以上あること。

3　前項（1）に規定するアンケートは委託先が個人情報に係る第三者認証を受けている場合には個人情報の保護水準を満たしているものとし、又は、業務を行うためには国が定めた資格が必要で、かつ法律により守秘義務を課されている者（弁護士、税理士、社会保険労務士等）は、それだけで選定基準を満たしていると評価でき、個別のチェックは必要としない。

4　第２項の評価の結果、委託可能な水準に達していると認められた場合、若しくは第３項に該当する場合は、個人情報保護管理者は理事会の承認を経て、当該外部事業者を個人情報取扱委託先として承認する。

5　第２項の評価の結果、委託可能な水準に達していないと認められた場合は、個人情報保護管理者は当該外部事業者を個人情報取扱委託先として承認しない。ただし、業務の都合上当該外部事業者を使用せざる得ない場合は、水準を満たすための暫定措置をとらせることで、リスクが許容できる範囲と判断できれば、理事会に上程し、期間を限定して特例承認を受けることができる。

6　前項の特例承認を受けた場合は、特例承認期間中に委託先が評価基準を満たすことができない場合は、期間満了時に委託契約を終了しなければならない。

評価基準を満たせた場合には、その時点で、第１項に規定する評価の再評価を実施し、改めて理事会の承認を経るとこととする。

（契約書等の締結）

第７条　前条第４項により、承認を受けた委託先に個人情報の取扱いを委託する場合には、個人情報保護管理者は委託契約の委託内容が利用目的の範囲内であることを確認したうえで、委託実施前に個人情報の取扱いに関する契約を締結するものとする。

2　契約は原則として「個人情報の取扱いに関する覚書（雛型）」を参照し、書面によって締結する。委託先が指定する個人情報に関する守秘義務契約書を求められた場合は、守秘義務契約書に含まれる事項が、下記第４項に規定する内容が含まれていれば、委託先の契約書を使用することも可能とする。

3　外部事業者に定型的業務を委託する場合、当該外部事業者が用意している約款等を吟味した結果、当該約款を遵守することにより委託する個人データの安全管理が図られると個人情報保護管理者が判断した場合には、当該定型的業務を委託することについて、必ずしも追加的に覚書を締結する必要はないものとする。ただし、その場合は約款を保存するものとする。

4　第１項に定める「個人情報の取扱いに関する覚書（雛型）」には、以下の事項を含んでいなければならない。

（１）委託者及び受託者の責任に関する事項
（２）個人情報の安全管理に関する事項
（３）再委託に関する事項
（４）個人情報の取扱状況に係る委託者への報告の内容及び頻度に関する事項
（５）契約内容が遵守されていることを委託者が確認できることに関する事項
（６）契約内容が遵守されなかった場合の措置に関する事項
（７）事件・事故が発生した場合の本協会・個人情報保護委員会への報告・連絡に関する事項

5　委託先における個人情報の漏えい等の報告に関する取り決め

前項の（７）において、委託先において個人情報保護委員会に報告しなければならない事態に該当する個人情報の漏えい等が発生した場合の個人情報保護委員会への報告について以下のいずれを適用するか、委託先との契約で明確にしておくものとする。

（１）委託元と委託先の双方が個人データを取り扱っていることとなるため、個人データの漏えい等が報告対象事態に該当する場合には、原則として委託元と委託先との双方が個人情報保護委員会に報告する義務をそれぞれが負う。（個人情報保護委員会ガイドライン 3-5-3-2）

（２）個人情報保護委員会に対する報告にあたって、委託元及び委託先が連名で報告することができることとされていることから、委託元が連名で報告する。（個人情報保護委員会

ガイドライン 3-5-3-2）

（３） 委託先は、報告義務を負っている委託元に当該事態が発生したことを通知したときは、委託先は個人情報保護委員会に対しての報告義務が免除されるため、通知を受けて委託元が個人情報保護委員会に速やかに報告する。（個人情報保護委員会ガイドライン 3-5-3-2）

（契約書等の保存）

第８条　前条の契約書等の書面又はこれに代わる記録は総務部で保管する。

２　前項の書面は個人情報の委託期間にわたって保存しなければならない。

（委託先の管理）

第９条　個人情報保護管理者は、委託契約の締結が終了の後、「委託業者リスト」に登録し、協会内に周知する。

２　委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託先を通じて再委託先にも本細則を適用するものとする。

３　再委託先が再々委託を行う場合以降も、前項と同様とする。

（委託先における個人データの取扱状況の把握）

第 10 条　個人情報保護管理者は、１年に１回、委託先において個人データがどのように取り扱われているかを把握するため、委託責任者に対して、個人データの取扱状況を報告させるものとする。

２　委託責任者は、前項の個人データの取扱状況を把握するため、本協会指定の委託に係る「個人データの安全管理措置等に関する報告書」を委託先から報告させ、個人情報保護管理者に提出する。報告内容としての合否の基準は本協会が要求する全ての項目が実施されていることとする。実施できていない項目があった場合には、当該委託先を所管する委託責任者は、委託先に対して３ヶ月以内での是正処置を施すよう指示するものとする。

是正期間中に是正処置の終了ができなかった場合は、原則として委託を終了する。ただし、理事会に報告し、リスクを受容できると理事会で判断された場合には、この限りでない。

３　当該業務を委託している担当者は、委託期間中、委託先における個人情報の取扱い状況に注意し、契約に違反し又は違反するおそれのあることを発見した場合は、直ちに、その旨を個人情報保護管理者に通知しなければならない。

４　個人情報保護管理者は、委託先において契約に違反し、又は違反するおそれのあることを発見した場合は、直ちに必要な措置を講じなければならない。

（安全管理措置等に関する報告書）

第11条 個人データの安全管理措置等に関する報告書

個人情報保護管理者は、前条第２項に規定する委託先の監督のために委託先から報告させる内容について、適切な報告事項を定めなければならない。

「報告内容」の項目は、以下のことが含まれていなければならない。

（１） 個人情報管理体制について

① 個人データの安全管理に係る基本方針・取扱規程等の整備

② 個人データの組織的安全管理措置

③ 個人データの人的安全管理措置
④ 個人データの物理的安全管理措置
⑤ 個人データの技術的安全管理措置
⑥ その他（受託業務固有の確認事項等）

（２） 特定個人情報の管理体制（特定個人情報の取扱いがある場合）
① 特定個人情報の物理的安全管理措置

２ 個人情報保護管理者は、報告書に含まれる報告内容を必要に応じて改定する。

（委託業者リストの最新化）

第 12 条 個人情報保護管理者は、第９条により委託先から報告を受け、個人データの取扱状況に関して問題がないと判断した場合は、委託業者リストを更新し、イントラネット上に掲出する。

第５章 支部での適用

（支部での適用）

第 13 条 本細則を支部で適用する際は、支部における個人データ等の取扱マニュアルに定めるものとする。

第６章 雑 則

（制定及び改廃）

第 14 条 本細則の制定及び改廃は、理事会の承認を得なければならない。

（附則）

本細則は、令和４年４月１日から施行する。

別表１　委託の範疇等に関する経産省 Q&A(旧)・個人情報保護委員会 FAQ

	質問	回答
選定	90 委託先において実施される個人データの安全管理措置が、委託する当該事業に応じて、少なくとも法律 20 条で求められる安全管理措置と同等であることを、合理的に確認するための方法として、どのような方法がありますか。	ガイドラインの安全管理措置として掲載されている事項等を参考にして、委託元は、委託先における個人データの安全管理措置の実施状況を確認するための**チェックリストをあらかじめ用意**し、委託先の選定時や、既存の委託契約の更新時に確認する方法が考えられる。 その他、**チェックリストを用いない場合**における委託先評価の一つとして、合理的、客観的な基準により公正な**第三者認証を得ている**こと等が考えられます。　2008.2.29
ホスティング等の判断	92 委託先が倉庫業、データセンター（**ハウジング、ホスティング**）等の事業者の場合で、預ける情報の中に個人データが含まれていることを**当該事業者に認識させることなく**預けることがあります。 この場合、当該事業者と契約を締結するときに、個人データの取扱いに関する条項を契約に盛り込む必要がありますか。	質問のケースにおいては、委託元が事前に当該個人データに安全管理措置を講じる（暗号化等の秘匿化等）ことになると考えますので、委託先との契約の中に個人データの取扱いに関する条項を盛り込む必要はありません。 ただし、**委託元は委託先を適切に選定する必要**があります。 2008.2.29
透明化	93 委託の有無、委託する事務の内容等を明らかにする等、委託処理の透明化を進めることが望ましいとありますが、どのような場面や方法で、どの程度行う必要がありますか。	プライバシーポリシーに盛り込む事や、取得の際に明らかにすることが考えられますが、例えば、委託先が多岐にわたり、事業の内容を個別に明らかにすることについて過度の負担が生じるような場面には、委託契約ごとではなく、類型化して事務の内容を明らかにするなど、実情に応じた対応が考えられます。 2010.4.1
監督	Ｑ４－８ 委託元は、委託先を監督するため、委託先に対する**定期的な立ち入り検査を実施する義務**はありますか。	Ａ４－８ 法第 22 条に基づく委託先の監督の一環として、委託先における個人データの取扱状況を把握することが必要であり、その手段として、必要に応じて個人データを**取り扱う場所に赴くことも考えられますが、これが義務付けられているわけではなく、**取扱いを委託する**個人データの内容や規模に応じて適切な方法（口頭による確認も含む。）**を講じれば足りるものと考えられます。

移送等	Ｑ５－26 **配送事業者、通信事業者等**の外部事業者を利用して、個人データを含むものを送る場合は、当該外部事業者に対して当該個人データの取扱いを委託（法第 23 条第５項第１号）しているものと考えられますか。	Ａ５－26 一般的に、外部事業者を利用して、個人情報データベース等に含まれる**相手の氏名、住所等宛に荷物等を送付する行為は、委託に該当すると解されます**。ただし、配送事業者を利用する場合、通常、当該配送事業者は配送を依頼された中身の 詳細については関知しないことから、当該配送事業者との間で特に中身の個人データの 取扱いについて合意があった場合等を除き、**当該個人データに関しては取扱いの委託をしているものではないものと解されます**。 また、通信事業者による通信手段を利用する場合も、当該通信事業者は、通常、通信手 段を提供しているにすぎず、通信を依頼された中身の詳細について関知するものでないことから、**同様に通信の対象である個人データについてはその取扱いを委託しているも のではないものと解されます。** なお、いずれの場合も、外部事業者を利用する個人情報取扱事業者には、安全管理措置を講ずる義務が課せられているため、中身の個人データが漏えい等しないよう、**適切な外部事業者の選択、安全な配送方法の指定等の措置を講ずる必要**があります。
DM委託	Ｑ５－25 **ダイレクトメールの発送業務を業者に委託**する場合、ダイレクトメールの発送業務の委託に伴い、ダイレクトメールの送付先である顧客の氏名や住所等を本人の同意なくこの業者に伝えることはできますか。	Ａ５－25 個人情報取扱事業者が、その利用目的の達成に必要な範囲内において、ダイレクトメールの発送業務を業者に「委託」（法第 23 条第５項第１号）する場合には、顧客の氏名や住所等をダイレクトメールの発送業者に伝えても第三者提供の制限に違反することにはなりません。ただし、**委託者は、委託先を監督**する義務があります（法第 22 条）。
クラウド	Ｑ３－13 クラウドサービスが番号法上の委託に該当しない場合、クラウドサービスを利用する事業者が、クラウドサービスを提供する事業者に対して監督を行う義務は課されないと考えてよいですか。	Ａ３－13 クラウドサービスが番号法上の委託に該当しない場合、委託先の監督義務は課されませんが、クラウドサービスを利用する事業者は、自ら果たすべき安全管理措置の一環として、クラウドサービス事業者内にあるデータについて、適切な安全管理措置を講ずる必要があります。

クラウド	Ｑ５－33 個人情報取扱事業者が、**個人データを含む電子データを取り扱う情報システムに関して、クラウドサービス契約のように外部の事業者を活用している場合**、個人データを第三者に提供したものとして、「本人の同意」（法第 23 条第１項柱書）を得る必要がありますか。または、「個人データの取扱いの全部又は一部を委託」（法第 23 条第５項第１号）しているものとして、法第 22 条に基づきクラウドサービス事業者を監督する必要がありますか。	Ａ５－33 クラウドサービスには多種多様な形態がありますが、クラウドサービスの利用が、本人の同意が必要な第三者提供（法第 23 条第１項）又は委託（法第 23 条第５項第１号）に該当するかどうかは、保存している電子データに個人データが含まれているかどうかではなく、**クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準**となります。 当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はありません。 また、上述の場合は、個人データを提供したことにならないため、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供される場合」（法第 23 条第５項第１号）にも該当せず、法第 22 条に基づきクラウドサービス事業者を監督する義務はありません。 当該クラウドサービス提供事業者が当該個人データを取り扱わないこととなっている場合の個人情報取扱事業者の安全管理措置の考え方についてはＱ５－34 参照。 当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます。なお、法第 24 条との関係についてはＱ９－５参照。
安全管理措置	Ｑ５－34 クラウドサービスの利用が、法第 23 条の**「提供」に該当しない場合、**クラウドサービスを利用する事業者は、クラウドサービスを提供する事業者に対して監督を行う義務は課されないと考えてよいですか。	Ａ５－34 クラウドサービスの利用が、法第 23 条の**「提供」に該当しない場合、法第 22 条に基づく委託先の監督義務は課されません**が（Ｑ５－33 参照）、クラウドサービスを利用する事業者は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要があります。

保守	Ｑ５－35 個人データを含む電子データを取り扱う情報システム（機器を含む。）の保守の全部又は一部に外部の事業者を活用している場合、個人データを第三者に提供したものとして、「本人の同意」（法第 23 条第１項柱書）を得る必要がありますか。または、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供」（法第 23 条第５項第１号）しているものとして、法第 22 条に基づき当該事業者を監督する必要がありますか。	Ａ５－35 当該保守サービスを提供する事業者（以下本項において「保守サービス事業者」という。）がサービス内容の全部又は一部として情報システム内の個人データを取り扱うこととなっている場合には、個人データを提供したことになり、本人の同意を得るか、又は、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供」（法第 23 条第５項第１号）しているものとして、**法第 22 条に基づき当該保守サービス事業者を監督**する必要があります。 （例） ○ 個人データを用いて情報システムの不具合を再現させ検証する場合 ○個人データをキーワードとして情報を抽出する場合 一方、単純なハードウェア・ソフトウェア保守サービスのみを行う場合で、**契約条項によって当該保守サービス事業者が個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等には、個人データの提供に該当しません。** （例） ○システム修正パッチやマルウェア対策のためのデータを配布し、適用する場合 ○保守サービスの作業中に個人データが閲覧可能となる場合であっても、個人データの取得（閲覧するにとどまらず、これを記録・印刷等すること等をいう。）を防止するための措置が講じられている場合 ○保守サービスの受付時等に個人データが保存されていることを知らされていない場合であって、保守サービス中に個人データが保存されていることが分かった場合であっても、個人データの取得を防止するための措置が講じられている場合 ○不具合の生じた機器等を交換若しくは廃棄又は機器等を再利用するために初期化する場合等であって、機器等に保存されている個人データを取り扱わないことが契約等で明確化されており、取扱いを防止するためのアクセス

		制御等の措置が講じられている場合 ○不具合の生じたソフトウェアの解析をするためにメモリダンプの解析をする場合であって、メモリダンプ内の個人データを再現しないこと等が契約等で明確化されており、再現等を防止するための措置が講じられている場合 ○個人データのバックアップの取得又は復元を行う場合であって、バックアップデータ内の当該個人データを取り扱わないことが契約等で明確化されており、取扱いを防止するためのアクセス制御等の措置が講じられている場合
守秘義務契約締結	Ｑ４－10 外部事業者に定型的業務を委託する場合、必ず、当該外部事業者が用意している約款等に加えて、自己の社内内規を遵守するよう求める覚書を追加的に締結する等の対応が必要となりますか。	Ａ４－10 委託する事業の規模及び性質、個人データの取扱状況などに起因するリスクに応じて行うべきものと考えられます。当該約款を吟味した結果、当該約款を遵守することにより当該個人データの安全管理が図られると判断した場合には、当該定型的業務を委託することについて、必ずしも追加的に覚書を締結する必要まではないと考えられます。

個人情報保護に関する内部監査実施細則

第１章　総　則

（目的）

第１条　本細則は、公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）が個人情報の内部監査を行うにあたり、個人情報保護規程第32条に基づき、適切に内部監査を実施するための規律を定めたものである。

（用語の定義）

第２条　本細則で用いる用語の定義は、本協会の個人情報保護規程第２条に定めるものの他、以下に定めるものを含むものとする。

（１）　内部監査員（以下「監査員」という。）とは、個人情報保護に関する監査業務を担当する職員等をいう。

（２）　要求事項とは、個人情報の保護に関する法律及び本協会の個人情報保護規程、特定個人情報等取扱規程、情報システム管理規程、個人情報の安全管理に関する取扱細則、個人情報取扱いの外部委託細則、個人情報の開示等に関する細則、個人情報事故細則、個人情報保護に関する内部監査実施細則（以下「規程等」という。）により求められた事項をいう。又は、明示されている、通常暗黙のうちに了解されている又は義務として要求されているニーズ又は期待をいう。

（３）指摘事項とは、監査の結果、問題があると監査員が判断した事項をいう。

指摘事項には、不適合と観察事項があり、それぞれ以下のことをいう。

①　不適合とは、 要求事項を満たしていないことをいう。

例）

・ 規程類が法律等の改正に対応していない
・ 規程等に規定されている事項が実施されていない
・ 法令等遵守義務を果たしていない
・ 計画されたことが実施されていない 等

②　観察事項とは 不適合ではないが改善した方が良いこととして監査員が意見として表明した事項をいう。

例）

・ このままだと将来不適合になるおそれがあると思われる事項
・ 改善すればより安全・信頼性が高まると思われる事項 等

第２章　内部監査計画

（基本計画の策定と承認）

第３条　監査責任者は、原則として年１回、「個人情報保護に関する監査基本計画書」（以下「基本計画書」という。）を作成の上、個人情報保護管理者に提出し、会長の承認を得なけ

ればならない。

2　会長又は個人情報保護管理者が必要と認めた場合、第７条に定める「個人情報に関する内部監査通知書」をもって臨時の計画書とし、会長及び個人情報保護管理者の承認を得なければならない。

（適用範囲）

第４条　基本計画書に含める監査の適用範囲は、個人情報保護規程第３条が適用される範囲と同じものとする。

（基本計画書の内容）

第５条　基本計画書は、規程等の適合状況と、運用状況について計画するものとする。

2　基本計画書は、監査の実施時期、監査の目的、監査対象、監査チームリーダー、実施方法、実施内容、実施予定日等について計画するものとする。

第３章　内部監査の実施

（実施体制）

第６条　監査責任者は、内部監査に係る全てを主管する。

2　監査責任者は、監査員による内部監査の体制（以下「監査チーム」という。）を編成する。

3　監査責任者は、監査員自身が所属する部門の内部監査をしないよう体制を編成する。

4　監査チームのリーダーは、一人で内部監査する場合は本人がリーダーとなり、複数で内部監査する場合は監査チームを構成する監査員の一人がリーダーとなる。

（内部監査の実施準備）

第７条　監査責任者は、監査予定日の90日前までに、当該年度の監査員の候補者を選任し、当該候補者が所属する部門責任者の同意を得た上で、監査員として指名するものとする。

2　監査員は、内部監査の準備として、監査を担当する部門（以下「被監査部門」という。）の基本計画書及び個人情報に係る関係資料の内容を事前に確認するとともに、前年度の内部監査の結果等を踏まえて、被監査部門の「個人情報保護に関する監査個別計画書（以下「監査個別計画書」という。）」を作成する。

監査個別計画書は以下２つの計画書によって構成される。

①　個人情報保護に関する内部監査通知書

②　個人情報保護内部監査チェックリスト

3　監査員は、前項で作成した監査個別計画書を監査予定日の４週間前までに監査責任者に提出する。

4　監査責任者は、監査員が作成した監査個別計画書を確認し、承認する。

（内部監査の通知）

第８条　監査責任者は、監査予定日の２週間前までに被監査部門の責任者に対し、「個人情報保護に関する内部監査通知書」を提出する。

2　前項にかかわらず、本協会の個人情報保護規程第24条第1項に規定する事故、又は第29条第1項を担当する者から重大な相談等として報告があった場合は、事前の通知なしに、監査を実施することができる。

（内部監査の方法）

第９条　内部監査は、実地監査により行うものとする。ただし、監査責任者の判断により書面による監査を以って実地監査に替えることができる。

2　監査員は自ら所属する部門の監査を行ってはならない。

3　内部監査で発見された事項のうち、不適合とした事項は、監査終了時に被監査部門の責任者に説明するものとする。

第４章　監査結果の報告

（監査結果の報告）

第10条　監査員は、監査終了後、遅滞なく個人情報保護に関する監査個別報告書（以下「監査個別報告書」という。）を作成しなければならない。

2　監査個別報告書に監査実施中に発見した指摘事項を記載し、監査責任者に提出するものとする。

3　監査責任者は、監査個別報告書の内容を検証し、当該部門の責任者に監査個別報告書の内容について確認を得た上で、「個人情報保護に関する監査報告書」（以下「監査報告書」という。）を作成し、監査個別報告書を添えて、個人情報保護管理者に提出し、会長に報告する。

第５章　改善活動

（改善勧告）

第11条　会長及び個人情報保護管理者は、報告された監査報告書に重大な不適合が含まれていた場合には、当該被監査部門に対して改善計画書の提出を勧告する。

（改善計画書）

第12条　改善計画書の提出を勧告された被監査部門は、改善計画を策定し、会長及び個人情報保護管理者の承認を受け、改善措置に従って改善活動を行う。

第６章　監査報告と処置

（関係部門への通知と処置）

第13条　監査責任者は、内部監査の結果を個人情報保護管理者、被監査部門及び関係する場合は利害関係者に通知しなければならない。

2　監査結果に不適合がある場合には、当該被監査部門は不適合を解消するための処置を行うものとする。

3　監査結果に観察事項がある場合には、当該被監査部門は指摘内容を検証し、改善するか、現

状維持で行くのかを、リスク及び効果を勘案して、部門としての結論を得る。改善すると結論づけた場合には、自部門で改善する。この場合、改善が終了したことの報告は都度に報告するのではなく、次回の内部監査時に報告するものとする。

4　監査責任者は、第２項に該当した場合には、一定の期間をおいて、当該被監査部門における改善効果の確認を行うものとする。一定の期間は不適合の状態、種類、改善効果の現れるまでの期間等により異なることから、監査責任者の判断に依拠する。ただし、報告を受けて６ヶ月を超えない期間とする。

5　監査責任者は、改善効果の確認結果を会長及び個人情報保護管理者に報告しなければならない。

第７章　内部監査関係書類の整理及び保管

（内部監査関係書類の整理）

第14条　監査責任者は、内部監査終了後、速やかに関係資料を整理し、内部監査資料ファイルを作成しなければならない。

（内部監査関係書類の保管）

第15条　内部監査資料ファイルは、実施時期別、被監査部門別に整理し、保管しなければならない。

第８章　支部での適用

（支部での適用）

第 16 条　本細則を支部で適用する際は、支部における個人データ等の取扱マニュアルに定めるものとする。

第９章　その他

（改廃）

第 17 条　本実施細則の制定及び改廃は、理事会の承認を得なければならない。

（附則）

本実施細則は令和４年４月１日から施行する。

（附則）

本実施細則は令和８年２月 13 日から施行する。

公益社団法人 日本医業経営コンサルタント協会における個人情報保護に対する基本方針

（公社）日本医業経営コンサルタント協会
会　長　　川　原　丈　貴

１．基本方針

当協会は、個人情報保護に対する基本方針を定めるとともに、個人情報保護に必要な規則の制定および管理体制の確立などを内容とした個人情報保護実践遵守計画を策定し、会員およびすべての職員等に周知させ、個人情報の適切な保護に努める。

２．組織活動

当協会は、基本方針を具体化するため以下の活動を行う。

（１） 会員およびすべての職員等は、個人情報保護に関する法令および関連する規範を遵守する。

（２） 個人情報保護管理者を選任し、実践遵守計画の策定と実施および運用に関する責任と権限を与え、業務を遂行させる。

（３） 監査責任者を選任し、個人情報の状況について、定期的に監査を実施する。

（４） 実践遵守計画は継続的に改善する。

３．個人情報の取扱い

当協会は、個人情報を保護するために、以下の方針にしたがって個人情報を取り扱う。

（１） 個人情報の収集・利用・提供

当協会は、個人情報の収集にあたり、個人情報提供者（会員・研修受講者など）に対し収集目的を明らかにし、収集した個人情報の利用･提供範囲を限定し、適切に取り扱う。

（２） 権利の尊重

当協会は、個人情報に関する情報主体の権利を尊重し、情報主体から自己の個人情報に対し、開示、訂正、削除を求められたときは、合理的な期間、妥当な範囲内でこれに応じる。

（３） 安全対策の実施

当協会は、個人情報への不正アクセス、個人情報の紛失、破壊、改ざんおよび漏洩などが起こらないよう、予防ならびに是正に関する適切な措置を講じる。

注：用語の定義については、「個人情報保護基本規程」を参照のこと。

以上

令和４年６月 27 日現在

特定個人情報等の適正な取扱いについての基本方針

公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の適正な取扱いについて以下の方針で運用し、代表者、職員等に周知し徹底を図ります。

１．関係法令・ガイドライン等の遵守

本協会の関係者及び職員等の特定個人情報等を取得、保管、利用、提供又は廃棄する際は「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律」及び関連法令（以下、「関係法令等」という。）を遵守し、本協会が定めた取扱規程に従い適切に取り扱います。

２．利用目的

本協会は、特定個人情報等を以下の利用目的の範囲内で取り扱います。

（１）本協会の関係者に係る源泉徴収事務
（２）職員等に係る源泉徴収事務、社会保険関係事務及び労働保険関係事務
（３）前各号のほか、関係法令において特定個人情報等を用いると定められた事務
（４）前各号の事務に付随して行う行政機関への届け出事務

３．安全管理措置に関する対応

（１）特定個人情報等の漏えい、滅失又は毀損の防止等、特定個人情報等の事務取扱における責任体制を明確にするため「特定個人情報等取扱規程」を定め、必要かつ適切な安全管理措置を講じます。
（２）職員等に特定個人情報等を取り扱わせるに当たり、当該職員への定期的な研修を実施するとともに、必要かつ適切な監督を行います。
（３）特定個人情報ファイルを取り扱う情報システムを管理する管理区域及び特定個人情報等の取扱事務を実施する取扱区域を設けます。
（４）特定個人情報等を取扱う機器や電子媒体及び書類に対して、適切な盗難防止対策を講じます。
（５）特定個人情報へアクセスすることができる取扱事務担当者と情報の範囲を適切に設定するとともに、特定個人情報ファイルを取り扱うＰＣ，サーバー等への不正なアクセスを防止する措置を講じます。
（６）特定個人情報等を取り扱う事務の全部又は一部を委託する場合、委託先（再委託先を含む。）において、関係法令等に基づき本協会が採るべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行います。
（７）「２．利用目的」で定めた目的の範囲内で特定個人情報等を利用、収集及び保管し、当該目的の範囲外での利用、収集及び保管を防止するための措置を講じます。

４．質問及び苦情処理等の窓口

特定個人情報等の取扱いに関するお問合せは、以下宛てにご連絡ください。

所 在 地：東京都千代田区三番町９－１５　ホスピタルプラザビル５階
　　公益社団法人日本医業経営コンサルタント協会
担当部署：総務部総務課
電話番号：０３－５２７５－６９９６
電子メール：somu@jahmc.or.jp

令和４年６月 27 日現在

令和７年 12 月５日改定

プライバシーポリシー

公益社団法人日本医業経営コンサルタント協会（以下、「本協会」といいます。）は、個人情報を保護することが本協会定款第４条に定める事業活動の基本であるとともに、社会的責務であると認識し、以下の個人情報保護方針を制定し、確実な履行に努めるものとします。

１．法令等の遵守
本協会は、個人情報の保護に関する関係法令、国が定める指針その他の規範及び本協会における個人情報保護規程等を遵守いたします。

２．個人情報の利用目的
本協会は、ご提供いただいた個人情報を、資格認定事業（資格試験・検定の実施）、人材育成事業（継続研修、セミナー、地域研究交流会、学会活動等）、調査研究・提言活動事業（調査研究、提言、経営相談等）、相談・助言事業（医療勤務環境改善支援、持分なし医療法人移行等）、共通事業（機関誌発行、医業経営コンサルタントの紹介等）、共益事業（広報活動、会員管理等）（以下、「本協会の事業」といいます。）のため、以下の目的で利用いたします。
（１）本協会の事業のための運営、管理、連絡及び関連情報のご提供
（２）本協会の事業における、サービス提供及びサービスのご案内
（３）本協会が発行する書籍の販売
（４）お問い合せへの対応及びお問い合せに関連し、事後に接触をとる必要が発生した場合の連絡
（５）本協会の事業の改善及び新規事業の実施
（６）官公庁・行政機関への届出・報告
（７）その他本協会の運営に必要な範囲内での利用

上記の利用目的を変更する場合は、あらかじめ利用目的を通知、又は公表いたします。

３．個人データの第三者への提供
本協会は、以下の各号に定める場合を除き、あらかじめ本人の同意を得ることなく、個人データを本協会以外の第三者に開示・提供いたしません。
ただし、本協会が保有及び管理する個人データの取扱いを第三者に委託する場合若しくは特定の第三者と個人データを共同利用させていただく場合があります。そのときは委託先又は共同利用先での個人データの取扱いを本協会と同等以上の安全管理の確保に

努めます。
（１）法令に基づく場合
（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
（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

４．個人データに関する管理体制
（１）本協会は、個人データの利用目的の達成に必要な範囲内で正確かつ最新の内容に保つとともに、利用する必要が無くなったときは、当該データを遅滞なく消去するよう努めます。
（２）本協会は、取得した個人データへの不正アクセス、漏えい、滅失又は毀損等のリスクに対して適切な予防措置及び取得した情報の適切な管理のために必要な措置を講じ、改善が必要とされた場合には速やかに是正いたします。

５．個人情報の開示、訂正等及び利用停止等
本協会は、個人情報について本人から開示・訂正等・利用停止等の要求があった場合には、適切な方法で本人確認を行い速やかに対応いたします。
ただし、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、本協会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、他の法令に違反することとなる場合は、この限りではありません。

６．相談・苦情対応
本協会は、個人情報の取扱いに関する相談・苦情等に誠実に対応いたします。

個人情報保護に関するお問合せ窓口
公益社団法人日本医業経営コンサルタント協会
総務部総務課
〒102-0075　東京都千代田区三番町 9-15
ホスピタルプラザビル 5 階
TEL.03-5275-6996　FAX.03-5275-6991
E-メール: info@jahmc.or.jp

公益社団法人日本医業経営コンサルタント協会
会長　川原　丈貴

令和 4 年 5 月 20 日制定
最終改定日：令和 7 年 12 月 5 日

以下、リンクページ

個人情報の取扱いについての重要事項

公益社団法人日本医業経営コンサルタント協会

１．クッキー（Cookie）等の利用

公益社団法人日本医業経営コンサルタント協会（以下、「本協会」といいます。）のホームページ（以下、「当サイト」といいます。）は、当サイト利用者のコンピュータの記憶装置に、「クッキー」と呼ばれるテキストファイルを送付し、保存・利用させていただくことがあります。クッキーの利用目的は、当サイト利用者のサービスログイン時の必要情報を自動入力することや、興味をお持ちであろう分野のコンテンツを表示するなどの利便性向上のために使用します。

なお、当サイト利用者は、「クッキー」を受け取る前にブラウザが警告を出すように設定しておくことにより、当サイト利用者の判断で「クッキー」を受け取ることを拒否できますが、当サイトの機能又は本サービスがご利用になれない場合があります。

また、当サイトでは、ウェブサイト又はアプリケーションを改善する目的で Google Analytics を利用し、それに伴いかかる目的で当サイト利用者の情報を利用しています。Google Analytics は、クッキーを利用して当サイト利用者の情報を収集します。Google Analytics の利用規約及びプライバシーポリシーに関する説明については、以下の Google Analytics のサイトをご覧ください。

・Google のサービスを使用するサイトやアプリから収集した情報の Google による使用
https://policies.google.com/technologies/partner-sites
・Google アナリティクス　オプトアウト　ブラウザ　アドオン
https://tools.google.com/dlpage/gaoptout?hl=jp
・Google アナリティクスの広告向け機能について
https://support.google.com/analytics/answer/3450482?hl=ja

２．個人情報の第三者提供について
本協会は、以下の各号に規定する個人情報を本人の同意を得て、第三者に公開又は提供いたします。
（１）認定登録 医業経営コンサルタント名簿を公開
（２）医業経営コンサルタント一次試験合格者及び二次試験合格者を公開
（３）コンサルタント無料相談コーナーに相談内容を公開
（４）相談内容を相談者が指定した認定登録 医業経営コンサルタントに提供
（５）当協会に寄附をいただいた方を公開
（６）役員等の氏名等を公開及び行政機関等への提供

なお、以下の各号に定める場合を除き、あらかじめ本人の同意を得ることなく、本人より取得した個人データを本協会以外の第三者に提供することはありません。
（１）法令に基づく場合
（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な場合
（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
（５）本協会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ことに伴って当該個人データが提供される場合
（６）合併その他の事由による事業の承継に伴って当該個人データが提供される場合
（７）特定の者との間で共同利用される個人データが当該特定の者に提供される場合

３．委託
本協会は、利用目的の達成に必要な範囲内において、個人情報の一部又は全部の取扱いを本協会外の者に委託する場合があります。委託にあたっては、委託先選定基準に基づく適切な委託先の選定、個人情報に関する守秘義務契約の締結、委託先における個人データの取扱い状況の把握等、個人情報保護ガイドラインで求められている規範に基づき、必要かつ適切な措置及び監督を行います。
本協会において、外部の者に個人情報を取り扱わせる場合としては、概ね、以下の事項が考えられます。
・本協会内の情報管理システム開発・保守を第三者に委託する場合

・試験・研修等の協会事業の一部を第三者に委託する場合
・会員に対する通信や刊行物の配送を委託する場合
・データを保管する場合

４．個人情報の共同利用
本協会は、本協会並びに連携する組織と会員等の個人情報に関して共同利用させていただく場合があります。
共同利用をさせていだたく場合には、事前に本協会ホームページ又は書面で下記について通知するか、又は公表させていただきます。
（１）共同利用する旨
（２）共同利用される個人データの項目
（３）共同して利用する者の範囲
（４）利用する者の利用目的
（５）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、住所並びに会長名

５．保有データの適正な取扱いの確保
（１）社内規範の制定
本協会は、個人情報保護方針実施のため個人情報保護に関する規定を定めること等により個人情報の適切な取扱いについて、本協会の役員及び職員等に周知徹底して実施させ、また適時に実施状況を監査する等、必要な改善に努めてまいります。
（２）安全管理措置の実施
本協会は、取得した個人情報への不正アクセス、漏えい、滅失又は毀損等のリスクに対して適切な予防措置及び取得した情報の適切な管理のために必要な措置を講じ、改善が必要とされた場合には速やかに是正いたします。
（３）安全管理のために講じた措置
【基本方針策定】
個人データの適正な取扱いの確保のため関係法令・ガイドの遵守、苦情・相談窓口等についての基本方針を策定
【個人データの取扱いに係る規律の整備】
　個人データの取得、利用、提供、保存、削除、廃棄等を行う場合の安全管理措置を個人データ等の取扱いマニュアルとして整備
【組織的安全管理措置】
　整備した取扱いマニュアルに従って個人データの取扱い状況について、定期的に自己点検を実施するとともに、内部監査を実施
【人的安全管理措置】

個人データについての秘密保持に関する契約を締結し、定期的な教育の実施

【物理的安全管理】

個人データを取扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが紛失又は公表されないよう措置を実施

【技術的安全管理】

個人データを取扱う情報システムに、外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入

【外的環境の把握】

外国の事業者が提供するクラウドサービスを利用する場合など、外国において個人データを取り扱う場合には、当該外国における個人情報の保護に関する制度を把握したうえで安全管理措置を実施

６．開示等の求めに応じる手続

・本協会は、個人情報に関する本人からのお問合わせに対応するための窓口を設置いたします。

・当該窓口では、本協会が管理する保有個人データのうち本人ご自身の個人情報について、開示・訂正等・利用停止等（以下「開示等」といいます。）の求めに対応いたします。

・開示等の求めに際し、本人確認のために運転免許証、パスポート等の公的書類のコピーをご提供いただく場合がありますので、あらかじめご了承ください。

・開示等のお求めは、「個人情報保護に関するお問合せ窓口」にご連絡ください。受付け次第、開示等の手続きに関する「開示等請求手続書」等請求に必要な書類をお送りいたします。

・開示等の求めの対応にあたっては、手数料（1,000 円税込み）及び郵送料等の実費を申し受けることがあります。

公益社団法人日本医業経営コンサルタント協会

個人情報の取扱いについて

公益社団法人日本医業経営コンサルタント協会
会長　川原　丈貴

【個人情報の利用目的と第三者提供について】

１．個人情報の利用目的

公益社団法人日本医業経営コンサルタント協会（以下「本協会」といいます。）では、個人情報を以下の利用目的の範囲で使用します。

１）会員情報は各種連絡等、協会活動のために使用します。
２）厚生労働省・自治体等の要請に基づいて、会員情報を提供する場合があります。この場合は、その都度会員の意向を確認します。
３）本人の承諾を得た会員について会員名簿（ホームページ含む）を作成し、本協会の広報活動を目的に第三者に提供する場合があります。
４）医業経営コンサルタント指定認定講座・一次試験・二次試験・継続研修の受講者・講師等の情報は、当該事業の運営に使用します。
５）上記４）以外のセミナー等の受講者・講師等の情報は、当該セミナーの運営に使用します。
６）上記４）、５）の会員以外の方について、継続研修等の案内や本協会活動に関する案内を送付する場合があります。
７）個人情報保護法施行前に作成された会員名簿は、会員活動のみに使用し、会員各自が適切に管理します。

２．利用及び提供の制限

本協会では、以下の場合を除き、上記１で明示した利用目的以外の使用及び第三者提供を行いません。

１）会員・受講者等、当該本人の同意がある場合。
２）不正アクセス、脅迫等外部要因による違法行為が発生した際の原因究明及び対策を必要とする場合。

３．委託

本協会では、利用目的の達成に必要な範囲内において、個人情報の一部又は全部の取扱いを協会外の者に取扱わせる場合があります。委託にあたっては、個人情報の取扱い状況の評価選定、個人情報に係る守秘義務契約の締結、個人情報の適切な安全管理措置の実施、委託期間中の管理状況の報告等、個人情報保護ガイドラインで求められている規範に基づき、必要かつ適切な監督を行います。

【会員自身に関する情報の変更・訂正・削除】

会員本人から本協会に所定の書類「個人正会員名簿記載事項変更届」等を提出することにより、本協会の登録内容の変更・訂正・削除を行います。

【個人情報の「開示等の求め」に応じる手続き】

本協会が保有している個人データについて、本人又はその代理人様からの開示、訂正等、利用停止等の求めがあった場合に、合理的期間及び範囲で対応させていただきます。

開示等の求めに応じる窓口は、下記個人情報相談窓口となります。

【個人情報相談窓口】

上記方針に基づき、会員情報の機密保持・管理と運用を行うにあたり、下記の連絡先を設けています。

■個人情報保護管理者：事務局長
■個人情報相談窓口　：総務部総務課（連絡先電話番号：03-5275-6996）

令和４年６月 27 日現在

役員等の個人情報の取扱いについて

公益社団法人日本医業経営コンサルタント協会
会長　川原　丈貴

【個人情報の利用目的と第三者提供について】

１．個人情報の利用目的

公益社団法人日本医業経営コンサルタント協会（以下「本協会」という。）では、役員・委員・室長等（以下「役員等」という。）の個人情報を以下の利用目的の範囲で使用します。

１）役員等の個人情報は協会活動、広報活動及び各種連絡のために使用するとともに、対外的な情報発信媒体において使用します。
２）法律に基づき、内閣府に対して役員等の氏名・住所等を報告するために使用します。
３）役員の登記のために氏名等を法務局に提供し、不特定多数の者が閲覧可能とするために使用します。
４）役員選任の際の立候補者・当選者の個人情報について、当該選挙の運営に使用します。
５）本協会で作成される議事録について、事務局に備え、一定期間、閲覧できる状態で維持するために使用します。
６）前号議事録について、会員専用ホームページにおいて公表する際に使用します。
７）厚生労働省・自治体等の要請に基づいて、役員情報を提供する場合があります。

２．利用及び提供の制限

１）本協会では、第１項で明示した利用目的以外の利用を行いません。
２）本協会では、役員等が第１項で明示した利用目的及び第三者提供についてご同意いただいたうえで、役員等にご就任いただいたものとして取り扱います。
３）本協会では、役員等の個人情報を第１項で明示した第三者以外に提供する場合は、事前に当該役員等の同意を得るようにいたします。

３．提供されるデータの項目・提供方法

本協会では、第１項で明示した利用目的により、それぞれ当該第三者に提供される個人データは、住所、氏名、生年月日、経歴等であり、紙媒体又は電子媒体で提供いたします。

４．第三者提供の停止等

役員等ご本人から当該ご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旨の請求があった場合には速やかに応じます。

ただし、法的に提出義務がある場合、若しくは当協会としての各種規程等で公表義務が定められている場合、第三者提供の停止に応じられない場合がございます。

【個人情報相談窓口】

上記方針に基づき、役員等の個人情報の機密保持・管理・運用を行うとともに、個人情報に関するご相談等に応じるため、下記の連絡先を設けています。

また、その他詳細につきましては、本協会の関係規定をご参照ください。

■個人情報保護管理者: 事務局長
■個人情報相談窓口　: 総務部総務課（連絡先電話番号：03-5275-6996）

令和４年６月 27 日現在