一般社団法人大分県医師会

マ イ ナ ン バ ー 関 連 規 程 集

〔文 書 名〕

特定個人情報等の適正な取り扱いに関する基本方針

一般社団法人大分県医師会（以下「本会」といいます。）は、個人番号および特定個人情報（以下「特定個人情報等」といいます。）の適正な取り扱いの確保に取り組むために、取引先様及び本会の従業員等の特定個人情報等の保護を重視し、「特定個人情報の適正な取り扱いに関する基本方針」を以下のとおり定め、本会のすべての役職員に周知し、徹底を図ります。

１．特定個人情報の適正な取り扱い

本会は、取引先及び本会の従業員等（以下「本人」といいます。）の特定個人情報等を取得、保管、利用、提供または廃棄するにあたって、本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 雇用保険法に関する資格取得、資格喪失、給付等の事務手続きに使用するため。
② 労働者災害補償保険法に関する給付、社会復帰促進事業等の事務手続きに使用するため。
③ 健康保険法、船員保険法、国民健康保険法、高齢者の医療の確保に関する法律に関する資格取得、資格喪失、給付等の事務手続きに使用するため。
④ 厚生年金保険法に関する資格取得、資格喪失、給付等の事務手続きに使用すため。
⑤ 国家公務員共済組合法、地方公務員等共済組合法、私立学校教職員共済法に関する事務手続きに使用するため。
⑥ 確定給付企業年金法、確定拠出年金法に関する給付等の事務手続きに使用するため。
⑦ 独立行政法人農業者年金基金法による農業者年金事業の給付等の事務手続きに使用するため。
⑧ 介護保険法に関する事務手続きに使用するため。
⑨ 相続税法に関する退職手当等受給者別支払調書等の事務手続きに使用するため。
⑩ 租税特別措置法に関する法定調書等の事務手続きに使用するため。
⑪ 所得税法に関する法定調書、源泉徴収票の作成等の事務手続きに使用するため。
⑫ 内国税の適正な課税の確保を図るための国外送金等に係る調書の提出等に関する法律に関する法定調書の作成等の事務手続きに使用するため。
⑬児童扶養手当法、母子及び父子並びに寡婦福祉法、障害者総合支援法、特別児童扶養手当法、生活保護法、被災者生活再建支援金に関する事務等に使用するため。

⑭ 被災者台帳の作成に関する事務等に使用するため。
⑮ その他、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第１９条各号のいずれかに該当し、特定個人情報の提供を受けることができる関連事務等に使用するため。

３. 安全管理措置に関する事項

（１）本会は、特定個人情報の漏えい、流失または毀損の防止等、特定個人情報等の管理のために別途取扱規程を定め、必要かつ適切な安全管理措置を講じます。

また、役職員に特定個人情報等を取り扱わせるにあたり、特定個人情報等の安全管理措置が適切に講じられるよう、当該役職員に対する必要かつ適切な監督を行います。

（２）特定個人情報の取り扱いについて、本人の許諾を得て、第三者に委託する場合には、特定個人情報保護に関する十分な水準を備える者を選定するとともに、契約等により安全管理措置を講じるよう定めた上で、委託先に対する必要かつ適切な監督を行います。

４. 関係法令、ガイドラインの遵守

本会は、個人情報及び特定個人情報等に関する法令、特定個人情報保護委員会およびその他の規範を遵守し、全役職員が特定個人情報等の保護の重要性を理解し、適正な取り扱い方法を実施します。

５. 継続的改善

本会は、特定個人情報等の保護が適正に実施されるよう、本基本方針および所内規程類を継続して改善します。

６. お問合せ

本会は、特定個人情報等の取り扱いに関するお問い合わせに対し、適切に対応いたします。

平成２８年１月１日

一般社団法人大分県医師会
会　長　　近　藤　　稔

特定個人情報等の適正な取扱に関する基本方針に関するお問合せ先
所 在 地：大分市大字駄原２８９２番地の1
電話番号：０９７－５３２－９１２１

特定個人情報の適正な取扱に関する規程

第１章　総則

第１条（目的）

本規程は、一般社団法人大分県医師会(以下「本会」という。)において、個人番号及び特定個人情報の適正な取扱いを確保するために遵守する事項を定める。

第２条（用語の定義）

(1)「個人情報」とは、個人情報の保護に関する法律第2条1項に規定する個人情報をいう。

(2)「個人番号」とは、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(以下「番号法」という。)第２条5項に定める個人番号をいい、同条8項括弧書きに定められたものを含む。

(3)「特定個人情報」とは、番号法第2条8項に定める特定個人情報をいう。

(4)「特定個人情報等」とは、個人番号及び特定個人情報をいう。

(5)「本人」とは、番号法第2条6項に定める本人をいう。

(6)「特定個人情報ファイル」とは、番号法第2条9項に定める特定個人情報ファイルをいう。

(7)「個人番号関係事務」とは、番号法第2条１１項に定める個人番号関係事務をいう。

(8)「個人番号利用事務実施者」とは、番号法第2条１１項に定める個人番号利用事務実施者をいう。

(9)「個人番号関係事務実施者」とは、番号法第2条１２項に定める個人番号関係事務実施者をいう。

(10)「従業員等ことは、本会の業務に従事する者をいい、役員、正社員、パートタイマー、アルバイト、派遣社員などの全ての者を含む。

第３条（適用関係）

（１）本規程は、本会の全ての従業員等に適用する。

（２）本規程は、本会が取扱う全ての特定個人情報等に適用する。

（３）本規程は、特定個人情報等の取扱いに関し、個人情報の保護に関する取扱規程、その他の内部規程に優先して適用される。

第2章 組織体制等

第4条（法令等の遵守）

本会は、番号法その他の法令を遵守し、特定個人情報等を適正に取扱うため、必要な組織体制を整備するとともに、本規程その他の内部規程を定め、これを運用する。

第5条（事務取扱責任者）

（1）本会は、特定個人情報等の管理に関する責任者として事務取扱責任者を置く。

（2）事務取扱責任者は、 事務局長とする。

（3）事務取扱責任者は、次の各号に定める事項その他本会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 特定個人情報等の適正な取扱いに関する基本方針の作成、従業員等への周知、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項の決定。承認

③ 特定個人情報等の適正な取扱い、安全対策を維持・推進するための施策の策定・実施

④ 事故発生時の対応策の策定・実施

第6条（事務取扱担当者）

（1）本会は、特定個人情報等に関する事務を取扱う者として、事務取扱担当者を置く。

（2）事務取扱担当者は、その取扱う事務の範囲を定めた上で、事務取扱責任者が選任する。

（3）事務取扱担当者は、特定個人情報等を取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、特定個人情報等に関する事務の運用状況を明確にするため、第9条に定める記録を作成する。

（5）事務取扱担当者は、個人番号事務を行うにあたり別途定める誓約書を本会へ提出しなければならない。

第7条（基本方針の策定）

本会は、本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、特定個人情報等の適正な取扱いに関する基本方針を定める。

第8条（本会が個人番号を取扱う事務の範囲）

本会が、個人番号関係事務を行う事務の範囲は以下の各号に定めるところとする。

① 雇用保険法に関する資格取得、資格喪失、給付等の事務手続きに使用するため。

② 労働者災害補償保険法に関する給付、社会復帰促進事業等の事務手続きに使用するため。

③ 健康保険法、船員保険法、国民健康保険法、高齢者の医療の確保に関する法律に関する資格取得、資格喪失、給付等の事務手続きに使用するため。

④ 厚生年金保険法に関する資格取得、資格喪失、給付等の事務手続きに使用するため。

⑤ 国家公務員共済組合法、地方公務員等共済組合法、私立学校教職員共済法に関する事務手続きに使用するため。

⑥ 確定給付企業年金法、確定拠出年金法に関する給付等の事務手続きに使用するため。

⑦ 独立行政法人農業者年金基金法による農業者年金事業の給付等の事務手続きに使用するため。

⑧ 介護保険法に関する事務手続きに使用するため。

⑨ 相続税法に関する退職手当等受給者別支払調書等の事務手続きに使用するため。

⑩ 租税特別措置法に関する法定調書等の事務手続きに使用するため。

⑪ 所得税法に関する法定調書、源泉徴収票の作成等の事務手続きに使用するため。

⑫ 内国税の適正な課税の確保を図るための国外送金等に係る調書の提出等に関する法律に関する法定調書の作成等の事務手続きに使用するため。

⑬ 児童扶養手当法、母子及び父子並びに寡婦福祉法、障害者総合支援法、特別児童扶養手当法、生活保護法、被災者生活再建支援金に関する事務等に使用するため。

⑭ 被災者台帳の作成に関する事務

⑮ その他、番号法第19条各号のいずれかに該当し、特定個人情報の提供を受けることができる関連事務

第9条（取扱状況を確認する手段の整備）

本会は、特定個人情報ファイル等の取扱状況を確認するため、事務取扱責任者が別途定める事項を記録する。なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。

第１０条（本規程に基づく運用）
　本会は、当規程等に基づく運用状況を確認するため、事務取扱責任者が別途定めるシステムログ又は利用実績を記録する。

第3章　特定個人情報等の取得、利用等

第１１条（個人番号の取得、提供の求め）
　本会は、個人番号関係事務を処理するために必要がある場合に限って、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に対して個人番号の提供を求めることができる。

第１２条（本人確認措置）
（１）本会は、前条に基づいて本人から個人番号の提供を受けるときは、別途定める「本人確認の手順」により従業員等から個人番号の提供を受けるものとする。
（２）従業員等は、個人番号の提供が番号法の定めにより個人番号関係事務に必要なものである限り、本会が行う本人確認の措置に協力しなければならない。
（３）前項にかかわらず個人番号の提供に協力しなかったことによる不利益は当該従業員等が負うものとする。

第１３条（通知カードまたは個人番号カードの取扱い）
（１）全ての従業員等は自らの通知カード又は個人番号カードを、本人の責任を持って保管しなければならない。また、本会の責めによらない紛失は、従業員等各自が、責任および対応を負うものとする。
（２）本会は、従業員等の通知カード又は個人番号カードを保管してはならないものとする。

第１４条（提供を求める時期）
　個人番号の提供を求める時期は、個人番号関係事務が発生したときとする。ただし、個人番号関係事務が発生することが明らかなときは、事前に個人番号の提供を求めることができる。

第１５条（収集制限）
　本会は、番号法に基づき許される場合を除き、他人の特定個人情報を収集し、又は、保管してはならない。

第１６条（利用目的を超えた利用の禁止）

（１）本会は、前個人番号関係事務を処理するために必要な場合に、予め通知又は公表する利用目的の範囲で個人番号を利用するものとする。なお、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。

（２）前項の規定にかかわらず、人の生命、身体又は財産の保護のために必要がある場合において、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、本会が保有している個人番号を利用することができる。

第１７条（利用目的の変更）

（１）本会は、利用目的を変更する場合、本人の同意を取得個人番号関係事務の範囲内で、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。

（２）本会は、利用目的を変更した場合、変更された利用目的について、本人に通知、又は公表する。

第１８条（特定個人情報ファイルの作成の制限）

本会は、個人番号関係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ことができる。

第４章　特定個人情報等の提供、保管、管理、廃棄等

第１９条（特定個人情報等の提供）

本会は、法令で認められた場合を除き、特定個人情報を提供しない。

第２０条（保管期間）

本会は、個人番号関係事務を処理するため必要な期間に限り、特定個人情報等を保管する。ただし、所管法令等によつて一定期間保存が義務付けられている場合、当該期間保管することとする。

第２１条（廃棄）

本会は、前条に定める保管期間が経過した場合、第31条に定める方法により、特定個人情報等をできるだけ速やかに廃棄又は削除しなければならない。

第5章 委託の取扱い

第22条（委託の取扱い）

⑴本会は、個人番号関係事務の全部又は一部を外部に委託をする場合、委託先において、特定個人情報等の安全管理措置が適切に講じられるよう必要かつ適切な監督を行う。

⑵前項の監督を行うため、次の措置を講じる。

① 委託先の適切な選定

② 委託先に安全管理措置を遵守させるために必要な契約の締結

③ 委託先における特定個人情報の取扱状況の把握

⑶前項2号に定める契約は、その内容に、秘密保持義務、特定個人情報の持出しの禁上、特定個人情報の目的外利用の禁上、再委託における条件(再々委託について最初の委託先の許諾を要することを含む。)、漏えい事故等が発生した場合の委託先の責任、委託契約終了後の特定個人情報等の返却又は廃棄、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定等を盛り込まなければならない。

第23条（再委託の要件）

（1）本会が委託を受けた個人番号関係事務の全部又は一部を再委託する場合、本会は、当該事務の最初の委託者の許諾を受ける。

⑵再委託に関しても、前条を適用する。

第6章 安全管理措置

第1部 組織的安全管理措置

第24条（情報漏えい等事案に封応する体制の整備）

すべての従業員等が情報の涌えいの発生、または兆候を把握した場合、またはその可能性が高いと判断した場合は、速やかに事務取扱責任者に報告し、事務取　扱責任者は二次被害の防止、類似事案の発生防止等の観点から速やかに以下の手法等により対策を講じるものとする。

① 事実関係の調査及び原因の究明

② 影響を受ける可能性のある本人への連絡

③ 委員会及び主務大臣等への報告

④ 再発防止策の検討及び決定

⑤ 事実関係及び再発防止策等の公表

第２５条（取扱状況の把握及び安全管理措置の見直し）

本会は、特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善のために特定個人情報等の取扱状況について、必要に応じて点検を行うものとする。なお、事務取扱責任者は、その判断により、外部機関による監査を実施することができる。

第2部 人的安全管理措置

第２６条（従業員等の教育・監督）

本会では、特定個人情報等が本指針に基づき適正に取扱われるよう、従業員等に対し必要かつ適切な教育及び監督を行うものとする。

第２７条（秘密保持）

（1）本会は、特定個人情報等を秘密として保持し、本規程第１９条に基づく場合、及び、第三者に委託する場合を除き、第三者に提供、開示、漏洩等をしないものとする。

⑵本会は、特定個人情報等に関する秘密を保持するため、本規程その他の内部規程における定め、誓約書の徴収などにより、従業員等に対し、特定個人情報等についての秘密保持に関する事項を周知徹底するものとする。

第3部　物理的安全管理措置

第２８条（特定個人情報等を取扱う区域の管理）

⑴本会では、特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを管理する区域(以下「管理区域」という。)及び特定個人情報等を取扱う事務を実施する区域(以下「取扱区域」という。)を明確にする。

⑵管理区域においては、間仕切りの設置、座席配置の工夫等、区域の明確化及びキャビネット等の施錠等の安全管理措置を講じる。

⑶取扱区域においては、壁又は間仕切り等の設置及び座席配置の工夫等の安全管理措置を講じる。

第２９条（機器及び電子媒体等の盗難等の防止）

管理区域及び取扱区域における特定個人情報等を取扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、以下の措置を講じる。

① 特定個人情報等を取扱う機器は、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により固定する。

② 特定個人情報等を含む書類及び電子媒体等は、施錠できるキャビネット・書庫等に保管する。

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上で、これを保存し、当該パスワードを適切に管理する。

第３０条（電子媒体等を持ち出す場合の漏えい等の防止）

特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、以下に例示するような容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等の安全な方策を講じる。なお「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外へ移動させることをいい、事業所内での移動等であっても、紛失・盗難等に留意する。

① 特定個人情報等が記録された電子媒体は、持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等を行う。

② 特定個人情報等が記録された書類は、外部から容易に閲覧されないよう封筒に入れる。

③ 特定個人情報等を記録する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を利用する。

第３１条（特定個人情報等の削除、機器及び電子媒体等の廃棄）

⑴本会は、第２１条に基づき特定個人情報等を廃棄又は削除する場合、次の方法によるものとし、削除又は廃棄した記録を保存するものとする。

① 特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段による。

② 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段による。

③ 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、容易に復元できない手段による。

⑵本会は、前項の廃棄又は削除を第三者に委託する場合には、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。

⑶本会は、保存期間経過後に速やかに特定個人情報等を廃棄又は削除するため、 特定個人情報等を取扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築し、また、特定個人情報等が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定めるものとする。

第4部 技術的安全管理措置

第３２条（アクセス制御）

本会は、情報システムを使用して個人番号関係事務を行う場合、事務取扱担当者及び当該事務で取扱う特定個人情報ファイルの範囲を限定するために、以下の措置に沿って適切なアクセス制御を行うものとする。

① 個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。

② 特定個人情報ファイルを取扱う情報システムを、アクセス制御により限定する。

③ ユーザーIDに付与するアクセス権により特定個人情報ファイルを取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。

第３３条（アクセス者の識別と認証）

特定個人情報等を取扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、以下の措置等によって識別した結果に基づき認証するものとする。

① 事務取扱担当者の識別方法としては、ユーザーID、パスワード、磁気・ICカード等による識別と認証を行う。
② 特定個人情報等を取扱う機器を特定し、その機器を取扱う事務取扱担当者を限定する。
③ 機器に標準装備されているユーザー制御機能(ユーザーアカウント制御)により、情報システムを取扱う事務取扱担当者を限定する。

第３４条（外部からの不正アクセス等の防止）

本会は、以下に定める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仕組みを導入し、適切に運用するものとする。

① 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。
② 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(ウイルス対策ソフトウェア等)を導入する。
③ 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。
④ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。
⑤ ログ等の分析を定期的に行い、不正アクセス等を検知する。

第３５条（情報漏えい等の防止）

本会は、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場合、通信経路における情報漏えい等を防止するために以下の措置を講じるものとする。

① 通信経路における情報漏えい等の防止策として、通信経路の暗号化等を行う。
② 情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等を行う。

第7章 その他

第36条（禁止事項）

本会はすべての従業員等に対し、特定個人情報等について、以下の各号に掲げる事項を禁止する。

① 不正な手段により特定個人情報等を収集すること
② 当初の収集目的以外で特定個人情報等利用すること
③ 業務上の必要なく管理区域および取扱区域に立ち入ること
④ 業務上の必要および権限がなく特定個人情報ファイルにアクセス、閲覧し、保管された特定個人情報等を記録すること

第37条（罰則及び損害賠償）

本会は、本規程に違反した従業員等に対して就業規則に基づき処分を行い、その他の従業員等に対しては契約又は法令に照して処分を決定する。

また、本会に損害を与えた場合には、損害賠償を請求するものとする。

附則

1．本規程は、平成28年1月1日より実施する。

マイナンバー対応

盗難防止マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

1．本マニュアルの運用対象者

本マニュアルの主たる運用対象者は下記の者とします。

(ア)事業主　個人番号関係事務実施者

2．本マニュアルの目的

事業主および個人番号関係事務実施者は、個人番号ならびに特定個人情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の管理のために必要かつ適切な安全管理措置を講じなければなりません。

本マニュアルでは、物理的安全管理措置のうち特定個人情報等を保管する機器(PCなど)、電子媒体(CDR、USBなど)、および書類などの盗難防止措置、ならびに盗難の事実が発覚した場合の対応について定めています。

事業主、および個人番号関係事務実施者は、本マニュアルの内容を熟知したうえで特定個人情報等の盗難防止にあたらなければなりません。

3．特定個人情報等の盗難防止措置

(ア)特定個人情報等を保管する媒体ごとの対応

① クラウドサーバーで特定個人情報等を保管

・特定個人情報等を取り扱う取扱区域および保管する管理区域への入退室管理が実質的に困難な場合、特定個人情報等は十分なセキュリティを確保できる社外のクラウドサーバーで保管します。

・クラウドサーバーでのみ特定個人情報等を保管する場合、社内で特定個人情報等を保管する必要がなくなります。

・クラウドサーバー上の特定個人情報を適切に保管するため、社外の情報報システムを導入し保管します。

② クラウドサーバー以外の方法で特定個人情報等を保管

<機器(PCなど)、電子媒体(CDR、USBなど)および書類などによる保管>

1．特定個人情報等を取り扱う取扱区域および保管する取扱区域への入退室を管理し、日的が無い、もしくは不明な入退室を抑制します。

・ICカード、ナンバーキーなどの入退室管理システムを設置します。

・入室時に入り口での許可制を導入し、入室時間、入室者名、入室理由、退室時間、確認者名を入退室管理表に記載し記録します。

2．特定個人情報等を保管する情報システムが機器(PCなど)のみで運用されている場合、ボルト、セキュリティワイヤーなどにより設置場所(デスクなど)に固定します。

3．機器(PCなど)および電子媒体(CDR、USBなど)に保管、もしくは書類に記載した特定個人情報等などは業務時間中に個人番号関係事務を行う必要がなくなつたとき、1日の業務時間が終了し最終退室するとき、または個人番号関係事務が終了した書類を一定期間保管するときにキャビネットや書庫などに施錠保管します。

(イ)取扱区域および管理区域における対応

① 取扱区域および管理区域には下記の機器(PCなど)および電子媒体(CDR、USBなど)の持ち込みを制限することで特定個人情報等の不正な持ち出し、情報の分散などを抑制します。

《持ち込みを禁止するもの》

・PC ・USB、CDRなどの電子媒体 ・カメラ、ビデオなどの撮影機器。なお、事前に事業主、もしくは、個人番号関係事務実施者の許可を得た機器(PCなど)、電子媒体(CDR、USBなど)は持ち込み制限の対象から除外とします。

② 取扱区域および管理区域からの最終退室者は、キャビネットや書庫などの施錠を確認し、確認者名、確認時間を入退室管理表に記録します。

(ウ)特定個人情報等の移動にともなう対応

事業所内での情報の移動、行政窓口への書類の提出など、特定個人情報等が記録された機器(PCなど)、電子媒体(CDR、USBなど)および書類などを持ち出す場合は、盗難にあわないよう細心の注意をします。また、万が一の盗難に備え下記の対応を実施します。

<特定個人情報等の移動にともなう対応>

・機器(PCなど)、電子媒体(CDR、USBなど)および書類などを持ち出す場合は、施錠可能な搬送容器(施錠、ダイヤルロックができるカバンなど)を利用します。

・書類などは封緘、もしくは特定個人I情報等への目隠しシールを貼付します。

・機器(PCなど)および電子媒体(CDR、USBなど)は第三者に解読できない難解なパスワードを設定します。

(エ)事業主および個人番号関係事務実施者は特定個人情報等の盗難防止措置が適正に運用されているかを都度確認します。

4. 盗難の事実が発覚した場合の対応

① 特定個人情報等の盗難の事案が発覚した場合は、下記のとおり適切かつ迅速に対応します。

1. 事案を確認した者から事業主、個人番号関係事務実施者へ報告
2. 影響を受ける可能性のある本人への連絡
3. 特定個人情報保護委員会および主務大臣などへの報告

② 特定個人情報等の盗難の事案が発覚した場合は下記のとおり再発防止措置を講します。

1. 事業主および個人番号関係事務実施者全員参加による盗難防止ミーティングを開催します。

A)時期:事案が発覚後3日以内

B)議事:

(1)周知－－－特定個人情報等の盗難の事案の事実確認

(2)問題提起－－－原因、ならびに課題の究明、明確化

(3)改善策－－－再発防止措置の構築、決定

C)マニュアル改定:盗難防止ミーティング開催後、7日以内に再発防止措置を本マニュアルに追記。

2. 盗難防止ミーティング終了後、7日以内にミーティング議事録を全職員へ公表します。
3. 特定個人情報保護委員会および主務大臣などへ報告します。

マイナンバー対応

漏えい防止防止マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

1. 本マニュアルの運用対象者

本マニュアルの主たる運用対象者は下記の者とします。

(ア)事業主

(イ)個人番号関係事務実施者

2. 本マニュアルの目的

事業主および個人番号関係事務実施者は、個人番号ならびに特定個人情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の管理のために必要かつ適切な安全管理措置を請じなければなりません。

本マニュアルでは、物理的管理措置のうち特定個人情報等の漏えい防止措置、ならびに漏えいの事実が発覚した場合の対応について定めています。

事業主、および個人番号関係事務実施者は、本マニュアルの内容を熟知したうえで特定個人情報等の漏えい防止にあたらなければなりません。

3. 特定個人情報等の漏えい防止措置

(ア)書類などに記載された特定個人情報等の漏えい防止措置

① 個人番号関係事務の実施前には下記手順を施します。

1. 机止の作業スペースを十分に確保します。

2. 作業スペースには、取り扱う特定個人情報等以外の書類などを放置してはいけません。

3. 個人番号関係事務の未実施書類ならびに個人番号関係事務の実施済み書類などは箱などに分けて配置することとし、事務作業の過程における書類の導線を明確にします。

4. 特定個人情報等の運用管理表に「日付」「利用目的」「対象者名」「特定個人情報等の利用者名」を記載し、事務取扱責任者による確認を受け、その履歴を記録します。

② キャビネット・書庫などに保管された特定個人情報等を作業スペースに移動させます。

③ 個人番号関係事務の未実施書類は所定の場所(箱など)に配置します。

④ 個人番号関係事務を実施後の特定個人情報等や書類などは、所定の場所(箱など)に配置し、不用意に放置しないようにします。

⑤ 特定個人情報等が記載された書類などは、複製(コピー)してはいけません。

⑥ 利用した、もしくは書類に記載した特定個人情報等は、速やかに特定個人情報等を保管するキャビネット・書庫などに格納し、その履歴は運用管理表に記録します。

⑦ 特定個人情報等を取り扱う場合、細心の注意を払い紛失防止に努めます。

(イ)情報システムなどで管理された特定個人情報等の漏えい防止措置

① 特定個人情報等は電子媒体(CDR・USBなど)に複製してはいけません。

② 特定個人情報等を取り扱う機器(PCなど)には、別途作成するフォルダなどに特定個人情報等を複製してはいけません。

(ウ)本マニュアルに記載のない技術的安全管理措置(アクセス制御・不正アクセス・メール送信等)については他マニュアルを遵守します。

(エ)事業主および個人番号関係事務実施者は、特定個人情報等の取り扱いおよび管理のルールを遵守し、漏えい防止に努めます。

４. 漏えいの事実が発覚した場合の対応

(ア)特定個人情報等の漏えいの事案が発覚した場合は、下記のとおり適切かつ迅速に対応します。

① 事案を確認した者から事業主、個人番号関係事務実施者へ報告

② 影響を受ける可能性のある本人への連絡

③ 特定個人情報保護委員会および主務大臣などへの報告

(イ)特定個人情報等の漏えいの事案が発覚した場合は、下記のとおり再発防止措置を講します。

① 事業主および個人番号関係事務実施者全員参加による漏えい防止ミーティングを開催します。

１. 時期:事案が発覚後3日以内

２. 議事:

⑴周知－－－特定個人情報等の漏えいの事案の事実確認

⑵問題提起－－－原因、ならびに課題の究明、明確化

⑶改善策－－－再発防止措置の構築、決定

３. マニュアル改定:漏えい防止ミーティング開催後、７日以内に再発防止措置を本マニュアルに追記。

② 漏えい防止ミーティング終了７日以内にミーテイング議事録を全職員へ公表します。

③ 特定個人情報保護委員会および主務大臣などへ報告します。

マイナンバー対応

アクセス制御マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

1．本マニュアルの運用対象者

本マニュアルの主たる運用対象者は、事業主並びに個人番号関係事務実施者とします。

2．本マニュアルの目的

事業主および個人番号関係事務実施者は、個人番号ならびに特定個人情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の取扱いのために必要かつ適切な安全管理措置を講じなければなりません。

本マニュアルでは、技術的安全管理措置のうちアクセス制御による特定個人情報等を取り扱う情報システム及び機器(PCなど)への不正アクセス防止措置、ならびに不正アクセスの事実が発覚した場合の対応について定めています。

事業主、および個人番号関係事務実施者は、本マニュアルの内容を熟知したうえで特定個人情報等の不正アクセス防止にあたらなければなりません。

3．特定個人1情報等への不正アクセス防止措置

(ア)アクセス制御

個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行います。

1．特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定します。

2．ユーザーIDに付与す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します。

3．機器(PCなど)に標準装備されているユーザー制御機能(ユーザーアカウント制御)により、情報システムを取り扱う事務取扱担当者を限定します。

(イ)アクセス者の識別と認証

特定個人情報を取り扱う情報システム及び機器(PCなど)は、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証します。

1．情報システムにアクセスする事務取扱担当者は、ユーザーID、パスワード、磁気・ICカード等を用いてアクセスし、第三者による操作・閲覧の起こらないように注意を払わなければなりません。

2．アクセスする際のパスワードの取り扱い

A)パスワードは英数字を使用し、5桁以上のランダムな組合せにします。

B)パスワードは少なくとも2か月以内に1回、定期的に変更します。

C)パスワードのメモ書きをしてはいけません。

D)情報システムと同一パスワードを使い回してはいけません。

(ウ)外部からの不正アクセス等の防止

① 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仕組みを導入し、適切に運用します。

1．情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断します。

2．情報システム及び機器(PCなど)にセキュリティ対策ソフトウェア等(ウィルス対策ソフトウェア等)を導入します。

3．導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認します。

4. 機器(PCなど)やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とします。
5. ログ等の分析を定期的に行い、不正アクセス等を検知します。

4. 不正アクセスの事実が発覚した場合の対応

① 特定個人情報等への不正アクセスの事案が発覚した場合は、下記のとおり適切かつ迅速に対応します。

1. 事案を確認した者から事業主、個人番号関係事務実施者へ報告
2. 影響を受ける可能性のある本人への連絡
3. 特定個人情報保護委員会および主務大臣等への報告

② 特定個人情報等への不正アクセスの事案が発覚した場合は、下記のとおり再発防止措置を講じます。

1. 事業主および個人番号関係事務実施者全員参加による不正アクセス防止ミーティングを開催します。

A)時期:事案が発覚後3日以内

B)議事:

(1)周知ーーー特定個人情報等への不正アクセスの事案の事実確認

(2)問題提起ーーー原因、ならびに課題の究明、明確化

(3)改善策ーーー再発防止措置の構築、決定

C)マニュアル改定:不正アクセス防止ミーティング開催後7日以内に再発防止措置を本マニュアルに追記

2. 不正アクセス防止ミーティング終了後7日以内にミーティング議事録を全職員へ公表します。
3. 特定個人情報保護委員会および主務大臣等への報告をします。

マイナンバー対応

アクセスログ管理マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

１．本マニュアルの運用対象者

本マニュアルの主たる運用対象者は下記の者とします。

(ア)事業主

(イ)システム管理者：本会のシステムを保守・管理する責任者

(ウ)システム利用者：本会のシステムを利用する従業員等の全ての関係者

2．本マニュアルの目的

事業主・システム管理者およびシステム利用者は、個人番号ならびに個人情報・特定個人情報(以下「特定個人情報等」といいます。)の漏えい、滅失、毀損の防止など特定個人情報等の管理のために必要かつ適切な安全管理措置を講じなければなりません。

本マニュアルでは、社内の情報システムにおけるアクセスログ(以下「ログ」といいます。)についての、特定個人情報等の適切な管理をするための方策および特定個人情報等の漏えい、滅失、毀損の防止等について定めています。

事業主・システム管理者は、本マニュアルの内容を熟知したうえで、ログの適切な管理を、またシステム利用者はログの適切な管理のための協力に努めなければなりません。

3．本マニュアルの対象情報

職場のパソコン、サーバ、その他ネットワークデバイス等の全て機器(以下「機器」といいます。)からアクセス可能な、Office、ブラウザ、メーラー、業務ソフト等のフォーマットを問わず全ての情報(以下「情報」といいます。)が対象になります。

4．ログ管理システムの導入

システム管理者は、ベンダーおよびインターネットやマスコミ広報などを通して、広くログ管理に関する情報の収集を行います。収集した情報を基に、当社のネットワーク状況・ログ管理システムの態様およびその費用等を勘案した上で対策を実施します。選定にあたつては以下を主な基準とします。

（ア）対象となる機器や情報のログの内容を1つにまとめて保管する一元管理機能があること。

(イ)収集したログの内容から、さまざまな事象を分析する機能があること。

（ウ）ログの内容の分析結果やログ管理対象の一覧、ログの保存状況等の情報を表示、レポートとして出力する機能があること。

(エ)ログの改ざん防止や改ざんされていないことを証明する機能があること。

5．システム利用者への周知

事業主またはシステム管理者は、システム利用者に対し、本マニュアルで決定したログ管理対策について、その目的、方法、開始日時、実施対象者を周知します。これにより、システム利用者の意識を高め、安易なアクセス防止の抑止効果を図ります。

6．ログの収集

システム管理者は、業務システムごとにログを取得します。ログには、アクセス開始時間、ユーザーID、アクセス対象ファイル、アクセス内容(参照、更新)、アクセス終了時間等を記録するものとします。

7. ログ収集のタイミング

ログ収集は、毎週金曜日午後6時に収集するものとします。

8. ログの保管期間

システム管理者は、収集したログを9年間保管するものとします。

9. ログの分析

システム管理者は、毎月、前月分のアクセスログを点検します。毎月の点検に関わらず不審な動きが見られた場合には、その都度、点検・分析を行うものとします。

10. ログの改ざん防止

ハ―ドウェアやソフトウェアが記録・作成したログの原本が、改ざんされていないことを確認します。

11. 情報の漏えい等の情報への不審なアクセスの事実が発覚した場合の対応

(ア)情報の漏えい等のI青報への不審なアクセスの事実が発覚した場合は下記のとおり適切かつ迅速に対応します。

①システム管理者から事業主へ報告

②ログ状況の事実関係の調査及び原因の究明

③再発防止策の検討及び決定

(イ)情報の漏えい等の情報への不審なアクセスの事実が発覚した場合は下記のとおり再発防止措置を講します。

①事業主・システム管理者およびに事案に関係するシステム利用者よる盗難防止ミーティングを開催します。

(1)時期:事案が発覚後3日以内

(2)議事:

・周知－－－情報の漏えい等の情報への不審なアクセスの事実確認

・問題提起－－－原因、ならびに課題の究明、明確化

・改善策－－－再発防止措置の構築、決定

②マニュアル改定:ミーティング開催後、7日以内に再発防止措置を本マニュアルに追記

③ミーティング終了後、7日以内にミーティング議事録を全職員へ公表します。

マイナンバー対応

不正アクセス防止マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

1. 本マニュアルの運用対象者

本マニュアルの主たる運用対象者は下記の者とします。

(ア)事業主

(イ)システム管理者:本会のシステムを保守・管理する責任者

(ウ)システム利用者:本会のシステムを利用する従業員等の全ての関係者

2. 本マニュアルの目的

事業主・システム管理者およびシステム利用者は、個人番号ならびに特定個人情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の管理のために必要かつ適切な安全管理措置を講しなければなりません。

本マニュアルでは、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し、適切に運用するための方策ならびに不正アクセス又は不正ソフトウェアの感染等の事実が発覚した場合の対応について定めています。

事業主・システム管理者およびシステム利用者は、本マニュアルの内容を熟知したうえで、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に努めなければなりません。

3. 機器やソフトウェア等に標準装備されている自動更新機能等の活用

(ア)情報システムのハードウェア、ソフトウェア、ネットワークなどで構成された運用環境と開発環境は、ハードウェアを別管理するなどの物理的、またはプログラム、ソースコード等の違いにより論理的に分離します。

(イ)システム構成情報の管理

情報システムのハードウェアおよびソフトウェア構成情報を最新の状態に維持管理します。

(ウ)業務システムの変更履歴管理

システム運用管理者は、業務システムを構成するソフトウェアに変更があったとき、変更情報(変更日、変更したソフトウェア、変更事由、変更箇所、変更内容)を管理します。

(エ)システム受入れ時の確認

情報システムの新規導入・変更の際、運用環境に移す前に適切な試験を計画し実施します。

4. セキュリティ対策ソフトウェア(ウィルス対策ソフトウェア)等の導入

外部ネットワークにつながっているサーバ《およびPCに対して、コンピュータウイルス対策を講じることによって、コンピュータウイルスによる個人データに係る事故の発生を防止します。

(ア)アンチウイルスソフトの導入

本会は、情報システムを構成するすべてのサーバ《およびPCにアンチウイルスソフトを導入します。導入するアンチウイルスソフトは、以下の要件が満たされていることを条件にシステム管理者が選定します。

①最新パターンファイルのタイムリーな更新

②常時ウイルススキャン機能(ファイル、電子メールの添付ファイル)

③ベンダがウイルスに関する豊富な情報提供、アンチウイルスソフトの適切なバージョンアップ、パターンファイルのタイムリーな更新を行っていること

(イ)アンチウイルスソフトの設定

システム管理者は、パターンフアイルの更新および常時ウイルススキャン機能が正しく動作するように、アンチウイルスソフトの設定を定め周知を図ります。システム利用者は、本会外から持ち込んだノートPCなどの情報機器やFDなどの媒体をPCで使用する場合、必ず事前に、アンチウイルスソフトを利用してスキャンを行わなければなりません。

(ウ)ウイルスに関する情報収集と適用

システム管理者は、ベンダーおよびインターネットやマスコミ広報などを通して、広くウイルスに関する情報の収集を行います。収集した情報を基に、ウイルス対策のためにOSのセキュリティパッチなどの適用が必要と判断した場合には、対策を実施します。

(エ)メール送受信時の留意事項

①電子メール受信時、アンチウイルスソフトの常時ウイルススキャン機能によつて、自動的にウイルスチェックを行います。

②電子メールを利用している最中にウイルスに感染したと思われる状況を発見した場合、速やかにシステム管理者へ報告を行い、対応についての指示を受けます。

③システム利用者は、送信元不明の電子メールおよびその添付フアイルに対しては、操作を加えずに削除します。

(オ)ソフトウェアインストールに対する対策

①ソフトウェアのインストールに際しては、システム管理者の許可を得なければなりません。

②ソフトウェアをインストールする際、ウイルスチェックを必ず行うものとします。

③フリーウェアのインストールは原則として禁止とします。どうしても必要な場合には、システム管理者の許可を得なければなりません。

5. ファイアウォール等の設置

システム管理者は、本会のインターネット環境およびインターネットに接続するコンピュータ(パソコンなど)が備えるべきセキュリテイ要件について取り決め、周知を図ります。

(ア)インターネットサービスの決定

システム管理者は、電子メールおよびWebサイト閲覧以外の、本会が業務において利用するオンライン決済、eラーニング、チャット、動画配信などインターネット上で提供される様々なサービス(以下「インターネットサービス」といいます。)を決定し、システム利用者に対して利用できるインターネットサービスおよびその利用方法を周知します。

(イ)ファイアウォールの選定と設置

Webサーバとインターネットとの間には、必ずファイアウォールを設置し、外部からの不正アクセスを防御します。システム管理者は、不正アクセスに対する防御の強度を選定基準の第一として、ファイアウォールを選定し、設置したファイアウォールに対して、不正アクセスを防止するためのフィルタリングの設定を行います。

(ウ)ファイアウォールによる不正アクセスの監視

システム管理者は、ファイアウォールのログ採取機能を利用して、インターネットを通しての外部から社内ネットワークへのアクセスのログを採取し保管します。ファイアウォールのログの保存期間は、半年とし、1ヶ月に1度、採取したファイアウォールのログをチェックし、不正アクセスの有無を確認します。

(エ)インターネットのセキュリティに関する情報収集と適用

システム管理者は、プロバイダおよびマスコミ広報などを通して、広くインターネットのセキュリティに関する情報を収集します。収集した情報を基に、インターネット環境の構築・設定、インターネットの運用・利用に関するセキュリティ維持のために、対応が必要と判断した事項があれば、その適用を図ります。

(オ)業務目的以外でのインターネット利用禁止

システム利用者は、本会のインターネット環境を業務目的以外で利用してはなりません。また、許可したインターネットサービス以外のサービスを利用してはなりません。

(カ)インターネット利用上の留意

システム利用者は、インターネットを利用する際、次のことに留意しなければなりません。

①リンク先を確認した上でのWebサイトへのリンク

②信頼性の低いWebサイトからのデータのダウンロードの禁止

③Webサイトからダウンロードしたフアイルに対するコンピュータウィルスチェックの実施

④Webサイトからダウンロードした情報を利用する際の知的所有権の保護

6. ログ等の定期的な分析

(ア)アクセスログの取得

システム管理者は業務システムごとに、アクセスログを取得します。アクセスログには、アクセス開始時間、ユーザーID、アクセス対象ファイル、アクセス内容(参照、更新)、アクセス終了時間を記録し、取得したアクセスログは5年間保管します。

(イ)アクセスログの分析

システム管理者は、毎月、前月分のアクセスログを点検し、不審な動きが見られた場合には、その度、点検・分析を行います。

7. 不正アクセス又は不正ソフトウェアの感染等の事実が発覚した場合の対応

(ア)不正アクセス又は不正ソフトウェアの感染等の事案が発覚した場合は、下記のとおり適切かつ迅速に対応します。

①事案を確認した者から事業主、システム管理者へ報告

②事実関係の調査及び原因の究明

③再発防止策の検討及び決定

(イ)不正アクセス又は不正ソフトウェアの感染等の事案が発覚した場合は、下記のとおり再発防止措置を講します。

①事業主・システム管理者および事案に関係するシステム利用者よる盗難防止ミーティングを開催します。

(1)時期:事案が発覚後3日以内

(2)議事:

・周知－－－不正アクセス又は不正ソフトウェアの感染等の事案の事実確認

・問題提起－－－原因、ならびに課題の究明、明確化

・改善策－－－再発防止措置の構築、決定

②マニュアル改定:ミーティング開催後7日以内に再発防止措置を本マニュアルに追記

③ミーティング終了後、7日以内にミーティング議事録を全職員へ公表します。

マイナンバー対応

メール取扱マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

1. 本マニュアルの運用対象者

本マニュアルの主たる運用対象者は下記の者とします。

(ア)事業主

(イ)個人番号関係事務実施者

2. 本マニュアルの目的

事業主および個人番号関係事務実施者は、個人番号ならびに特定個人・情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の管理のために必要かつ適切な安全管理措置を講じなければなりません。

本マニュアルでは、技術的安全管理措置のうち特定個人情報等をメールで取り扱う場合の情報漏えいの防止措置、ならびに情報漏えいの事実が発覚した場合の対応について定めています。

事業主および個人番号関係事務実施者は、本マニュアルの内容を熟知したうえで、特定個人情報等を扱うメールを適切に行わなければなりません。

3. 特定個人情報等を扱うメールの情報漏えい防止措置

(ア)メール送信時の情報漏えい防止措置

① 誤送信の防止

1. メールソフトに直接メールアドレスの入力を行う場合は、入力間違いが無いように慎重に行いダブルチェックを行います。ダブルチェックは一人で行わず複数人の目で確認をします。

2. 特定個人情報を扱うメールは、必ず送信前に送信内容とその宛先が相違していないかどうか確認します。

3. 特定個人情報を扱うメールに添付ファイルのある場合は、必ず送信前にフアイルを開けて内容を確認します。

② 送信内容の確認

1. 本会外宛メールを送信する場合は必ず上長のメールアドレスなどをBCC(相手先が上長のメールアドレスを知っている場合はCCでもよい)に入れ、情報漏えいが起こっていないかどうかの確認体制をつくります。

③ 外部からの不正アクセスに対する対策

1. 送信したメールソフト内の特定個人情報を含むメールは定期的に削除し、ソフト内に情報を残しません。

(イ)メール受信時の情報漏えい防止措置

1. 外部からの不審なメールに添付されたファイルは開封しません。

2. 受信するメールソフト内の特定個人情報を含むメー)レは定期的に削除し、ソフト内に情報を残しません。

4. 情報漏えいの事実が発覚した場合の対応

① 特定個人情報等の情報漏えいの事案が発覚した場合は、下記のとおり適切かつ乱凍に対応します。

1. 事案を確認した者から事業主、事務取扱責任者へ報告

2. 影響を受ける可能性のある本人への連絡

3. 特定個人情報保護委員会および主務大臣等への報告

② 特定個人情報等の漏えい事案が発覚した場合は、下記のとおり再発防止措置を講じます。

１．事業主および個人番号関係事務実施者全員参加による情報漏えい防止のミーティングを開催します。

A)時期：事案が発覚後、３日以内

B)議事：

(1)周知－－－特定個人情報等の漏えい事案の事実確認

(2)問題提起－－－原因、ならびに課題の究明、明確化

(3)改善策－－－再発防止措置の構築、決定

C)マニュアル改定：特定個人情報の漏えい防止ミーティング開催後、７日以内に再発防止措置を本マニュアルに追記

２．特定個人情報の漏えい防止ミーティング終了後、７日以内にミーティング議事録を全職員へ公表します。

３．特定個人情報保護委員会および主務大臣等への報告をします。

マイナンバー対応

運 用 マ ニ ュ ア ル

一般社団法人大分県医師会

平成２８年１月１日制定

1. 本マニュアルの運用対象者

本マニュアルの主たる運用対象者は下記の者とします。

(ア)事業主

(イ)個人番号関係事務実施者

2. 本マニュアルの目的

事業主および個人番号関係事務実施者は、個人番号ならびに特定個人情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の取扱いのために必要かつ適切な安全管理措置を講じなければなりません。

本マニュアルでは、事業主及び個人番号関係事務実施者における特定個人情報等の取得、提出、保管、利用、提供、委託及び廃棄に関する適切な運用手順、ならびに特定個人情報等の不適切な運用の事実が発覚した場合の対応について定めています。

事業主、及び個人番号関係事務実施者は、本マニュアルの内容を熟知したうえで、特定個人情報等の取扱い運用にあたらなければなりません。

3. 各種マニュアルに定めている安全管理措置の運守

(ア)特定個人情報の取得・保管・利用・提供・委託・廃棄においては盗難防止マニュアル、漏えい防止マニュアル、アクセス制御マニュアル、不正アクセス防止マニュアル、アクセスログ管理マニュアル、メール取扱いマニュアルに定めている安全管理措置を遵守します。

4. 特定個人情報等の取得

(ア)個人番号関係事務が発生する際には、個人番号を回収します。

(イ)契約内容等から個人番号関係事務が明らかに発生しないと認められる場合には、個人番号を回収しません。

(ウ)個人番号を回収する際には、事前に提出書類を案内します。

(エ)個人番号を回収する際の提出警類は以下の通りとします。

① 個人番号確認書類

1. 通知カード
2. 個人番号カード
3. 住民票(個人番号付き)
4. その他個人番号確認書類として関係省庁が適切と認めるもの

② 身元確認書類

1. 写真付きのもの

A)運転免許証
B)パスポート
C)個人番号カード
D)写真付き身分証明書・資格証明書・学生証
E)その他写真付き身元確認書類として関係省庁が適切と認めるもの

2. 写真のないもの

A)住民票(個人番号の有無にかかわらない・6か月以内のもの)
B)印鑑登録証明書(6か月以内のもの)
C)戸籍謄本・抄本(6か月以内のもの)
D)国税・地方税・社会保険料・公共料金の領収書(6か月以内のもの)
E)その他写真なし身元確認書類として関係省庁が適切と認めるもの

※ 個人番号カードを提示された場合は、1枚で身元確認と番号確認が可能です。
※ 身元確認書類に写真がない場合、複数の身元確認書類による確認を行います。
※ 扶養家族(第三号被保険者を除く)の身元確認を従業員本人が行う場合、身元確認書類の提出は求めません。

③ 委任状

1. 第三号被保険者等、個人番号を本人以外から回収する際は委任状を提出するよう求めます。

④ 提出された個人番号確認書類および身元確認書類をコピー又は保管する場合は、特定個人情報等と同様の安全管理措置を行います。

5. 特定個人情報等の提出時期等

(ア)提出時期

① 個人番号通知開始までに在籍し、個人番号関係事務が発生する従業員は、本人及び扶養家族について個人番号の通知が届き次第、速やかに個人番号確認書類を提出するよう求めます。

② 個人番号通知開始以降に入職し、個人番号関係事務が発生する従業員は、入職時に個人番号確認書類を提出するよう求めます。

③ 系列会社等の別の法人格から出向又は転籍により異動した職員は、異動時に個人番号確認書類を提出するよう求めます。

④ 扶養家族の追加等が発生した場合は、速やかに個人番号確認書類を提出するよう求めます。

⑤ 報酬支払等により従業員以外から個人番号を回収する必要がある場合は、回収の必要がわかり次第、速やかに個人番号確認書類を提出するよう求めます。

(イ)提出先

① 個人番号関係事務実施者に提出を求めます。個人番号関係事務実施者以外には提出を求めません。

(ウ)提出方法

① 対面での提出

1. 対面で特定個人情報等の提供を受ける際には、以下の点に注意します。

A)覗き見や盗撮がされない環境で提供を受けます。

② 郵送での提出

1. 郵送で特定個人情報等の提供を受ける際には以下の点に注意します。

A)必ず個人番号関係事務実施者を宛先とするよう求めます。

B)郵送手段は書留を指定します。

③ 本会内便での提出

1. 本会内便で特定個人情報等の提供を受ける際には、以下の点に注意します。

A)必ず個人番号関係事務実施者を宛先とします。

B)親展を記載します。

C)個人番号確認書類。身元確認書類、委任状以外の書類を一緒に送りません。

④ メールでの提出

1．メールにて提出を受ける際には、以下の点に注意します。

A)個人番号確認書類および身元確認書類をデータ添付にて提供を受ける場合は、パスワード設定が行われた状態で提出するよう求めます。

B)スマートフォンやタブレットなどを利用して、メールに画像データが添付された状態でメールを受け取る際には、覗き見や盗撮などがされない環境でメールを開封し、データを閲覧します。

6．特定個人情報等の保管

(ア)保管方法

① 特定個人情報等を取扱う情報システムがない場合は本会所定の用紙に記録し、鍵付きのキヤビネット等に保管します。

② 特定個人情報等を取扱う情報システムがある場合は本会所定の情報システムへ記録します。

(イ)保管制限

① 個人番号関係事務を処理する必要がなくなった場合であっても、所轄法令に定められた保存期間を経過するまでは保管します。

② 従業員等が体職しており、復職が未定であっても特定個人情報等は継続的に保管します。

③ 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に定められた事務以外の目的で、従業員等の特定個人情報等を管理してはなりません。

7．特定個人情報等の利用

(ア)個人番号の利用目的

① 本会は「特定個人情報等の適正な取り扱いに関する基本方針」に定められた利用目的に則り、個人番号を利用します。

② 特定個人情報の利用目的は、個人番号の提出を求める際に明示します。

③ 利用目的の変更は、当初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内で行い、対象となる従業員へ速やかに通知します。変更後の利用目的に関する個人番号の利用は、通知後に行います。

(イ)特定個人情報等の利用制限

① 本会は主として社会保障、税及び災害対策に関する特定の事務において、従業員等の個人番号を記載して行政機関及び健康保険組合等に提出します。

② 本会は本人の同意があったとしても例外として認められる場合を除き、社会保障、税及び災害対策に関する特定の事務以外に個人番号を利用してはなりません。

1．利用してはならない場合

A)職員番号として利用する場合など

2．例外として認められる場合

A)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場合など

③ 取得した個人番号を一定の法則に従って置き換えてはなりません。

1．数字をアルファベットに置き換えることなど

(ウ)特定個人情報等関係事務を委託しない場合

① 社会保障、税及び災害対策に関する特定の事務で特定個人情報等が記載された書類等を本会外へ持ち出す場合

1. 本会が指定した特定個人情報専用の封筒等に入れます。

A)特定個人情報専用の封筒等は、本会名、所在地、連絡先、持出担当者が識別できるようにします。

B)封緘、日隠し、シールの貼り付け等をします。

2. 特定個人情報等が記載された書来類の放置は禁止します。

A)飲食店等で座席へ放置すること。

B)業務車やマイカーを業務利用している場合などに車中へ放置することなど。

3. 特定個人情報等を本会外に持ち出す場合は、事業主もしくは個人番号関係事務責任者へ事前に報告し承認を得ます。

(エ)特定個人情報等関係事務を委託する場合

① 委託先(社会保険労務士や税理士など)と協議の上、運用ルールを作成します。

8. 特定個人情報等の提供

(ア)提供とは法的な人格を超える特定個人情報等の移動を意味します。

(イ)番号法で限定的に明記された場合を除き、特定個人情報を提供してはなりません。

① 提供に当たる場合

1. 同系列の医師会間等の提供など

2. 出向者本人以外が共有データベースを操作することによる出向先への移転など

② 提供に当たらない場合

1. 総務部から経理部などの部門間での移動

2. 出向者本人の意思に基づく共有データベースの操作による出向先への移転 など

(ウ)特定個人情報等を提供できるのは以下の場合です。

① 個人番号関係事務のための提供

1. 個人番号関係事務実施者は、個人番号関係事務を処理するために、法令に基づき行政機関等、健康保険組合等又はその他の者に特定個人情報を提供します。

② 委託、合併に伴う提供

1. 特定個人情報の取扱いの全部もしくは一部の委託又は合併その他の事由による事業の承継が行われたときは、特定個人情報を提供します。

③ その他提供ができる場合

1. 委員会からの提供の求めによる提供の場合

2. 各議員審査等その他公益上の必要があるときの提供の場合

3. 人の生命、身体又は財産の保護のための提供の場合

9. 特定個人情報等の委託

(ア)委託先の適切な選定

① 個人番号関係事務を委託する場合、本会内で定めた安全管理措置と同等もしくはそれ以上の措置が請しられるかをあらかじめ確認し、適切な措置が講じられていると確認した場合に委託先として選定します。

② 委託先について確認する内容

1. 基本方針
2. .取扱規程
3. 組織的安全管理措置
   A)事務取扱責任者の設置、役割及び責任の明確化の状況
   B)事務取扱担当者の明確化及びその役割の明確化の状況
   C)取扱状況記録の方法
   D)取扱状況を確認する手段の整備状況
   E)情報漏えい等事案の発生、または兆候を把握した場合の報告運絡体制
4. 人的安全管理措置
   A)従業者に対する監督
   B)従業者に対する教育
5. 物理的安全管理措置
   A)管理区域、取扱区域の明確化
   B)機器、電子媒体及び書類等の漏えい、盗難または紛失等の防止策
   C)機器、電子媒体及び書類等を持ち出す場合の漏えい、盗難または紛失等の防止策
   D)個人番号の削除方法
   E)機器及び電子煤体等の廃棄方法
6. 技術的安全管理措置
   A)情報システムを使用する場合のアクセス制御方法
   B)情報システムを使用する場合のアクセス者の識別と認証方法
   C)外部からの不正アクセス等の防止方法
   D)外部との通信経路における情報漏えい等の防止方法
7. その他委託先の選定に必要と思われること

(イ)委託先における必要かつ適切な監督

① 委託先において、本会内で定めた安全管理措置と同等もしくはそれ以上の措置が講じられるかを監督するため、委託先との契約内容に基づき取扱状況の報告を受けます。

② 委託先を監督する項目は委託先について確認する内容に準じます。

③ 監督の方法は、報告を求めるだけでなく実地の調査も場合によって選定します。

(ウ)委託先に安全管理措置を遵守させるための必要な契約の締結

① 委託先との委託契約の内容としては、下記のことを定めます。

1. 秘密保持義務
2. 事業所内からの特定個人情報の持ち出し制限
3. 特定個人情報の目的外利用の禁止
4. .再委託における条件
5. 情報漏えい事案が発生した場合の委託先の責任
6. 委託契約終了後の特定個人情報の返却又は廃棄
7. 委託先の従業者に対する教育・監督
8. 委託契約の遵守がされているかの状況報告を求める規程
9. 特定個人情報を取り扱う従業者の明確化
10. 実地の調査を行うことができる規程 など

(エ)特定個人情報等の再委託

① 個人番号関係事務を委託した先から、さらにその先の委託先(再委託先)への再委託は、事前に承諾した場合のみ可能とします。

② 個人番号関係事務を再委託先する場合は、委託先と再委託先の委託契約に、本会内で定めた安全管理措置と同等もしくはそれ以上の措置が講しられるよう契約内容を定め、監督できる体制にします。

③ 再委託先への選定および取扱状況の把握においても、委託先と同等もしくはそれ以上の安全管理措置が講じられていることを確認し、契約内容に基づき取扱状況の報告を受けます。

④ 再委託先から更にその先の委託先(再々委託先)への再々委託は、再委託を承諾、監督する場合と同様に取り扱います。

10. 個人番号関係事務を行う必要がなくなった場合の番号廃棄について

(ア)特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄の時期

① 個人番号関係事務を行う必要がなくなつた場合で、所管法令等において定められている保存期間等を経過した場合、当該年度の3月31日に番号の削除、また機器(PCなど)及び電子媒体(CDR、USBなど)の記録を廃棄します。

※各帳票の所管法令によって定められた保存期間は、本マニュアル末尾に記載します。

(イ)特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄の方法

① 特定個人情報が記載された書類を廃棄する場合、裁断・焼却・溶解等の復元不可能な手段を採用します。また、本会で対応が困難な場合は、専門業者に廃棄を依頼します。

② 特定個人情報等が記載された機器(PCなど)及び電子媒体(CDR、USBなど)を廃棄する際、自社で対応する場合は専用のデータ削除用ソフトウェアもしくは強磁気を発する特殊装置を利用します。また、本会で対応できない場合は、専門業者に廃棄を依頼します。

(ウ)特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄の記録

① 特定個人情報等を削除した場合、または電子媒体(CDR、USBなど)を廃棄した場合には、削除または廃棄した情報を個人番号取扱記録簿に記録します。

1. 個人番号取扱記録簿などに記録する場合は、削除内容をその業務を行うごとに記載し、あらかじめ運用で決められた頻度で記録が記載されているかチェックします。

2. 情報システムにおいては、保存期間経過後における特定個人情報の削除とその記録を前提としたシステムを構築し、削除及びその記録をとります。

② 特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄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、証明書等によりその記録を確認します。

11. 特定個人情報等の運用記録

(ア)取得・保管・利用・提供・廃棄状況を記録表へ記録します。

(イ)記録票には、下記事項を記載します。

① 対象者氏名
② 操作日時
③ 操作内容
④ 目的
⑤ 方法(廃棄の場合)
⑥ 操作者氏名

（例）① 対象者氏名　　大分花子
② 操作日時　　20××／00／00　00:00
③ 操作内容　　取得
④ 目的　　入職のため
⑤ 方法(廃棄の場合）　ー
③ 操作者氏名　　大分一郎

12. 本マニュアルに記載した手順が適切に運用されているかの確認
（ア)6ヶ月に一度は、自主点検または他部署等による監査を実施します。
（イ)1年に一度は、外部主体(顧問契約を締結している社会保険労務士等)による監査を実施します。

13. 本マニュアルに記載した手順が適切に運用されていないことが発覚した場合は、下記のとおり再発防止措置を講します。
1. 事業主および個人番号関係事務実施者全員参加によるミーティングを開催します。
A)時期:事案が発覚後3日以内
B)議事:
(1)周知ーーー事実確認
(2)問題提起ーーー原因、ならびに課題の究明、明確化
(3)改善策ーーー再発防止措置の構築、決定
C)マニュアル改定:ミーティング開催後、7日以内に再発防止措置を本マニュアルに追記。
2. ミーティング終了後、7日以内にミーティング議事録を全職員へ公表します。

マイナンバー対応

番号廃棄マニュアル

一般社団法人大分県医師会

平成２８年１月１日制定

1．本マニュアルの運用対象者

本マニュアルの主たる運用対象者は、下記の者とします。

(ア)事業主

(イ)個人番号関係事務実施者

2．本マニュアルの目的

事業主および個人番号関係実務実施者は、個人番号ならびに特定個人情報(以下「特定個人情報等」という)の漏えい、滅失、毀損の防止など特定個人情報等の取扱いのために必要かつ適切な安全管理措置を講じなければなりません。

本マニュアルでは、物理的安全管理措置のうち個人番号関係事務を行う必要がなくなった場合の番号廃葉に関するする業務、ならびに番号廃棄が適切になされていない事実が発覚した場合の対応について定めています。

事業主、および個人番号関係事務実施者は、本マニュアルの内容を熟知したうえで番号廃棄の事務にあたらなければなりません。

3．個人番号関係事務を行う必要がなくなった場合の番号廃棄について

(ア)特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄の時期

① 個人番号関係事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合、当該年度の３月３１日に番号の削除、また機器(PCなど)及び電子媒体(CDR、USBなど)の記録を廃棄します。

※各帳票の所管法令によって定められた保存期間は、本マニュアルの末尾に記載

(イ)特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄の方法

① 特定個人情報が記載された書類を廃棄する場合、裁断・焼却・溶解等の復元不可能な手段を採用します。また、本会で対応が困難な場合は、専門業者に廃棄を依頼します。

② 特定個人情報等が記載された機器(PCなど)及び電子媒体(CDR、USBなど)を廃棄する際、自社で対応する場合は専用のデータ削除用ソフトウェアもしくは強磁気を発する特殊装置を利用します。また、本会で対応できない場合は、専門業者に廃棄を依頼します。

(ウ)特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄の記録

① 特定個人情報等を削除した場合、又は電子媒体(CDR、USBなど)を廃棄した場合には、削除または廃棄した情報を個人番号取扱記録簿に記録します。

1．個人番号取扱記録簿などに記録する場合は、削除内容をその業務を行うごとに記載し、あらかじめ運用で決められた頻度で記録が記載されているかチェックします。

2．情報システムにおいては、保存期間経過後における特定個人情報の削除とその記録を前提としたシステムを構築し、削除及びその記録をとります。

② 特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄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、証明書等によりその記録を確認します。

4．個人番号関係事務を行う必要がなくなった場合での番号廃棄が、適切に行われなかった事実が発覚した場合の対応

① 個人番号関係事務を行う必要がなくなった場合に、番号廃棄が適切に行われなかった事実が発覚した場合は、下記のとおり適切かつ迅速に対応します。

1．事実を確認した者から事業主、個人番号関係事務実施者へ報告

2．影響を受ける可能性のある本人への連絡

② 個人番号関係事務を行う必要がなくなった場合での番号廃棄が、適切に行われなかった事実が発覚した場合は、下記のとおり再発防止措置を講じます。

1．事業主および個人番号関係事務実施者全員参加による個人番号関係事務を行う必要がなくなった場合での番号廃棄の適正化をするミーティングを開催します。

A)時期：事実の発覚後3日以内

B)議事：

(1)周知－－－特定個人情報の削除、機器(PCなど)及び電子媒体(CDR、USBなど)の廃棄が適切に行われなかった事実の確認

(2)問題提起－－－原因、ならびに課題の究明、明確化

(3)改善策－－－再発防止措置の構築、決定

2．マニュアル改定：個人番号関係事務を行う必要がなくなった場合での番号廃棄の適正化をするミーティング開催後、7日以内に再発防止措置を本マニュアルに追記します。

3．個人番号関係事務を行う必要がなくなった場合での番号廃棄の適正化のミーティング終了後、7日以内にミーティング議事録を全職員へ公表します。