7. 在宅医療を取り巻く個人情報保護法制の現状と課題

京都大学医学部附属病院医療情報企画部
黒田 知宏
Tomohiro KURODA

1. 遠隔モニタリング：在宅医療の形―議論の前提として

「遠隔医療解禁」と呼ばれた平成30年度の診療報酬改定では，情報通信機器を用いた診療（いわゆる遠隔診療）を三つの類型に分類し，それぞれについて診療報酬と運用ルールの整備が行われた（**図1**）[1]。一つ目が，医師が画像を情報ネットワーク越しに提供して専門医の判断を仰ぐ「遠隔画像診断」，二つ目が，医師と患者をテレビ電話で結んで外来診療を行う「オンライン診療」，三つ目が，患者の日常生活空間におかれた医療機器の動作・計測データを医師が情報ネットワーク越しに閲覧して患者管理を行う「遠隔モニタリング」である。

このうち，人工臓器導入後の患者の在宅診療において最も中心的役割を担うと期待されるのは三つ目の，「遠隔モニタリング」であろう。人工臓器や各種の生体計測装置の動作・計測データを情報ネットワークにのせることができれば，遠隔モニタリングの実施は技術的には大きな課題ではなくなる。あとは，遠隔モニタリングを実施した場合の患者管理の状況が，一定間隔で来院した場合に比較して，「非劣勢」であることを示す[2]ことができれば，患者の来院負担の軽減や，（将来的なAIなどの導入も含む）情報処理技術導入による問題発生の予兆発見の可能性向上などを考慮すると，遠隔モニタリング・オンライン診療を妨げる科学的・経済的な理由はなくなる。

遠隔モニタリングを支える情報システムの多くは，**図2**に示すように医療機器から携帯通信回線などを通じて医療機器ベンダーのサーバに情報を収集し，そこで医療機器の固有番号をキーに患者の個人情報と結びつける。医師は医療機器ベンダーのサーバにアクセスしてデータを閲覧し，診療を行う。

遠隔モニタリングを支障なく実施するためには，診療情報の取り扱いにかかる各種の法制に沿った形で情報システムを構成し，得られたデータを適切に診療録に収める必要がある。本稿では，遠隔モニタリングにおける，個人情報の取り扱い方[3]について整理する。

2. 診療情報を取り巻く法制

ヒポクラテスの誓い以来，医師の守秘義務は医師の職業倫理の重要な一要素をなしてきた。現在の日本の法令では，医師の守秘義務は刑法134条1項[4]に

> 医師，薬剤師，医薬品販売業者，助産師，弁護士，弁護人，公証人又はこれらの職にあった者が，正当な理由がないのに，その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは，六月以上の懲役又は十万円以下の罰金に処する。

と記載されており，違反には刑事罰（秘密漏示罪）が科せられるようになっている。刑法134条は守秘義務を有する職業を列挙する条文であるが，その冒頭に「医師」が記載されている。なお，同条2項は宗教関係者に同じ義務を課している。宗教関係者に守秘義務を課すことで，「懺悔」などを信者が安心してできるようになることと照らして考えれば，医師の守秘義務という職業倫理の持つ意味も明らかであろう。

守秘されるべき「病歴」については，個人情報保護法（個人情報の保護に関する法律）[5]においても，「要配慮個人情報」（2条3項）に指定し，「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

■ 著者連絡先
京都大学医学部附属病院医療情報企画部
（〒606-8507　京都府京都市左京区聖護院川原町54）
E-mail. tomo@kuhp.kyoto-u.ac.jp

平成30年度診療報酬改定　Ⅱ－2－1）遠隔診療の評価①

診療報酬における遠隔診療（情報通信機器を用いた診療）への対応

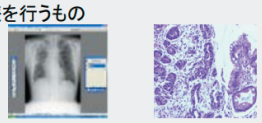
	診療形態		診療報酬での対応
医師対医師（D to D）	情報通信機器を用いて画像等の送受信を行い特定領域の専門的な知識を持っている医師と連携して診療を行うもの 		**[遠隔画像診断]** ・ 画像を他医療機関の専門的な知識を持っている医師に送信し、その読影・診断結果を受信した場合 **[遠隔病理診断]** ・ 術中迅速病理検査において、標本画像等を他医療機関の専門的な知識を持っている医師に送信し、診断結果を受信した場合（その後、顕微鏡による観察を行う。） ・（新）生検検体等については、連携先の病理医が標本画像の観察のみによって病理診断を行った場合も病理診断料等を算定可能
医師対患者（D to P）	情報通信機器を用いた診察	医師が情報通信機器を用いて患者と離れた場所から診療を行うもの 	**[オンライン診療]** ・（新）オンライン診療料 ・（新）オンライン医学管理料 ・（新）オンライン在宅管理料・精神科オンライン在宅管理料 対面診療の原則の上で、有効性や安全性等への配慮を含む一定の要件を満たすことを前提に、情報通信機器を用いた診察や、外来・在宅での医学管理を行った場合 **※電話等による再診** （新）患者等から電話等によって治療上の意見を求められて指示をした場合に算定が可能であるとの取扱いがより明確になるよう要件の見直し （定期的な医学管理を前提とした遠隔での診察は、オンライン診療料に整理。）
	情報通信機器を用いた遠隔モニタリング	情報通信機能を備えた機器を用いて患者情報の遠隔モニタリングを行うもの 	**[遠隔モニタリング]** **・心臓ペースメーカー指導管理料（遠隔モニタリング加算）** 体内植込式心臓ペースメーカー等を使用している患者に対して、医師が遠隔モニタリングを用いて療養上必要な指導を行った場合 ・（新）在宅患者酸素療法指導料（遠隔モニタリング加算） ・（新）在宅患者持続陽圧呼吸療法（遠隔モニタリング加算） 在宅酸素療法、在宅CPAP療法を行っている患者に対して、情報通信機器を備えた機器を活用したモニタリングを行い、療養上必要な指導管理を行った場合

図1　遠隔医療の三分類[1)]

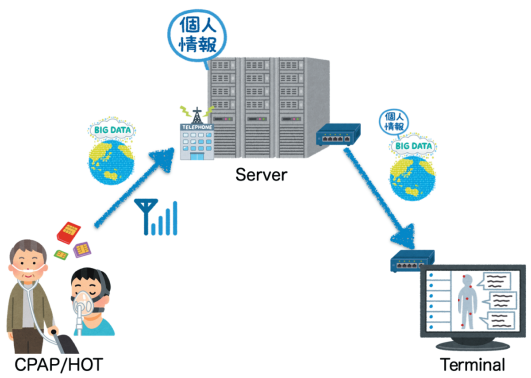


図2　遠隔モニタリングシステムの基本構造

要する」とされている。なお，同法2条1項では，個人情報は「生存する個人」に関する情報で，「特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む。）」を「個人情報」と定めている。すなわち，個人情報であるかないかは，特別な知識を有しない一般人が，このデータは誰の者かを「識別」できるか否か（識別可能性）によって判断される。例えば，医療機関が発行する患者IDは，その医療機関の所属者でなければ誰のものであるかを識別できないことから，一般的な意味での「個人情報」ではないことになる。一方，医療機関の構成員であればそのIDが誰のものかを識別できるので，その医療機関の関係者にとっては「個人情報」に他ならない。したがって，患者IDが記載されたX線フィルムが紛失されたときには，「（紛失した病院にとっては）個人情報を紛失したが，（それをどこかで拾った人にとっては識別可能性がないので）個人情報は漏洩していない」という，一見理解しにくい謝罪会見が行われることになる。

個人情報保護法では，個人情報の取得・利用・第三者提供において，「本人」にその目的や提供先を明示して同意を取ることを求めているが，医療現場での診療情報を診療目的で取り扱うことについては，「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」[5)]において，「黙示の同意」で扱ってよいとしている。これは，医療機関において「問診票」に書き込んだ時点で，患者本人はその情報が自分自身の診療目的で利用されることに「同意」していると見なせる，ということである。患者が他病院を受診したときに，その病院からの要請に応じて自院のデータを提供することもまた，「黙示の同意」の範囲である。ただし，医療機関などがどういう場合に個人情報を「黙示の同意」で取り扱うのかについては，掲示などで示すことが求められている。

一方，某かの「委託」に伴って，その委託業務の遂行に必要な個人情報を業者に渡すことは，「第三者提供」ではな

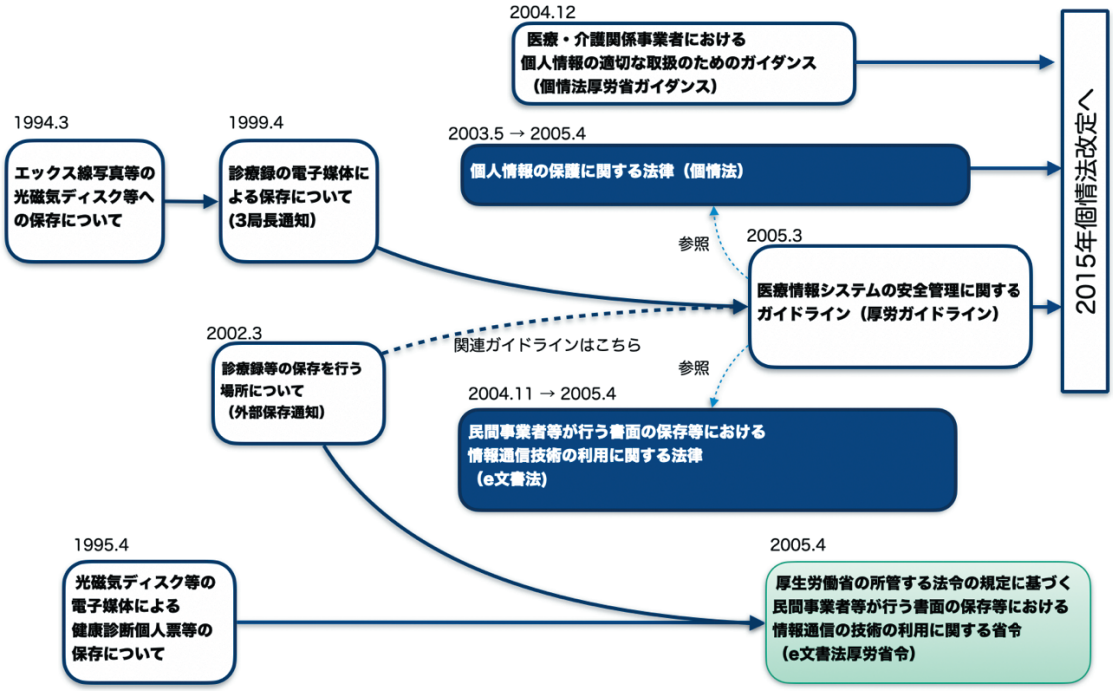


図3　診療記録のルールと厚労ガイドライン

く，「自法人での個人情報の利用」と見なされる。例えば，医療機関が，遠隔モニタリング用の機器を患者宅に貸し出す（処方する）際に，故障時のメンテナンスなどのために患者の住所などを機器ベンダーに提供する場合は，第三者提供に当たらない。

したがって，遠隔モニタリングにおいては，患者にあらかじめ説明をしておけば，特に同意書をとらずとも医療機器ベンダーに患者情報を委託契約の下で提供することが可能である。

最後に，同法の下で個人情報を安全に管理するための一般的なルールについては，「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）」[5]で示されている。例えば，個人情報を保存しておく場所については，同ガイドラインの8-5において，「個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（管理区域）」と「個人データを取り扱う事務を実施する区域（取扱区域）」を分け，管理区域については「入退室管理及び持ち込む機器等の制限」を求めている。したがって，患者を含めた誰もが自由に出入りできて，出入りした人物が誰かを記録できない診察室にあるパソコンに，患者の病歴を保存してはいけないということになる。

3.　3省2ガイドライン

遠隔モニタリングにおいては，病歴（患者の要配慮個人情報）は情報ネットワークを通じて伝送される。何らかのサイバーアタックによって，遠隔モニタリングを支える情報システムが破壊されたり攻撃者の侵入を許したりしてしまえば，病歴は漏洩してしまう。

保険診療の下での情報システムの安全性確保の方法などについては，厚生労働省「医療情報システムの安全管理に関するガイドライン」（以下，厚労ガイドライン）[6]と経済産業省・総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下，経産総務ガイドライン）[7]の二つのガイドライン，いわゆる3省2ガイドラインによって示されている。厚労ガイドラインは医療機関に対する，経産総務ガイドラインは医療機関に情報サービスを提供する事業者に対するガイドラインである。

厚労ガイドラインは，そもそも，1999年の「三局長通知」[8]に端を発している（**図3**）。この通知では，それまで紙媒体での保存を義務づけていた診療録について，「真正性」†1，「見読性」†2，「保存性」†3の三要件を満たしている場合には，電子媒体に保存してよいという，いわゆる「電子カルテ解禁」の通知である。この通知は，公文書の電子保存を初めて認めた通知であった。

2005年の公文書一般の電子保存を認めた，e文書法†4の施行に伴い，同通知が廃止されるにあたって，上記の通知などの各種関連文書をまとめる形で発出されたのが，厚労

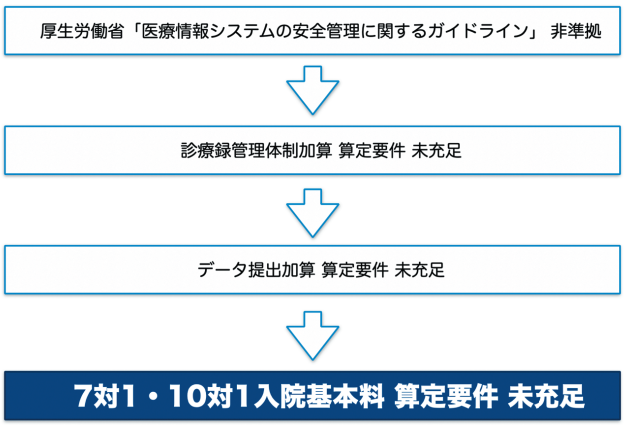


図4　3省2ガイドラインと診療報酬

ガイドラインである。

現在，厚労ガイドラインは，図4に示すように，保険診療の仕組みの下に組み入れられている。厚労ガイドラインの遵守は「診療録管理体制加算」の要件とされ，同加算の取得は「データ提出加算」の要件とされている。DPC（diagnosis procedure combination）データを厚生労働省に提出することに対して，提供される「データ提出加算」が取得できないということは，DPC対象となる「急性期」病院ではないと解釈されることから，「7対1入院基本料」や「10対1入院基本料」の算定要件を満たさないと解釈される。つまり，3省2ガイドラインの遵守は，保険診療上の重要な要件の一つなのである。

厚労ガイドラインは，個別の技術的事項について細かいルールを定めた「パターナル」なガイドラインである。具体的には，本人認証（ログイン）の有り様についていわゆる「二要素認証」†5を求めたり，通信路の情報セキュリティについていわゆる「政府推奨暗号」[9]を用いた仮想専用線（VLAN）などの整備を求めたりしている。これは，情報セキュリティ知識が必ずしも豊富ではない医療者や監査者が「言われたとおりにするだけ」で最低限の安全性を確保できるようにするための配慮であるが，近年の急激な技術発達の中で，更新されてもすぐに技術的に陳腐化したり，かえって危険であることが明らかになっている記載がそのまま残されてしまっていたりするなどの問題も起きている。

一方，経産総務ガイドラインは，「情報技術のプロ」である事業者に「リスクベースアプローチ」でのリスク管理を求め，顧客である医療機関との「リスクコミュニケーション」を求めている。具体的には，厚労ガイドラインを参考に事業者が対応すべき「リスク」を洗い出し，そのそれぞれについて，厚労ガイドラインの示す，あるいは，それと同等以上と考えられる措置の適用を行って，そのようにしていることを医療機関に示して理解を得ることが求められている。事業者には「サービス仕様適合開示書」の開示と「サービス・レベル合意書（service level agreement, SLA）」の締結を求めている。サービス仕様適合開示書においては，どのようなリスク対応がとられているかに加えて，パスワードの適切な管理を行うことや，運用に関するルールの医療機関の関連規定への書き込みなど，医療機関が行うべき対応に関する依頼事項を記載することとされており，SLA締結した医療機関はこれらの依頼事項を遵守することが必要になる。

経産総務ガイドラインは，事業者に最大限の技術選択の自由を与えているが，医療者が法的義務を履行できるようにすることを事業者に課している。例えば，他国の法令が自国政府に情報システム内に保管されている情報の閲覧を認めている場合には，刑法134条1項で求められる守秘義務を医師が履行できなくなってしまう。したがって，経産総務ガイドラインでは，「情報システムを国内法の及ぶ範囲に置く」ことを求めている。したがって，本稿執筆時点では，GDPR†6と個人情報保護法の同一性認証†7を相互

†1 真正性：正当な人が記録し確認された情報に関し第三者から見て作成の責任と所在が明確であり，かつ，故意又は過失による，虚偽入力，書き換え，消去，及び混同が防止されていること。
†2 見読性：診療，患者への説明，監査，訴訟等に際して，その目的に応じて，保存された内容を必要に応じて肉眼で見読可能な状態に容易にできること。
†3 保存性：記録された情報が，法令等で定められた期間にわたって，真正性を保ち，見読可能にできる状態で保存されること。
†4 e文書法：「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」の二つの法律の総称。
†5 二要素認証：パスワード（記憶要素：人の記憶に頼る認証鍵）と携帯端末に提示される番号（所有要素：あらかじめ登録された携帯電話を持っているという所有の事実を確認することによる認証鍵）など，複数の要素を用いた認証。
†6 GDPR：General data protection regulation（欧州一般データ保護規則）。欧州連合（European Union，EU）加盟各国に共通して遵守が求められる，個人情報を含むデータ保護に関する法律。
†7 同一性認証：GDPRの概念。EU域外の国が欧州GDPRと同等のデータ保護に関する法制を持っていることを認証する制度。認証された国への個人情報の移転は認められるが，認証されていない国への移転を行う際には，移転を希望する法人（企業）が個別に欧州委員会の承認を得ることが必要になる。

に実施している欧州にあるサーバに病歴などのデータを置くことは可能であるが，パトリオット法を有する米国にあるサーバに病歴などのデータを置くことは許されていない。

4. 遠隔モニタリングシステムのあり方

個人情報保護法制と3省2ガイドラインに照らして考えると，**図2**に示した遠隔モニタリングシステムが満たすべき要件は相当明確に規定されることが分かる。

まず，遠隔モニタリングシステムの情報発生源である在宅用医療機器から機器ベンダーのサーバまでのデータ伝送においては，医療機器のシリアル番号に紐付いた形で，動作・計測情報が送付される。このデータには「個人識別性」はないことから，「個人情報」にあたらず，直接的な法的規制は発生しない。したがって，例えば患者が米国へ海外旅行をしていて，計測機器が米国内からデータを送付しても，法的な問題は発生しない。無論，データが簡単に窃取されることのないように，暗号化などを施しておくべきことは言うまでもない。

データが医療機器ベンダーのサーバに収まると，一般的にここで患者の氏名などの個人情報と結びついて保管されることになる。したがって，医療機器ベンダーのサーバは「国内法の及ぶ範囲」におかれることが必須の要件になる。

医療機器ベンダーのサーバ上のデータを医療機関が閲覧するにあたっては，医師が当該システム上にアカウントの発行を受け，接続して閲覧することになる。この時，この接続には「政府推奨暗号」を用いたセキュリティの高い接続〔TLS（transport layer security）接続〕が求められ，ユーザには二要素認証を行うことが推奨される。無論，二要素認証は「パスワード」（記憶要素）と「接続端末の認証」（所有要素）の組み合わせでも成立し，所有要素の確認のために「電子証明書」と呼ばれる，公開鍵暗号方式[†8]などを用いた電子ファイルを用いて実施することも許容される。

閲覧した情報は診療を行った証左であることから，適切に診療録に写されなければならない。数値記録を目で見て書き写すという方法がとられることも考えられるが，PDFファイルなどでレポートをダウンロードして診療録に貼り付けることも考えられる。ダウンロードをする方式をとるときには，それをカルテに貼り付けた後は速やかに削除しなければならないことに注意が必要である。そうしておかないと，「個人情報管理区域」におかれていない診察室のパソコンに個人情報が保管されてしまうことになる。

上記の「面倒さ」を解消するためには，機器ベンダのサーバと自院の電子カルテを直接接続し，データを直接電子カルテにあらかじめ書き込んでおいて，医師がそのデータを開いたときに「閲覧した」という記録を残す方法も考えられる。今後，機器ベンダーのサーバ上に他のソフトウエアが接続するAPI[†9]が設けられ，直接接続が増えるようになるものと期待される。

最後に，個人情報を医療機器ベンダーが扱うことは，医療機関からの「業務委託」（あるいはシステム利用）の範囲になることから，個人情報の第三者提供にはあたらない。一方で，個人情報保護法は，委託先に自法人の個人情報の保護のルールを遵守させることを求めており，経産総務ガイドラインは，事業者に「サービス仕様適合開示書」の開示と「サービス・レベル合意書（SLA）」の締結を求めている。医療機関は事業者から適合開示書の提示を受けてその説明を理解し，SLAを締結するとともに，自院の個人情報管理に関するルールを事業者に説明して理解させ，これを遵守することを契約・覚書などで求めなければならない。個人情報保護法も経産総務ガイドラインも，事業者への「丸投げ」を許容しておらず，あくまでも管理を行うのは医療機関自身であるとしていることを強く意識する必要がある。

結局重要なことは，医療機器ベンダーが個人情報を安全・適法に扱えるシステムを構築して，丁寧な説明書を作成し，医療機関はきちんとこれを理解した上で利用する，協調関係を構築することにある。

5. 今後の展望

本稿執筆時において，保険収載されている遠隔モニタリングの対象機器は，埋め込み型ペースメーカーや睡眠呼吸管理装置などに限られている。人工臓器を埋め込んで以降，あるいは，特定の医療機器を利用した治療を在宅で実施することで，大きな不自由なく日常生活を送っている人々が，状況のチェックだけのために頻回に医療機関を訪れることを強要されることは，患者のQoL（Quality of Life）や社会全体の経済活動の活性化の観点から好ましくない。今後，遠隔モニタリングを可能とする仕組みが構築され，「非劣勢」

†8 公開鍵暗号方式：ある鍵で鍵をかけた情報は，それと組になる別の鍵でなければ解錠されない鍵を作り，一方の鍵（公開鍵）を相手方に渡して，自らの鍵（秘密鍵）でデータを暗号化して相手方に送り，相手方が渡された公開鍵でそのデータを復号できることをもって，自らの正当性を相手に確認させる方式。

†9 API (application programming interface)：外部のソフトウエアが自らのソフトウエアと接続する際に使ってもらう，ソフトウエア接続用の出入り口。

を確認する研究が速やかに実施されて，人工臓器を利用している患者が，医療機関を訪れる負担なく，医師に適切に見守られながら，日常生活を送れるようになることが望まれる。

最後に，データが機器ベンダーサイトに送られ，様々な情報が機械分析可能になれば，危険な状態になる可能性があることを予測するAI（人工知能）などのソフトウエア（SaMD†10）が作られ，より人工臓器利用者のQoLが高まっていくとともに，APIを通じて医療者の手を煩わせずとも必要な記録が残されるような，未来への途も開かれるのではないかと思われる。そうなるためには，現在の「紙の資料を電子的に取り扱うことを許す」法制から脱して，「電子的にデータが生成・伝送・保存・加工・分析・提示される前提」で，医療を取り巻く法制を整理し直すことが求められる。医師法24条が「医師は，……診療に関する事項を診療録に『記載』しなければならない。」と「紙にインクを載せる」前提で規定しているようでは，情報化時代の医療の姿を紡ぎ出す途を速やかに進むことは，なかなかできないだろう。

本稿の著者には規定されたCOIはない。

文　献

1) 未来投資会議 構造改革徹底推進会合「健康・医療・介護」会合 第4回 オンライン診療の推進．厚生労働省．2018．https://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/suishinkaigo2018/health/dai4/siryou1.pdf Accessed 22 Sep 2021
2) Murase K, Tanizawa K, Minami T, et al: A Randomized Controlled Trial of Telemedicine for Long-Term Sleep Apnea Continuous Positive Airway Pressure Management. Ann Am Thorac Soc **17**: 329-37, 2020
3) 黒田知宏，黒田佑輝，陳　和夫：遠隔モニタリングを支える情報システムのあり方について．日遠隔医療会誌 **14**: 98-100, 2018
4) 刑 法．E-gov法 令 検 索．https://elaws.e-gov.go.jp/document?lawid=140AC0000000045 Accessed 22 Sep 2021
5) 法令・ガイドライン等．個人情報保護委員会．https://www.ppc.go.jp/personalinfo/legal/ Accessed 22 Sep 2021
6) 医療情報システムの安全管理に関するガイドライン 第5.1版．厚生労働省．2021．https://mhlw.go.jp/stf/shingi/0000516275.html Accessed 22 Sep 2021
7) 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン．経済産業省．https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html Accessed 22 Sep 2021
8) 診療録等の電子媒体による保存について．健政発第517号，医薬発第587号，保発第82号．（三局長通知）厚生労働省健康政策局長，医薬安全局長，保険局長．1999．https://www.mhlw.go.jp/www1/houdou/1104/h0423-1_10.html Accessed 22 Sep 2021
9) TLS暗号設定ガイドライン ～安全なウェブサイトのために（暗号設定対策編）～．情報処理推進機構（IPA）．2020．https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html Accessed 22 Sep 2021

† 10 SaMD (software as a medical device)：医療機器プログラム。医療機器として機能するソフトウエア。薬機法（医薬品，医療機器等の品質，有効性及び安全性の確保等に関する法律）の下で，医療機器としての薬事認証・承認が必要になる。