

オンライン診療の適切な実施に関する指針

○ 新旧対照表

新	旧
<p>目次 (略)</p> <p>I オンライン診療を取り巻く環境 (略)</p> <p>II 本指針の関連法令等 <u>無診察治療等の禁止</u> (略)</p> <p><u>医療提供場所</u> 医療法（昭和 23 年法律第 205 号）（抄） 第 1 条の 2 （略） 2 <u>医療は、国民自らの健康の保持増進のための努力を基礎として、医療を受ける者の意向を十分に尊重し、病院、診療所、介護老人保健施設、介護医療院、調剤を実施する薬局その他の医療を提供する施設（以下「医療提供施設」という。）、医療を受ける者の居宅等（居宅その他厚生労働省令で定める場所をいう。以下同じ。）において、医療提供施設の機能に応じ効率的に、かつ、福祉サービスその他の関連するサービスとの有機的な連携を図りつつ提供されなければならない。</u></p>	<p>目次 (略)</p> <p>I オンライン診療を取り巻く環境 (略)</p> <p>II 本指針の関連法令等 <u>無診察治療等の禁止</u> (略)</p> <p><u>医療提供場所</u> 医療法（昭和 23 年法律第 205 号）（抄） 第 1 条の 2 （略） 2 <u>医療は、国民自らの健康の保持増進のための努力を基礎として、医療を受ける者の意向を十分に尊重し、病院、診療所、介護老人保健施設、調剤を実施する薬局その他の医療を提供する施設（以下「医療提供施設」という。）、医療を受ける者の居宅等（居宅その他厚生労働省令で定める場所をいう。以下同じ。）において、医療提供施設の機能に応じ効率的に、かつ、福祉サービスその他の関連するサービスとの有機的な連携を図りつつ提供されなければならない。</u></p>

医療法施行規則（昭和 23 年厚生省令第 50 号）（抄）

第 1 条 医療法（昭和 23 年法律第 205 号。以下「法」という。）

第 1 条の 2 第 2 項の厚生労働省令で定める場所は、次のとおりとする。

- 一 老人福祉法（昭和 38 年法律第 133 号）第 20 条の 4 に規定する養護老人ホーム（第 9 条第 3 項第 3 号において同じ。）
- 二 老人福祉法第 20 条の 5 に規定する特別養護老人ホーム（第 9 条第 3 項第 4 号において同じ。）
- 三 老人福祉法第 20 条の 6 に規定する軽費老人ホーム（第 9 条第 3 項第 5 号において同じ。）
- 四 有料老人ホーム
- 五 前各号に掲げる場所のほか、医療を受ける者が療養生活を営むことができる場所であつて、法第 1 条の 2 第 2 項に規定する医療提供施設（以下単に「医療提供施設」という。）以外の場所

情報セキュリティ関係

個人情報の保護に関する法律（平成 15 年法律第 57 号）（抄）
（安全管理措置）

第 23 条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安

医療法施行規則（昭和 23 年厚生省令第 50 号）（抄）

第 1 条 医療法（昭和 23 年法律第 205 号。以下「法」という。）

第 1 条の 2 第 2 項の厚生労働省令で定める場所は、次のとおりとする。

- 一 老人福祉法（昭和 38 年法律第 133 号）第 20 条の 4 に規定する養護老人ホーム
- 二 老人福祉法第 20 条の 5 に規定する特別養護老人ホーム
- 三 老人福祉法第 20 条の 6 に規定する軽費老人ホーム
- 四 老人福祉法第 29 条第 1 項に規定する有料老人ホーム
- 五 前各号に掲げる場所のほか、医療を受ける者が療養生活を営むことができる場所であつて、法第 1 条の 2 第 2 項に規定する医療提供施設以外の場所

情報セキュリティ関係

個人情報の保護に関する法律（平成 15 年法律第 57 号）（抄）
（安全管理措置）

第 20 条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安

全管理のために必要かつ適切な措置を講じなければならない。

(従業者の監督)

第 24 条 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

(委託先の監督)

第 25 条 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

医療情報システムの安全管理に関するガイドライン（平成 17 年 3 月 31 日医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長、医薬食品局長及び保険局長連名通知；令和 4 年 3 月改定）

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（令和 2 年 8 月策定、令和 4 年 8 月改定 総務省、経済産業省）

個人情報の適切な取扱いに係る基幹システムのセキュリティ対策の強化について（依頼）（平成 27 年 6 月 17 日老発 0617 第 1

全管理のために必要かつ適切な措置を講じなければならない。

(従業者の監督)

第 21 条 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

(委託先の監督)

第 22 条 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

医療情報システムの安全管理に関するガイドライン（平成 17 年 3 月 31 日医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長、医薬食品局長及び保険局長連名通知；令和 3 年 1 月改定）

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（令和 2 年 8 月策定 総務省、経済産業省）

個人情報の適切な取扱いに係る基幹システムのセキュリティ対策の強化について（依頼）（平成 27 年 6 月 17 日老発 0617 第 1

号・保発 0617 第 1 号厚生労働省老健局長及び保険局長連名通知)

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（平成 29 年 4 月 14 日個情第 534 号・医政発 0414 第 6 号・薬生発 0414 第 1 号・老発 0414 第 1 号個人情報保護委員会事務局長、厚生労働省医政局長、医薬・生活衛生局長及び老健局長連名通知；令和 4 年 3 月改正）

Ⅲ 本指針に用いられる用語の定義と本指針の対象

(1) 用語の定義

(略)

(2) 本指針の対象

(略)

Ⅳ オンライン診療の実施に当たっての基本理念

(略)

i 医師－患者関係と守秘義務

(略)

ii 医師の責任

号・保発 0617 第 1 号厚生労働省老健局長及び保険局長連名通知)

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（平成 29 年 4 月 14 日個情第 534 号・医政発 0414 第 6 号・薬生発 0414 第 1 号・老発 0414 第 1 号個人情報保護委員会事務局長、厚生労働省医政局長、医薬・生活衛生局長及び老健局長連名通知)

Ⅲ 本指針に用いられる用語の定義と本指針の対象

(1) 用語の定義

(略)

(2) 本指針の対象

(略)

Ⅳ オンライン診療の実施に当たっての基本理念

(略)

i 医師－患者関係と守秘義務

(略)

ii 医師の責任

(略)

iii 医療の質の確認及び患者安全の確保

(略)

iv オンライン診療の限界などの正確な情報の提供

(略)

v 安全性や有効性のエビデンスに基づいた医療

適切なオンライン診療の普及のためには、その医療上の安全性・必要性・有効性が担保される必要があり、医師は安全性や有効性についてのエビデンスに基づいた医療を行うことが求められる。特に、オンライン診療においては、対面診療と比べて、医療へのアクセスが向上するという側面がある一方で、得られる情報が少なくなってしまうという側面もあることを考慮し、安全性・必要性・有効性の観点から、学会のガイドライン等を踏まえて、適切な診療を実施しなければならない。

また、オンライン診療は、上記のとおり、対面診察に比べて得られる情報が少なくなってしまうことから、治験や臨床試験等を経ていない安全性の確立されていない医療を提供すべきではない。

vi 患者の求めに基づく提供の徹底

(略)

(略)

iii 医療の質の確認及び患者安全の確保

(略)

iv オンライン診療の限界などの正確な情報の提供

(略)

v 安全性や有効性のエビデンスに基づいた医療

適切なオンライン診療の普及のためには、その医療上の安全性・必要性・有効性が担保される必要があり、医師は安全性や有効性についてのエビデンスに基づいた医療を行うことが求められる。

また、オンライン診療は、対面診察に比べて得られる情報が少なくなってしまうことから、治験や臨床試験等を経ていない安全性の確立されていない医療を提供すべきではない。

vi 患者の求めに基づく提供の徹底

(略)

V 指針の具体的適用

(略)

1. オンライン診療の提供に関する事項

(1) 医師－患者関係／患者合意

(略)

(2) 適用対象

(略)

(3) 診療計画

①考え方

(略)

②最低限遵守する事項

- i 医師は、オンライン診療を行う前に、患者の心身の状態について、直接の対面診療により十分な医学的評価（診断等）を行い、その評価に基づいて、次の事項を含む「診療計画」を定め、2年間は保存すること。
 - ・ オンライン診療で行う具体的な診療内容（疾病名、治療内容等）
 - ・ オンライン診療と直接の対面診療、検査の組み合わせに関する事項（頻度やタイミング等）

V 指針の具体的適用

(略)

1. オンライン診療の提供に関する事項

(1) 医師－患者関係／患者合意

(略)

(2) 適用対象

(略)

(3) 診療計画

①考え方

(略)

②最低限遵守する事項

- i 医師は、オンライン診療を行う前に、患者の心身の状態について、直接の対面診療により十分な医学的評価（診断等）を行い、その評価に基づいて、次の事項を含む「診療計画」を定め、2年間は保存すること。
 - ・ オンライン診療で行う具体的な診療内容（疾病名、治療内容等）
 - ・ オンライン診療と直接の対面診療、検査の組み合わせに関する事項（頻度やタイミング等）

- ・ 診療時間に関する事項（予約制等）
- ・ オンライン診療の方法（使用する情報通信機器等）
- ・ オンライン診療を行わないと判断する条件と、条件に該当した場合に直接の対面診療に切り替える旨（情報通信環境の障害等によりオンライン診療を行うことができなくなる場合を含む。）
- ・ 触診等ができないこと等により得られる情報が限られることを踏まえ、患者が診察に対し積極的に協力する必要がある旨
- ・ 急病急変時の対応方針（自らが対応できない疾患等の場合は、対応できる医療機関の明示）
- ・ 複数の医師がオンライン診療を実施する予定がある場合は、その医師の氏名及びどのような場合にどの医師がオンライン診療を行うかの明示
- ・ 情報漏洩等のリスクを踏まえて、セキュリティリスクに関する責任の範囲（責任分界点）及びそのとぎれがないこと等の明示

ii ~ iv （略）

③推奨される事項

（略）

(4) 本人確認

- ・ 診療時間に関する事項（予約制等）
- ・ オンライン診療の方法（使用する情報通信機器等）
- ・ オンライン診療を行わないと判断する条件と、条件に該当した場合に直接の対面診療に切り替える旨（情報通信環境の障害等によりオンライン診療を行うことができなくなる場合を含む。）
- ・ 触診等ができないこと等により得られる情報が限られることを踏まえ、患者が診察に対し積極的に協力する必要がある旨
- ・ 急病急変時の対応方針（自らが対応できない疾患等の場合は、対応できる医療機関の明示）
- ・ 複数の医師がオンライン診療を実施する予定がある場合は、その医師の氏名及びどのような場合にどの医師がオンライン診療を行うかの明示
- ・ 情報漏洩等のリスクを踏まえて、セキュリティリスクに関する責任の範囲及びそのとぎれがないこと等の明示

ii ~ iv （略）

③推奨される事項

（略）

(4) 本人確認

①考え方

(略)

②最低限遵守する事項

(削る)

- i 緊急時などに医師、患者が身分確認書類を保持していない等のやむを得ない事情がある場合を除き、原則として、医師と患者双方が身分確認書類を用いてお互いに本人であることの確認を行うこと。ただし、かかりつけの医師がオンライン診療を行う場合等、社会通念上、当然に医師、患者本人であると認識できる状況であった場合には、診療の都度本人確認を行う必要はない。
- ii 初診でオンライン診療を実施する場合、当該患者の本人確認は、原則として、顔写真付きの身分証明書（マイナンバーカード、運転免許証、パスポート等）で行うか、顔写真付きの身分証明書を有しない場合は、2種類以上の身分証明書をを用いる、あるいは1種類の身分証明書しか使用できない場合には、当該身分証明書の厚みその他の特徴を十分に確認した上で、患者本人の確認のための適切な質問や全身

①考え方

(略)

②最低限遵守する事項

- i 医師が医師免許を保有していることを患者が確認できる環境を整えておくこと。ただし、初診を直接の対面診療で行った際に、社会通念上、当然に医師であると認識できる状況であった場合、その後に実施するオンライン診療においては、患者からの求めがある場合を除き、医師である旨の証明をする必要はない。
- ii 緊急時などに医師、患者が身分確認書類を保持していない等のやむを得ない事情がある場合を除き、原則として、医師と患者双方が身分確認書類を用いてお互いに本人であることの確認を行うこと。ただし、社会通念上、当然に医師、患者本人であると認識できる状況であった場合には、診療の都度本人確認を行う必要はない。

(新設)

観察等を組み合わせ、本人確認を行う。

iii 医師の本人証明の方法として、なりすまし防止のために、社会通念上、当然に医師本人であると認識できる場合を除き、原則として、顔写真付きの身分証明書（HPKI カード、マイナンバーカード、運転免許証、パスポート等）を用いて医師本人の氏名を示すこと。なお、身分証明書の提示は医師の氏名の確認が目的であり、医籍登録番号、マイナンバー、運転免許証番号、パスポート番号、住所、本籍等に係る情報を提示することを要するものではない。

iv 「医籍登録年」を伝える（医師免許証を用いることが望ましい。）など、医師が医師の資格を保有していることを患者が確認できる環境を整えておくこと。また、必要に応じて、厚生労働省の「医師等資格確認検索」（氏名、性別、医籍登録年）を用いて医師の資格確認が可能である旨を示すこと。ただし、初診を直接の対面診療で行った際に、社会通念上、当然に医師であると認識できる状況であった場合、その後実施するオンライン診療においては、患者からの求めがある場合を除き、医師である旨の証明をする必要はない。

③確認書類の例

（削る）

i 患者の本人確認：健康保険証（被保険者証）、マイナンバーカード、運転免許証、パスポート等の提示

（新設）

（新設）

③確認書類の例

i 医師の免許確認：HPKI カード（医師資格証）、医師免許証の提示の活用

ii 患者の本人確認：健康保険証（被保険者証）、マイナンバーカード、運転免許証等の提示

<p>ii <u>医師の本人証明：HPKI カード（医師資格証）、マイナンバーカード、運転免許証、パスポート等の提示</u></p> <p>iii <u>医師の資格証明：HPKI カード（医師資格証）、医師免許証の提示の活用</u></p> <p>(5)・(6) (略)</p> <p>2. オンライン診療の提供体制に関する事項</p> <p>(1) 医師の所在</p> <p>①考え方 (略)</p> <p>②最低限遵守する事項</p> <p>i <u>オンライン診療を行う医師は、医療機関に所属し、その所属及び当該医療機関の問い合わせ先を明らかにしていること。</u></p> <p>ii～v (略)</p> <p>vi <u>オンライン診療を実施する医療機関は、ホームページや院内掲示等において、本指針を遵守した上でオンライン診療を実施している旨を公表するものとする。</u></p> <p>③推奨される事項 (略)</p>	<p>(新設)</p> <p>(新設)</p> <p>(5)・(6) (略)</p> <p>2. オンライン診療の提供体制に関する事項</p> <p>(1) 医師の所在</p> <p>①考え方 (略)</p> <p>②最低限遵守する事項</p> <p>i オンライン診療を行う医師は、医療機関に所属し、その所属を明らかにしていること。</p> <p>ii～v (略)</p> <p>(新設)</p> <p>③推奨される事項 (略)</p>
--	--

(2)～(4) (略)

(5) 通信環境（情報セキュリティ・プライバシー・利用端末）

①考え方

オンライン診療の実施に当たっては、利用する情報通信機器やクラウドサービスを含むオンライン診療システム（※1）及び汎用サービス（※2）等を適切に選択・使用するために、個人情報及びプライバシーの保護に配慮するとともに、使用するシステムに伴うリスク（機密情報の漏洩や不正アクセス、データの改ざん、サービスの停止等）を踏まえた対策を講じた上で、オンライン診療を実施することが重要である。

※1 (略)

※2 (略)

1) 医療機関が行うべき対策

医療機関は、オンライン診療に用いるシステムによって講じるべき対策が異なることを理解し、オンライン診療を計画する際には、患者に対してセキュリティリスクを説明し、同意を得なければならない。医療機関は、システムは適宜アップデートされ、リスクも変わり得ることなど、理解を深めるべきである。

(2)～(4) (略)

(5) 通信環境（情報セキュリティ・プライバシー・利用端末）

①考え方

オンライン診療の実施に当たっては、利用する情報通信機器やクラウドサービスを含むオンライン診療システム（※1）及び汎用サービス（※2）等を適切に選択・使用するために、個人情報及びプライバシーの保護に配慮するとともに、使用するシステムに伴うリスクを踏まえた対策を講じた上で、オンライン診療を実施することが重要である。

※1 (略)

※2 (略)

1) 医師が行うべき対策

医師は、オンライン診療に用いるシステムによって講じるべき対策が異なることを理解し、オンライン診療を計画する際には、患者に対してセキュリティリスクを説明し、同意を得なければならない。医師は、システムは適宜アップデートされ、リスクも変わり得ることなど、理解を深めるべきである。

<p>1-1) <u>基本事項</u></p> <ul style="list-style-type: none"> ・ <u>医療機関は、オンライン診療に用いるシステムを提供する事業者（以下「事業者」という。）による説明を受け（システムに関する個別の説明を受けることのみならず、事業者が提示している情報提供内容を自ら確認することを含む）、十分な情報セキュリティ対策が講じられていることを確認すること。また、当該確認に際して、医療機関は責任分界点について確認し、システムの導入に当たっては、そのリスクを十分に理解すること。</u> ・ <u>オンライン診療の際、医療情報システム（※1）に影響を及ぼす可能性がある（※2）オンライン診療システムを使用する際は、「医療情報安全管理関連ガイドライン」に沿った対策を併せて実施すること。なお、汎用サービスを使用する際は、汎用サービスが医療情報システムに影響を与えない設定とすること。</u> <p>※1 <u>医療情報システムは、医療機関のレセプト作成用コンピュータ、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も対象として想定される。また、患者情報の通信が行われる院</u></p>	<p>1-1) <u>共通事項</u></p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p>
--	---

内・院外ネットワークも含む。

※2 例えば、電子カルテを利用する端末で、オンライン診療に用いるシステムを直接起動し、オンライン診療を行うと、セキュリティ上の問題が生じた場合、当該診療に係る患者だけではなく、電子カルテデータベースやそれと連結した医事システムやレセプト作成用コンピュータ内のすべての患者の情報に影響が及ぶ可能性がある。

- ・ 医療機関は、患者に対してオンライン診療の実施に伴うセキュリティリスクを説明し、オンライン診療に用いるシステムを利用することについての合意を得た上で、双方が合意した旨を診療録に記載し、オンライン診療を実施すること。
- ・ 「診療計画」を作成する際、患者に対して使用するオンライン診療システムに伴うセキュリティリスク等とその対策及び責任の所在について患者からの問い合わせに対応できるよう、説明文書の準備（ウェブサイト等の患者が適切にアクセスできる方法による開示や、電磁的記録による説明文書と同等の内容のもの提供を含む。）又は対応者の準備を行うこと。
- ・ オンライン診療システムを用いる場合は、医療機関

(新設)

(新設)

- ・ 「診療計画」を作成する際に、患者に対して使用するオンライン診療システムを示し、それに伴うセキュリティリスク等と対策および責任の所在について患者に説明し、合意を得ること。
- ・ OS やソフトウェア等を適宜アップデートすると

は OS やソフトウェアのアップデートについて、事業者と協議・確認した上で実施するとともに、アップデートができない等の個別対応が必要な場合には、事業者からの説明、情報提供等を受け、必要な対応を実施すること。

- ・ 医療機関は、必要に応じてセキュリティソフトをインストールすること。
- ・ オンライン診療に用いるシステムを使用する際には、多要素認証を用いるのが望ましい。
- ・ オンライン診療を実施する際は、患者がいつでも医師の本人確認及び医師の所属医療機関の確認ができるように必要な情報を準備すること。
- ・ オンライン診療システムを用いる場合は、患者がいつでも医師の本人確認ができる情報及び医療機関の問い合わせ先をオンライン診療システム上に掲載すること。
- ・ オンライン診療システムが後述の2)に記載されている要件を満たしていることを確認すること。
- ・ 医師がいる空間において診療に関わっていない者が診察情報を知覚できないこと。また、患者がいる空間に第三者がいないことを確認すること。ただし、患者がいる空間に家族等やオンライン診療支援者がいることを医師及び患者が同意している場合を除く。
- ・ 医師は、オンライン診療実施時に、意図しない第三

者に、必要に応じてセキュリティソフトをインストールすること。

(新設)

- ・ オンライン診療に用いるシステムを使用する際には、多要素認証を用いるのが望ましいこと。
- (新設)
- ・ オンライン診療システムを用いる場合は、患者がいつでも医師の本人確認ができるように必要な情報を掲載すること。
 - ・ オンライン診療システムが後述の2)に記載されている要件を満たしていることを確認すること。
 - ・ 医師がいる空間に診療に関わっていない者がいるかを示し、また、患者がいる空間に第三者がいないか確認すること。ただし、患者がいる空間に家族等やオンライン診療支援者がいることを医師及び患者が同意している場合を除く。
- (新設)

者が当該通信に紛れ込むような三者通信（患者が医師の説明と一緒に聞いてもらうために、医師の同意なく第三者を呼び込む場合等）や患者のなりすましが起こっていないことに留意すること。

- ・ プライバシーが保たれるように、患者側、医師側ともに録音、録画、撮影を同意なしに行うことがないよう確認すること。
- ・ オンライン診療においてチャット機能を補助的に用いる場合には、医療機関が、セキュリティリスクとベネフィットを勘案したうえで、使用するソフトウェアやチャット機能の使用方法について患者側に指示を行うこと。

- ・ 医療機関や患者から、検査結果画像や患者の医療情報等を画面共有機能を用いて提示すること及び画面共有機能を用いずに画面を介して提示することは、多くの場合、後述の場合と比較して相対的にセキュリティリスクが低減されているものと考えられる。一方で、患者から提示された二次元バーコードや URL 等のリンク先へのアクセス及びファイルのダウンロード等はセキュリティリスクが高いため、セキュリティリスクが限定的であることを医療機関が合理的に判断できる場合を除き、このようなアクセスやダウンロー

- ・ プライバシーが保たれるように、患者側、医師側ともに録音、録画、撮影を同意なしに行うことがないよう確認すること。
- ・ チャット機能やファイルの送付などを患者側に利用させる場合には、医師側（所属病院等の医療従事者、スタッフ等を含む）から、セキュリティリスクを勘案したうえで、チャット機能やファイルの送付などが可能な場合とその方法についてあらかじめ患者側に指示を行うこと。

（新設）

ド等を行わないことが望ましい。

- ・ オンライン診療を実施する医師は、オンライン診療の研修等を通じて、セキュリティリスクに関する情報を適宜アップデートすること。

(削る)

- ・ 医療機関が、オンライン診療を実施する際に、医療情報を取得する目的で外部のPHR等の情報を取り扱うことが、医療情報システムに影響を与える場合は、「医療情報安全管理関連ガイドライン」に沿った対策を実施しなければならない。他方で、医療機関が、医療情報システムに影響を与えずに当該情報を取り扱う場合には、セキュリティリスクについて医療機関と患者の間で合意を得た上で、オンライン診療を実施すること。

1-2) 医療機関が汎用サービスを用いる場合に特に留意すべき事項

医療機関が汎用サービスを用いる場合は、1-1)に加えて下記の事項を実施すること。

- ・ オンライン診療を実施する医師は、オンライン診療の研修等を通じて、セキュリティリスクに関する情報を適宜アップデートすること。

- ・ 患者が入力したPHRをオンライン診療システム等を通じて診察に活用する際には、当該PHRを管理する事業者との間で当該PHRの安全管理に関する事項を確認すること。

(新設)

1-2) 医師が汎用サービスを用いる場合に特に留意すべき事項

医師が汎用サービスを用いる場合は、1-1)に加えて下記の事項を実施すること。

・ 意図しない三者通信を防ぐため、医療機関から患者側につなげることを徹底し、また通信の管理者権限を患者に委譲しないこと。

・ 医療機関又は医療機関から委託を受けた者は、汎用サービスのセキュリティポリシーを適宜確認し、患者の問い合わせに対応できるようにすること。

(削る)

・ 個別の汎用サービスに内在するセキュリティリスクを理解し、必要な対策を講じる責任は医療機関にあり、委託を受けた者が存在する場合は、委託契約に基づき協力する責務が委託を受けた者に課されることを理解すること。

・ 端末立ち上げ時、パスワード認証や生体認証などを用いて操作者の認証を行うこと。

(削る)

(削る)

・ 医師側から患者側につなげることを徹底すること（第三者がオンライン診療に参加することを防ぐため。）。

・ 汎用サービスのセキュリティポリシーを適宜確認し、必要に応じて患者に説明すること。

・ 汎用サービスを用いる場合は、医師のなりすまし防止のために、社会通念上、当然に医師本人であると認識できる場合を除き、原則として、顔写真付きの「身分証明書」(マイナンバーカード、運転免許証、パスポート等。ただし、マイナンバー、住所、本籍等に係る情報は含まない。以下同じ。)と「医籍登録年」を示すこと (HPKI カードを使用するのが望ましい。)

・ オンライン診療システムを用いる場合と異なり、個別の汎用サービスに内在するリスクを理解し、必要な対策を行う責任が専ら医師に発生するというを理解すること。

・ 端末立ち上げ時、パスワード認証や生体認証などを用いて操作者の認証を行うこと。

・ 汎用サービスがアドレスリストなど端末内の他のデータと連結しない設定とすること。

1-3) 医師が医療情報システムに影響を及ぼす可能性が

<p>2) オンライン診療システム事業者が行うべき対策</p> <p>※ 医療機関は、下記を踏まえて、所属する医師が行うべきセキュリティリスク対策を講じること。</p> <p>事業者は、下記を備えたオンライン診療システムを構築し、下記の項目を満たすセキュリティ面で安全な状態を保つこ</p>	<p><u>あるシステムを用いる場合</u></p> <p><u>医療情報システムに影響を及ぼす可能性があるオンライン診療システムを用いる時は、1-1)に加えて下記の事項を実施すること。</u></p> <ul style="list-style-type: none"> ・ <u>医師は、オンライン診療システムにおいては、チャット機能やダウンロード機能を用いるリスクを踏まえて、原則使用しないこと（使用するシステム上、リスクが無害化されている場合を除く。）。</u> <u>（オンライン診療システムにおいては、システム提供事業者がこれらの機能の使用に関して提供する情報を踏まえて利用を行う。）</u> ・ <u>「医療情報安全管理関連ガイドライン」に沿った対策を行うこと。特に、医師個人所有端末の業務利用（BYOD）については、原則禁止と記載されていることについて留意すること。</u> <p>2) オンライン診療システム事業者が行うべき対策</p> <p>※ <u>医療機関の医療情報管理責任者は、下記を踏まえて、所属する医師が行うべきセキュリティリスク対策を講じること。</u></p> <p><u>オンライン診療システムを提供する事業者は、下記を備えたオンライン診療システムを構築し、下記の項目を満たすセ</u></p>
---	---

と。また、オンライン診療システムを医療機関が導入する際、事業者は、医療機関に対して、医療機関が十分に理解できるまで、オンライン診療システムのセキュリティ等（患者および医療機関がシステムを利用する際の権利、義務、情報漏洩・不正アクセス等のセキュリティリスク、医療機関・患者双方のセキュリティ対策の内容、患者への影響等）に関する説明を行うこと（分かりやすい説明資料等を作成し医療機関に提示することが望ましい。）。

2-1) 基本事項

- ・ 医療機関に対して、医療機関が負う情報漏洩・不正アクセス等のセキュリティリスク及びシステム障害時の診療への影響を明確に説明すること。
- ・ 事業者は医療機関に対して、オンライン診療のセキュリティに係る責任分界点について明確に説明し、合意した範囲において責任を負うこと。
- ・ オンライン診療システムの中にビデオ会議システム等の汎用サービスを組み込んだシステムにおいても、事業者はシステム全般のセキュリティリスクについて、医療機関に明確に説明し、合意した責任分界点の範囲において責任を負うこと。
- ・ 事業者は、合意に基づき、脆弱性などのセキュリティリスク発生時には速やかに医療機関に状況や対応方法等の情報提供を行うなどの善管注意義務を適切

キュリティ面で安全な状態を保つこと。また、オンライン診療システム事業者は、平易で理解しやすい形で、患者および医師がシステムを利用する際の権利、義務、情報漏洩・不正アクセス等のセキュリティリスク、医師・患者双方のセキュリティ対策の内容、患者への影響等について、医師に対して説明すること（分かりやすい説明資料等を作成し医師に提示することが望ましい。）。

2-1) 共通事項

- ・ 医師に対して、医師が負う情報漏洩・不正アクセス等のセキュリティリスクを明確に説明すること。

(新設)

- ・ オンライン診療システムの中に汎用サービスを組み込んだシステムにおいても、事業者はシステム全般のセキュリティリスクに対して責任を負うこと。

(新設)

に履行すること。

- ・ オンライン診療システム等が医療情報システムに影響を及ぼし得るかを明らかにすること。（*）
- ・ 医療情報システム以外のシステム（端末・サーバー等）における診療にかかる患者個人に関するデータの蓄積・残存の禁止（*）（2-2）に該当する場合を除く。）。
- ・ システムの運用保守を行う医療機関の職員や事業者、クラウドサービス事業者のアクセス権限を管理すること（ID/パスワードや生体認証、ICカード等により多要素認証を実施することが望ましい。またシステム運用監督者は退職者アカウントの削除など管理外になりやすい要素を重点的に監視すること。）。（*）
- ・ 不正アクセス防止措置を講じること（IDS/IPSを設置する等）。（*）
- ・ 不正アクセスやなりすましを防止するとともに、患者が医師の本人確認を行えるように、「1-1）基本事項」における医師の本人証明と医師の所属医療機関の確認が常に可能な機能を備えること。（*）
- ・ アクセスログの保全措置（ログ監査・監視を実施す

- ・ オンライン診療システム等が医療情報システムに影響を及ぼし得るかを明らかにすること。（*）
- ・ 医療情報システム以外のシステム（端末・サーバー等）における診療にかかる患者個人に関するデータの蓄積・残存の禁止（*）（2-2）に該当する場合を除く。）。
- ・ システムの運用保守を行う医療機関の職員や事業者、クラウドサービス事業者におけるアクセス権限の管理（ID/パスワードや生体認証、ICカード等により多要素認証を実施することが望ましい。）。（*）
- ・ 不正アクセス防止措置を講じること（IDS/IPSを設置する等）。（*）
- ・ 不正アクセスやなりすましを防止するとともに、患者が医師の本人確認を行えるように、顔写真付きの身分証明書と医籍登録年を常に確認できる機能を備えること（例えば、①不正アクセス等の防止のため、JPKIを活用した認証や端末へのクライアント証明書の導入、ID/パスワードの設定、②不正アクセス等の防止及び患者による医師の本人確認のため、HPKIカード等）。（*）
- ・ アクセスログの保全措置（ログ監査・監視を実施す

ることが望ましい。)(*)

- ・ 端末へのウィルス対策ソフトの導入、OS・ソフトウェアのアップデートを定期的に促す機能。(*)
- ・ 信頼性の高い機関によって発行されたサーバー証明書を用いて、通信の暗号化(TLS1.2以上)を実施すること。(*)
- ・ オンライン診療時に、複数の患者が同一の施設からネットワークに継続的に接続する場合には、IP-VPNやIPsec+IKEによる接続を行うことが望ましいこと。(*)
- ・ 遠隔モニタリング等で蓄積された医療情報については、「医療情報安全管理関連ガイドライン」に基づいて、安全に取り扱えるシステムを確立すること。(*)
- ・ 使用するドメインの不適切な移管や再利用が行われないように留意すること。

2-2) 医療情報システムに影響を及ぼす可能性があるシステムの場合

オンライン診療システムが、医療情報システムを扱う端末で使用され、オンライン診療を行うことで、医療情報システムに影響を及ぼす可能性がある場合、2-1)に加えて「医療情報安全管理関連ガイドライン」に沿った対策を行うこと。特に留意すべき点を例示として下記に示す。

- ・ 法的保存義務のある医療情報を保存するサーバーを

ることが望ましい。)(*)

- ・ 端末へのウィルス対策ソフトの導入、OS・ソフトウェアのアップデートの実施を定期的に促す機能。(*)
- ・ 信頼性の高い機関によって発行されたサーバー証明書を用いて、通信の暗号化(TLS1.2以上)を実施すること。(*)
- ・ オンライン診療時に、複数の患者が同一の施設からネットワークに継続的に接続する場合には、IP-VPNやIPsec+IKEによる接続を行うことが望ましいこと。(*)
- ・ 遠隔モニタリング等で蓄積された医療情報については、医療情報安全管理関連ガイドラインに基づいて、安全に取り扱えるシステムを確立すること。(*)
- ・ 使用するドメインの不適切な移管や再利用が行われないように留意すること。

2-2) 医療情報システムに影響を及ぼす可能性があるシステムの場合

オンライン診療システムが、医療情報システムを扱う端末で使用され、オンライン診療を行うことで、医療情報システムに影響を及ぼす可能性がある場合、2-1)に加えて医療情報安全管理関連ガイドラインに沿った対策を行うこと。特に留意すべき点を例示として下記に示す。

- ・ 法的保存義務のある医療情報を保存するサーバーを

国内法の執行が及ぶ場所に設置すること。（*）

- ・ 医療機関に対してそれぞれの追加的リスクに関して十分な説明を行い、事故発生時の責任分界点を明らかにすること。
- ・ 医療情報を保存するシステムへの不正侵入防止対策等を講ずること。（*）

また、オンライン診療システムは、上記の2-1)及び2-2)の(*)を満たしているシステムであるかどうか、第三者機関に認証されるのが望ましい。第三者機関の認証としては以下のいずれかが望ましい。

一般社団法人保健医療福祉情報安全管理適合性評価協会(HISPRO)、プライバシーマーク(JIS Q15001)、ISMS(JIS Q 27001等)、ITSMS(JIS Q 20000-1等)の認証、情報セキュリティ監査報告書の取得、クラウドセキュリティ推進協議会のCSマークやISMSクラウドセキュリティ認証(ISO27017)の取得

3) 患者に実施を求めるべき内容

医療機関はオンライン診療を活用する際は、「診療計画」の作成時に患者に対して、オンライン診療を行う際のセキュリティおよびプライバシーのリスクを説明し、特に下記が遵守されるようにしなければならない。また、患者側が負うべき責任があることを明示しなければならない。

国内法の執行が及ぶ場所に設置すること。（*）

- ・ 医師(医療機関の医療情報管理責任者)に対してそれぞれの追加的リスクに関して十分な説明を行うこと。
- ・ 医療情報を保存するシステムへの不正侵入防止対策等を講ずること。（*）

また、オンライン診療システムは、上記の2-1)及び2-2)の(*)を満たしているシステムであるかどうか、第三者機関に認証されるのが望ましい。第三者機関の認証としては以下のいずれかが望ましい。

一般社団法人保健医療福祉情報安全管理適合性評価協会(HISPRO)、プライバシーマーク(JIS Q15001)、ISMS(JIS Q 27001等)、ITSMS(JIS Q 20000-1等)の認証、情報セキュリティ監査報告書の取得、クラウドセキュリティ推進協議会のCSマークやISMSクラウドセキュリティ認証(ISO27017)の取得

3) 患者に実施を求めるべき内容

医師はオンライン診療を活用する際は、「診療計画」の作成時に患者に対して、オンライン診療を行う際のセキュリティおよびプライバシーのリスクを説明し、特に下記が遵守されるようにしなければならない。また、患者側が負うべき責任があることを明示しなければならない。

3-1) 基本事項

(略)

3-2) 医療情報システムに影響を及ぼしうるケース (医療機関が判断の上、患者に通知した場合に限る)

- ・ 原則、医療機関が求めない限り、あるいは指示に反して、チャット機能の利用やファイルの送付などを行わないこと。特に外部 URL への誘導を含むチャットはセキュリティリスクが高いため行わないこと。

(削る)

3. その他オンライン診療に関連する事項

(略)

3-1) 共通事項

(略)

3-2) 医療情報システムに影響を及ぼしうるケース (医師が判断の上、患者に通知した場合に限る)

- ・ 原則、医師側が求めない限り、あるいは指示に反して、チャット機能の利用やファイルの送付などを行わないこと。特に外部 URL への誘導を含むチャットはセキュリティリスクが高いため行わないこと。

3-3) 初診でオンライン診療を用いる場合

- ・ 患者は、顔写真付きの身分証明書で本人証明を行うこと。顔写真付きの身分証明書を有しない場合は、2種類以上の身分証明書を用いて本人証明を行うこと。

3. その他オンライン診療に関連する事項

(略)