西村あさひ法律事務所

臨床試験に関する GDPR 上の論点

個人情報保護・データ保護規制ニューズレター　2022 年 5 月 26 日号

執筆者:
E-mail 岩瀬　ひとみ
E-mail 菊地　浩之
E-mail 河合　優子
E-mail 村田　知信
E-mail 五十嵐　チカ
E-mail 松本　絢子
E-mail 菅　悠人
E-mail 小出　章広

目次

Ⅰ　臨床試験に関する GDPR 上の問題点

はじめに

臨床試験を実施する際には、被験者の健康に関する情報を含む個人データの処理を行うことになるため、適用のある個人情報保護・データ保護規制を遵守しつつ臨床試験を実施することが求められる。他方で、臨床試験の実施にあたっては、いわゆるグッド・クリニカル・プラクティスといった諸基準を定めた医療関係の各種法令を遵守する必要もある。すなわち、欧州において臨床試験を実施する場合には、EU 規則である GDPR に加えて、同じく EU 規則である臨床試験に関する規制を定めている臨床試験規則(CTR)の遵守も必要となる。この点、CTR は、GDPR と類似した義務を課している場合もあり、このような場合、いずれの義務とも遵守することができるように、それぞれの義務の関係を理解した上で対応を検討することが重要である。以下では、GDPR の適用範囲とスポンサー及び実施医療機関の GDPR 上の位置づけについて整理した上で、個人データの処理の適法性根拠をどのように考えるか、その他 GDPR 上どのような点に留意する必要があるかについて解説する。

1.　GDPR の適用範囲

欧州経済領域(EEA)の域外にある製薬会社等の事業者が EEA 域内において臨床試験を実施する場合に、当該臨床試験における個人データの処理が GDPR の適用を受けるかについては、従前から見解の対立が存在していた。GDPR は、①EEA 域内の拠点の活動の過程で個人データを処理する場合、②EEA 域内のデータ主体に対する物品又はサービスの提供(無償のものを含む)に関連して、EEA 域内のデータ主体の個人データを処理する場合、及び③EEA 域内で行われるデータ主体の行動の監視に関連して、EEA 域内のデータ主体の個人データを処理する場合に適用される(GDPR3 条)。事業者が EEA 域内に拠点を有していない場合や、EEA 域内の拠点が臨床試験に関与しない場合等には、①EEA 域内の拠点の活動の過程で個人データを処理する場合に該当しない。この場合には、当該事業者が、③の EEA 域内で行われるデータ主体の行動の監視に関連して、EEA 域内のデータ主体の個人データを処理しているとされるかが問題となる。すなわち、欧州データ保護評議会(EDPB)は、GDPR の地理的適用範囲に関するガイドラインにおいて、データ主体の行動の監視に該当する場合として、個人の健康状態の監視又は定期的な

報告を挙げており[1]、臨床試験の過程で行われる個人データの処理はこれに含まれるとも考えられるところである。この点、近時、EEA 域外・英国国外の事業者が EEA 域内・英国国内において臨床試験を実施する場合の GDPR の適用の有無について、34 のデータ保護当局への照会による調査が行われたが、当該調査によれば、フランスやイタリア、英国等の 16 のデータ保護当局が GDPR の適用があると回答、ベルギーやオランダ等の 8 のデータ保護当局が GDPR の適用の有無は個別具体的に判断されると回答し、GDPR の適用がないと回答したデータ保護当局は 0(ポーランドやスペイン等の 10 のデータ保護当局は未回答)との結果であった[2]。かかる調査結果を踏まえると、EEA 域外・英国国外の事業者が EEA 域内・英国国内において臨床試験を実施する場合には、たとえ臨床試験の実施作業自体は全て現地の実施医療機関や CRO によって行われるものであるとしても、基本的には EEA・英国の域外にあるスポンサーに対して GDPR の適用があることを前提として対応を行うことが慎重であると考えられる。

なお、スポンサーが GDPR の域外適用を受ける場合、EEA 域内のデータ主体やデータ保護当局からスポンサーへのアクセス可能性を損なうことがないように、EEA 域内に代理人を選任する必要がある(GDPR27 条 1 項)。他方で、CTR においても、スポンサーが EEA 域外に所在する場合には、EEA 域内に代理人を選任することが義務付けられている(CTR74 条 1 項)。この点、CTR に基づく代理人は、スポンサーの CTR 上の義務の履行を確保し、スポンサーに対して CTR に基づいて行われる連絡の窓口となる役割を担うのに対し、GDPR に基づく代理人は、スポンサーによる GDPR の遵守を確保するために、個人データの処理と関連する事項について、データ主体やデータ保護当局との連絡窓口となる役割を担っており、CTR の遵守を確保するための地位であるか、GDPR の遵守を確保するための地位であるかという点でそれぞれ役割が異なっているため、これら代理人はいずれも別々に選任する必要がある。GDPR に基づく代理人と CTR に基づく代理人は、兼任することも禁止されていないが、実務上は、役割の違いによる利益相反を回避するために、別々の者を選任することが多いとも言われている。

2. スポンサー及び実施医療機関の GDPR 上の位置づけ

GDPR においては、個人データの処理の目的及び方法を決定する者である管理者が一次的なデータ保護義務を負い、管理者のために個人データの処理を行う処理者も、GDPR に基づく一部の義務を負うこととされている。臨床試験の実施のために必要となる個人データの処理との関係では、治験実施計画を策定するスポンサーが、個人データの処理の目的を決定するとともに、処理する個人データの種類や、処理の期間、個人データにアクセスできる者の範囲、誰の個人データを処理するか等の、個人データの処理の方法を決定することとなるため、スポンサーは管理者に該当すると考えられる。もっとも、実施医療機関の GDPR 上の位置づけは、スポンサーと比較して必ずしも明確ではなく、実施医療機関がスポンサーとともに GDPR における共同管理者の関係に立つのか、あるいは、スポンサーのみが単独で管理者となり、実施医療機関は処理者として位置づけられるのか、という問題がある。この問題に対して、EDPB は、GDPR における管理者及び処理者の概念に関するガイドラインにおいて、実施医療機関がスポンサーと共同で治験実施計画を決定している場合には、スポンサーと実施医療機関は共同管理者の関係に立ち、スポンサーが単独で治験実施計画を決定している場合には、スポンサーのみが単独で管理者となり、実施医療機関は処理者となるとの見解を示している[3]。日本企業がスポンサーとなって複数の実施医療機関とともに同様の治験実施計画の下で臨床試験を実施するような場合であれば、実施医療機関は処理者と位置づけられることが多いと思われるが、ケースバイケースであり、実務的に定まった扱いは存在しないというのが現状であると思われる。実施医療機関が処理者となる場合には、当該実施医療機関が適切な技術的・組織的措置を備えているか確認した上で GDPR28 条 3 項の要件を満たすデータ処理契約を締結することが必要となるのに対し、実施医療機関がスポンサーとの共同管理者となる場合には、GDPR26 条 1 項に従い共同管理者契約を締結することが必要となるため、スポンサー及び実施医療機関の GDPR 上の位置づけについては、スポンサーの側でもあらかじめ検討の上、整理しておく必要がある。

---

1 European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 12 November 2019, p.20,* available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf

2 https://iapp.org/news/a/how-does-the-gdpr-apply-to-clinical-trial-sponsors-outside-the-eea-views-of-eea-dpas/

3 European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR Adopted on 2 September 2020, p.21-22,* available at https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

3. データ処理の適法性根拠

GDPR は、個人データの処理を原則的に禁止した上で、GDPR6 条 1 項に掲げられている、データ主体の同意や法的義務の遵守、正当な利益等の適法性根拠のいずれかを充足する場合に限り個人データの処理を許容しているため、臨床試験の実施に伴い個人データを処理するためには、GDPR6 条 1 項に掲げられている適法性根拠のうちいずれに依拠するかを検討する必要がある。加えて、臨床試験においては、処理の対象となる個人データに被験者の健康に関する情報が含まれることになる。健康に関する情報は、GDPR9 条 1 項のセンシティブデータに該当するため、GDPR9 条 2 項に掲げられている、データ主体の明示的な同意等の、センシティブデータに特有の適法性根拠も充足する必要があることになる。

EDPB は、CTR と GDPR との交錯に関する Q&A に係る意見において、CTR 又は関連する国内法に基づく個人データの処理で、信頼性・安全性を確保するために行われるものについては、GDPR6 条 1 項(c)の法的義務の遵守(センシティブデータについては GDPR9 条 2 項(i)の公衆衛生の分野における EU 法又は EEA 加盟国の国内法に基づく公共の利益)が適法性根拠になるとの見解を示している [4]。CTR 又は関連する国内法に基づく個人データの処理で、信頼性・安全性を確保するために行われるものに該当する例としては、例えば、CTR41 条から 43 条に規定されている安全性レポートに関する義務の履行や、CTR58 条に基づく臨床試験マスターファイル及び医療ファイルの保管、関連する国内法に基づく監査目的での当局への臨床試験データの開示が挙げられている [5]。

他方で、EDPB は、臨床試験において調査・研究の目的で行われる個人データ処理については、GDPR6 条 1 項(a)の同意(センシティブデータについては GDPR9 条 2 項(a)の明示的な同意)、GDPR6 条 1 項(e)の公共の利益又は同項(f)の正当な利益(センシティブデータについては GDPR9 条 2 項(i)の公衆衛生の分野における EU 法又は EEA 加盟国の国内法に基づく公共の利益又は同項(j)の EU 法又は EEA 加盟国の国内法に基づく GDPR89 条 1 項に従って行われる科学的研究)が適法性根拠になるとの見解を示している [6]。ただし、同意については、GDPR 上、任意になされたものであることが求められているところ(GDPR4 条(11))、EDPB は、被験者の健康状態が不良である場合や経済的・社会的に不利な立場にある場合、制度的・階層的な依存関係に置かれている場合のように、被験者とスポンサー・実施医療機関との力関係に不均衡がある場合には、通常は同意に任意性が認められないことを指摘している [7]。このため、適法性根拠として同意に依拠する場合には、同意の任意性を確保することができるよう留意する必要がある。なお、CTR においては、臨床試験への参加・不参加の意思決定に関連する情報を全て提供した上で、臨床試験に参加し、治療を受けることについて、被験者の同意を取得することが求められている(CTR28 条 1 項(b)、2 条 2 項(21))が、CTR 上の同意は、あくまでも臨床試験への参加と、副作用等の可能性も認識した上で治療を受けることに関する同意(いわゆるインフォームド・コンセント)であって、個人データの処理に関する同意ではないため、個人データの処理に関する GDPR 上の同意を取得するためには、管理者の身元、処理の目的、個人データの種類、及び同意撤回権の存在等の個人データの処理に関する情報を提供する等して、GDPR の要件を満たす必要がある。

4. その他の GDPR 上の留意点

GDPR 上、データ処理が個人の権利及び自由に対する高いリスクを発生させるおそれがある場合には、データ保護影響評価(DPIA)を行うことが義務付けられている。GDPR35 条 3 項(b)は、センシティブデータ(及び犯罪に関するデータ)の大規模な処理を行う場合には、DPIA の実施が義務付けられる旨を規定しており、また、EDPB の前身である 29 条作業部会は、DPIA に関するガイドラインにおいて、臨床試験における地位の弱いデータ主体に関する仮名化されたセンシティブデータを記録保存のために保管することが、「個人の権利及び自由に対する高いリスクを発生させるおそれがある場合」に該当する可能性が高い例として挙げて

---

4 European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) Adopted on 23 January 2019, p.4,* available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf

5 European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) Adopted on 23 January 2019, p.5.*

6 European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) Adopted on 23 January 2019, p.5.*

7 European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) Adopted on 23 January 2019, p.6.*

いる[8]。このため、臨床試験を大規模に行う場合や、健康状態が不良な者、高齢者や子どもといった地位の弱いデータ主体を臨床試験の主な対象としているような場合には、DPIA が必要となる可能性が高いと考えられる。

また、GDPR 上、センシティブデータの大規模な処理を中心的業務とする場合には、データ保護責任者(DPO)を選任することが義務付けられている。センシティブデータの処理を必然的に伴う臨床試験を大規模に行う場合には、DPO の選任も必要になると考えられるので、留意する必要がある。

なお、CTR28 条 2 項は、被験者(被験者が同意を与えることができない場合はその法定代理人)の同意を得て、臨床試験を通じて取得したデータを、科学的目的のために限り、治験実施計画の範囲を超えて二次的に利用することを許容している。この点、GDPR5 条 1 項(b)は、当初の目的に適合しない態様で個人データの追加的な処理を行ってはならないが、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために行われる追加的な処理は、GDPR89 条 1 項に従う限りは、当初の目的に適合しないものとはされないことを規定している。EDPB は、CTR と GDPR との交錯に関する Q&A に係る意見において、臨床試験を通じて取得した個人データの科学的目的のための二次的な利用がいかなる条件の下で許容されるかについては、今後の EDPB によるガイダンスを待つ必要があるが、当面の間は、GDPR89 条 1 項に従う限りは、かかる二次的な利用は当初の目的と適合するものと推定されるものと考えるべきであるとの見解を示している[9]。このため、臨床試験を通じて取得した個人データを科学的目的のために二次的に利用する場合には、データ主体である被験者がかかる二次的利用を合理的に予測できるかを検討した上で、(特にデータ最小化の原則の遵守を確保するための)適切な技術的・組織的措置の実施を求めている GDPR89 条 1 項を遵守していると評価されるような措置を講じておくことが望ましいと考えられる。

Ⅱ 個人情報保護・データ保護規制 各国法アップデート

1. 日本

・ 「デジタル社会の形成を図るための関係法律の整備に関する法律」第 51 条により、地方公共団体等における個人情報等の取扱いに関する規律が個人情報保護法に定められることになる。同条による改正は 2023 年 4 月 1 日に施行される。これに関連して、2022 年 4 月 20 日、「個人情報の保護に関する法律施行令等の一部を改正する政令」が公布されるとともに新旧対照表が公表され、また、「個人情報の保護に関する法律施行規則の一部を改正する規則」及び「個人情報の保護に関する法律についてのガイドライン(行政機関等編)の一部を改正する告示」が公表された。いずれも、2023 年 4 月 1 日に施行される。これらの改正案に対する意見募集の結果も公表されている。

・ 個人情報保護委員会は、2022 年 4 月 28 日、「個人情報の保護に関する法律についての事務対応ガイド(行政機関等向け)」の改正版及び「個人情報の保護に関する法律についてのQ＆A(行政機関等編)」の改正版を公表した。これらも 2023 年 4 月 1 日に施行される。

2. 中国

・ 2022 年 4 月 29 日、「ネットワーク安全標準実践ガイドライン(意見募集稿)」が公表され、2022 年 5 月 13 日まで意見募集が行われた。

3. 欧州

・ 2022 年 5 月 4 日、欧州データ保護評議会(EDPB)及び欧州データ保護監督機関(EDPS)は、データ法案(Data Act)に関する共同意見を公表した。データ法案の内容については、ヨーロッパニューズレター(2022 年 2 月 25 日号)を参照。EDPB 及び

---

8 Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, p.11,* available at https://ec.europa.eu/newsroom/article29/items/611236/en

9 European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) Adopted on 23 January 2019, p.8.*

EDPS の共同意見は、個人データの保護の観点から、データ法案の改善点を指摘している。例えば、製品等の利用者がデータ主体と異なる者である場合、製品等の利用者は、GDPR や e プライバシー指令を含むデータ保護に関する法令に従う場合に限って生成されたデータを利用できる旨を明確化すべきであることや、製品等の利用者がデータ主体と異なる者である場合に、製品等の利用者により生成されたデータの利用に制限を加えること、公的機関に対してデータを利用可能とする義務の発生要件となる「緊急事態」の範囲をより明確に規定すること等が提案されている。

- 欧州司法裁判所は、2022 年 4 月 28 日、ドイツの消費者保護団体が、利用者への情報提供の仕方が不当(unfair)だとして、Meta Platforms Ireland Limited に対して差止訴訟を提起した事件において、同団体がデータ主体からの委任を受けることなく、かつデータ主体の特定の権利侵害を取り上げるわけでもなく代表訴訟(representative action)を提起できるか、という論点に関する判決を下した。同判決では、GDPR80 条 2 項において、加盟国には、データ主体から個別の委任を受けていない消費者保護団体等による訴えの提起を許容する法令を制定する裁量が認められていることを挙げた上で、消費者たるデータ主体の権利及び自由の保護等の公共目的を追求する消費者保護団体が個人の権利に影響を与えるデータ処理についての法的責任を問う場合には、データ主体からの委任を受けることなく、またデータ主体が被る損害も証明することなく代表訴訟を提起できる旨が判示されている。

- 2022 年 5 月 3 日、欧州委員会は、ヘルスデータ空間に関する規則案を公表した。同法案は、①自然人の電子ヘルスデータに関するアクセス及びコントロールを、ヘルスケアの文脈において(一次利用)、及び研究やイノベーション等の他の文脈において(二次利用)強化するとともに、②EU の価値に従い、電子ヘルスレコードシステム(HER システム)の開発・マーケティング・利用に係る統一的な法的枠組みを定めることにより、EU 域内市場の機能を向上させることが目指されている。産業界への利点としては、(i)標準化により他の EU 加盟国内の新たな電子ヘルスレコード(electronic health records)市場への参入が容易になること、(ii)識別不可能な電子ヘルスデータがより利用可能になることでイノベーションのためのデータ利用が可能となることが挙げられている。

4. 米国

- 2022 年 4 月、バージニア州において Virginia Consumer Data Protection Act (VCDPA)を修正する改正法が成立し、またケンタッキー州及びメリーランド州においてそれぞれ保険会社等に適用され得るデータ保護法が制定される等、複数の州法に動きがあった。さらに、ノースカロライナ州では、全米の州法としては初めて、州政府関連機関(州立大学等、州政府が監督責任を負う機関を含む)が、ランサムウェアによる攻撃を受けた場合において、脅迫に応じて攻撃者に金銭を支払うこと及び攻撃者との間で交渉等を行うことを禁止し、かかる場合には州政府内の担当機関に対して報告することを義務付ける州法が成立した。また、5 月に入り、コネティカット州では、州レベルの包括的なデータ保護法である Act Concerning Personal Data Privacy and Online Monitoring が成立した(施行は 2023 年 7 月 1 日とされている)。

5. インド

- インドコンピュータ緊急対応チーム(The Indian Computer Emergency Response Team, CERT-IN)は、2022 年 4 月 28 日、2000 年情報技術法第 70B 条(6)に基づき、情報セキュリティの実践、手順、予防、対応、サイバーセキュリティインシデントの報告義務等に関する新しい指令を発表した。本指令は発表から 60 日後に施行される予定である。

6. タイ

- タイでは、2022 年 5 月 10 日にデジタル経済社会省のウェブサイトにおいて個人情報保護法の下位規則の草案 3 本が公表され、同月 19 日までパブリックコメントが募集されていた。これらの草案は、①個人データ処理記録義務が免除される小規模事業者、②処理者の個人データ処理記録義務の内容及び③最低限の安全管理義務の内容を定めるものである。また、同月 19 日には新たに④データ主体からの同意取得及び⑤プライバシーノーティスに関する下位規則の草案 2 本が公表され、同月 25 日までパブリックコメントが募集されている。なお、2022 年 6 月 1 日から施行予定のタイの個人情報保護法については、2022 年 4 月にタイの民間企業の団体である JSCCIB(Joint Standing Committee on Commerce, Industry and Banking, Thailand)がタイ当局に対して更なる施行延期を求めるレターを提出したが、同年 5 月 20 日時点でタイ当局から更なる延期

に関するアナウンスメント等はされていない。

7. オーストラリア

・ 2022 年 4 月 22 日、オーストラリア連邦政府は、Data Security Action Plan に関するディスカッションペーパーを公表し、2022 年 6 月 10 日までの間、意見募集手続が行われている。ディスカッションペーパーでは、データに対する不正なアクセスを防ぐための政策がテーマであり、責任を政府、企業、産業界がどのように分担するのが適切かなど、施策のあるべき姿を議論している。

8. ニュージーランド

・ 2022 年 4 月 6 日、プライバシー・コミッショナーは、the Health Information Privacy Code(HIPC)の改正案を公表し、2022 年 5 月 4 日までの間、意見募集手続が行われた。HIPC は、保健分野における個人情報保護の原則を定めるものであり、保健機関が収集する個人情報の収集、使用、保管及び開示について規定している。本改正案は、ニュージーランド国民の健康を向上することを目的とする the Pae Ora (Healthy Futures) Bill が 2022 年 7 月 1 日に施行されることに伴うものである。

9. メキシコ

・ 2022 年 4 月 25 日、メキシコの最高裁判所(SCJN)は、携帯電話利用者登録制度(PANAUT)を創設する政令を無効とする判決を下した。PANAUT は、携帯電話利用者に対して、当局が求めた場合に、当該携帯電話利用者の個人情報や機密情報を提供することを義務付けるものであるが、当該義務の範囲が不明瞭であること等を理由に、プライバシーや個人情報の保護に関する基本的権利を不当に侵害するものと判断された。

10. カタール

・ カタール国内に設けられたフリーゾーンのひとつである Qatar Financial Centre では、2021 年 12 月 21 日、Data Protection Regulations 2021 及び Data Protection Rules 2021 が公布され、2022 年 6 月から施行予定である。いずれも現行の 2005 年版を改正したもので、概ね GDPR と平仄を合わせる形で改正されている。GDPR との主な相違点として、データ管理者は個人データ侵害をデータ主体に通知する義務を負わないことが挙げられる。

11. アフリカ

・ データ保護当局ネットワーク(“The Network of African Data Protection Authorities”)とスマートアフリカアライアンス(“Smart Africa Alliance”)は、アフリカにおいて調和の取れたデータ保護政策及びデータ保護規則の制定を推進するため、基本合意書を締結し、同合意書は 2022 年 3 月 10 日に効力発生した。このパートナーシップにより、アフリカ諸国は、データ保護規則の制定やデータ保護当局の設立等に際し、支援を得ることが可能となった。

西村あさひ法律事務所 広報室 E-mail