

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

중국 의료데이터 국외이전 규제에 관한 연구

— 베이징우의병원과 암스테르담대학교 의학센터의

공동연구 프로젝트를 분석대상으로 —

A Study on the Regulation of Cross-Border Transfer of Medical Data in China: An Analysis of the Collaborative Research Project between Beijing Friendship Hospital and Amsterdam UMC

마봉초(马鹏超)(인하대학교 법학과 박사생)

MA, Pengchao (Doctoral Student, Dept. of Law, Graduate School, Inha University)

목 차

I. 서론

- 연구대상
- 연구범위
- 의료데이터의 개념 확정
- 논문의 구성

II. 사건의 사실관계

- 사건 식별과 신고 경로
- 당사자
- 관련 공동연구 프로젝트
- 사건의 핵심 시간선
- 관련 데이터
- 데이터 흐름

7. 신고 및 심사 절차
8. 피험자 동의 문제
9. 공개자료상 확인되지 않는 사항

III. 법원(法源)

1. 법률
2. 행정법규
3. 부문규장
4. 지방성법규와 규범성 문건

IV. 데이터 분류등급 보호제도의 본 사건에서의 적용과 전개

1. 데이터 분류등급 보호제도의 규범적 기초
2. 본 사건 심사 시점에 적용된 분류등급 프레임워크
3. 본 사건 분류등급 판정의 관찰 가능한 사실: 병원 내부 3 단계
4. GB/T 43697-2024 「데이터안전기술 데이터 분류등급 규칙」의 체계적 해석
5. 본 사건과 관련된 그 밖의 데이터안전 기술표준
6. GB/T 43697-2024 방법에 따른 본 사건 데이터의 단계별 식별
7. 본 사건 심사 후 신설된 분류등급 규칙과 컴플라이언스 지속 단계
8. 분류등급과 네트워크안전등급보호의 본 사건에서의 연계
9. 소결: 규범 미완성 — 사실 선행

V. 네트워크안전등급보호제도에 의한 본 사건의 국내 시스템 보장

1. 네트워크안전등급보호제도의 규범적 기초
2. 네트워크안전등급보호제도 2.0 표준의 내용
3. 의료기관의 등급보호제도 시행과 본 사건 베이징우의병원의 등급보호 현황

4. 등급보호제도 2.0 과 본 사건 데이터 국외이전 신고의 연계관계

5. 등급보호제도와 그 밖의 규범의 병행적용 관계

VI. 의료데이터 전(全)생애주기 컴플라이언스의 매트릭스 집성

1. 전생애주기 관리의 규범적 기초

2. 본 사건에 적용되는 8 개 단계

3. 국외이전 단계와 상류 단계의 의존관계

4. 8 개 단계의 적용규범 매트릭스

VII. 본 사건 데이터 국외이전의 관할과 법적 책임

1. 중국 측의 규제관할과 법적 책임

2. EU·네덜란드 측의 규제관할

3. 두 관할체계의 교착과 충돌

4. 본 사건 규제관할의 전체상

VIII. 결론과 전망

1. 연구의 회고와 본 사건의 표본가치

2. 본 사건의 사실 제시가 도출하는 핵심 발견

3. 향후 연구방향

I. 서론

1. 연구대상

본 연구는 수도의과대학 부속 베이징우의병원(이하 ‘베이징우의병원’)과 네덜란드 암스테르담대학교 의학센터(Amsterdam University Medical Center, 이하 ‘Amsterdam UMC’) 사이의 국제 다기관 임상연구 협력 프로젝트를 연구대상으로 한다. 이 프로젝트는 2023 년 1 월 베이징시 인터넷정보판공실의 공시를 거쳐 공시번호 20220001 을 부여받았으며, 「데이터 국외이전 안전평가 방법」(2022 년 9 월 1 일 시행) 시행 이래 전국 최초로 데이터 국외이전

안전평가를 통과한 사례가 되었다.¹

이 협력 프로젝트는 실제로는 두 개의 독립된 국제 다기관 임상연구를 포함한다.

첫째, COLOR III 연구(‘중·하부 직장암에 대한 경향문 전직장간막절제술과 복강경 전직장간막절제술의 다기관 무작위 임상대조연구’, ClinicalTrials.gov 등록번호 NCT02736942)이다. 이 연구의 의뢰자(sponsor)는 Amsterdam UMC(구체적 등록주체는 Amsterdam UMC, location VUmc)이고, 등록번호는 2015.449이며, 2016년 12월부터 수행되었다.² 베이징우의병원 일반외과센터는 2018년 7월 초청을 받아 이 연구에 참여하였다.³ 2022년 4월 기준 베이징우의병원은 COLOR III 연구에서 전 세계 최초로 100례 등록을 돌파한 연구센터가 되었다.⁴

둘째, COLOR IV 연구(‘복강경 우측 결장암 절제술 후 복강내 문합과 복강외 문합을 비교하는 전향적·다기관·무작위 대조 임상연구’, ClinicalTrials.gov 등록번호 NCT05493033)이다. 이 연구의 의뢰자는 베이징우의병원으로(COLOR III와는 반대이다), 베이징우의병원 부원장 겸 일반외과센터 주임인 장중타오(张忠涛) 교수와 Amsterdam UMC 일반외과 H. Jaap Bonjer 교수가 공동으로 책임연구자(PI)를 맡았다. 연구계획서는 2025년 2월 Surgical Endoscopy지에 정식 게재되었으며, 재원에는 중국 국가중점연구개발계획 2017YFC0110904(2017년 과제 선정) 등이 포함된다.⁵ 이 연구는 참여기관

¹北京市卫生健康委员会：《全国首个获批数据出境安全评估案例落地北京友谊医院》，2023年2月2日，
https://wjw.beijing.gov.cn/xwzx_20031/jcdt/202302/t20230202_2910980.html。

²ClinicalTrials.gov, NCT02736942, "COLOR III Trial: Transanal vs Laparoscopic TME", Sponsor: Amsterdam UMC, location VUmc, Org Study ID 2015.449, Start Date: 2016-12-02.<https://clinicaltrials.gov/study/NCT02736942>

³北京市卫生健康委员会：《全国首个获批数据出境安全评估案例落地北京友谊医院》，2023年2月2日，
https://wjw.beijing.gov.cn/xwzx_20031/jcdt/202302/t20230202_2910980.html。

⁴北京市卫生健康委员会：《全国首个获批数据出境安全评估案例落地北京友谊医院》，2023年2月2日，
https://wjw.beijing.gov.cn/xwzx_20031/jcdt/202302/t20230202_2910980.html。

⁵Wu S, Wei P, Gao J, Shu W, Zhao H, Bonjer H, Tuynman J, Yao H, Zhang Z; COLOR IV study group. COLOR

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구
30~50 개소를 예정하고, 연구계획상 1,158 레의 환자를 등록할 계획이며(공개 보도에는 약 1,200 레라는 개괄적 표현도 있다), 2030 년까지 지속될 예정이다.

두 연구의 구조는 동일하다. 모두 베이징우의병원이 중국 내 제공자이고 Amsterdam UMC 가 국외 수령자이며, 데이터의 흐름도 일치한다. COLOR IV 연구는 번호 20220001 로 신고·평가된 데이터 국외이전 사안과 중국 내 제공자 및 국외 수령자가 동일하고, 그 등록 및 개시 시점 역시 해당 신고 시점과 매우 밀접하게 중첩된다. 감독기관이 해당 평가대상의 구체적 범위를 문서로 공표하지는 않았으나, 신고 책임자의 공개 설명에 따르면 본 신고·평가의 대상은 양 기관이 공동으로 구축한 데이터 국외이전 플랫폼, 즉 양 기관 협력 전체에 봉사하는 데이터 국외이전 체계이며, 두 연구는 모두 그 안에 포함된다.⁶ 본 연구는 두 연구의 주체와 데이터 흐름의 동일성에 근거하여 COLOR III 를 본 사건의 핵심 사실기반으로 삼고, COLOR IV 를 본 사건의 컴플라이언스 지속 시나리오로서 함께 분석에 포함한다.

2. 연구범위

본 연구는 본 사건과 관련된 중국법 적용 문제만을 정리한다. 본 연구는 ‘사실을 먼저, 규범을 나중에’라는 분석순서를 취한다. 즉 먼저 본 사건의 객관적 사실을 제시한 다음, 본 사건 각 단계에 적용되는 중국법 규범을 정리한다. 시간적 범위는 2017 년(COLOR IV 의 중국 측 재원이 의존하는 국가중점연구개발계획 과제가 선정된 해이며, 그 시험 자체는 2022 년에 임상시험 등록을 마치고 2025 년에 계획서가 정식 간행되었다)부터 현

IV: a multicenter randomized clinical trial comparing intracorporeal and extracorporeal ileocolic anastomosis after laparoscopic right colectomy for colon cancer. Surg Endosc. 2025 Feb;39(2):1182-1190. doi: 10.1007/s00464-024-11412-7. Epub 2024 Dec 28. PMID: 39733171; PMCID: PMC11794397.

⁶姚宏伟:《北京友谊医院数据出境安全评估案例申报经验分享与落地实践》(2023 年中欧数字领域二轨对话会议专题发言, 2023 年 3 月 24 日), 载澎湃新闻, 2023 年 4 月 3 日。해당 발표는 신고 대상이 베이징우의병원과 Amsterdam UMC 가 공동으로 구축한 데이터 국외이전 플랫폼임을 밝히고, "신고한 프로젝트는 전국 00001 호이고, 승인된 것도 00001 호"라고 명시하였다.

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

단계까지이다. 이 기간은 중국 데이터 거버넌스 입법체계가 무(无)에서 유(有)로, 점진적으로 정비되어 온 전 과정을 포괄하므로, 본 사건의 컴플라이언스 과정은 실제로 서로 다른 여러 시기의 규범상태를 거쳤다. 본 연구가 단일 사건을 연구대상으로 삼는 방법론적 기초는 본 사건의 삼중의 대표성에 있다. 첫째, 본 사건은 「데이터 국외이전 안전평가 방법」 시행 이래 전국 최초로 데이터 국외이전 안전평가를 통과한 사건으로서 제도 운용의 기점이라는 표본적 의의를 가진다. 둘째, 본 사건은 법원(法源)·분류등급·등급보호·전생애주기·국경 간 관할의 각 규범 차원을 가로지르므로, 의료데이터 국외이전 규제의 전체 구조를 온전히 드러내기에 충분하다. 셋째, 본 사건의 시간적 범위가 마침 중국 데이터 거버넌스 입법의 체계화 과정과 겹치므로 ‘언제 어떤 법이 적용되는가’라는 시간축 분석이 가능해진다. 단일 사건의 심층기술(深层记述)만으로도 규제구조에 대한 전체적 관찰을 담아내기에 충분한 이유가 여기에 있다.

3. 의료데이터의 개념 확정

본 연구는 ‘의료데이터 국외이전 규제’를 연구대상으로 한다. 그러나 ‘의료데이터’는 중국 현행법상 단일하고 통일된 법정 개념이 아니라, 개인정보보호·데이터안전·인류유전자원관리 등 위계와 주관부처가 서로 다른 여러 규범에 흩어져 있어 규범을 가로질러 재구성하여야 하는 분석적 개념이다. 이에 본 절에서는 먼저 일반적 의미에서 의료데이터의 내포와 다중적 법적 속성을 확정하고, 이를 토대로 본 사건(공시번호 20220001)이 관련된 데이터를 구체적으로 자리매김한다. 이 확정은 이후 규범적용의 논리적 출발점이자, ‘조합적용’과 ‘높은 기준에 따른 엄격 적용(就高从严)’이 성립하기 위한 전제이기도 하다.

가. 광의의 개념

중국의 현행 법률·행정법규·부문규장·국가표준은 모두 ‘의료데이터’를

명칭으로 하는 통일된 정의 조항을 두고 있지 않으며, 관련 개념은 서로 다른 규범에 흩어져 있고 각각의 규범목적과 보호강도도 일치하지 않는다. 각 규범 층위를 종합하면, 의료데이터는 중국법상 적어도 다음의 속성을 동시에 가질 수 있다. 즉 민감개인정보로서의 속성(「개인정보보호법」(이하 ‘PIPL’) 제 28 조는 ‘의료건강’을 민감개인정보로 열거한다)⁷, 건강의료데이터로서의 속성(GB/T 39725-2020 「정보안전기술 건강의료데이터 안전지침」은 특정 자연인을 식별하거나 그 생리적·심리적 건강상태를 반영할 수 있는 전자데이터와 그 파생데이터로 정의한다)⁸, 국가의 중요한 기초적 전략자원으로 자리매김되는 건강의료빅데이터로서의 속성(「국가 건강의료빅데이터 표준·안전·서비스 관리방법(시행)」)⁹, 인류유전자원정보로서의 속성(「인류유전자원관리조례」. 2023 년 「실시세칙」은 이를 유전자·게놈 데이터로 한정하고 임상·영상·단백질·대사 데이터를 제외하였다)¹⁰, 그리고 분류등급 체계하에서 중요데이터 또는 국가핵심데이터로 식별될 수 있는 속성(「데이터안전법」(이하 ‘DSL’) 제 21 조, 「네트워크데이터 안전관리조례」 제 62 조, GB/T 43697-2024 부록

⁷「중화인민공화국 개인정보보호법」 제 28 조 제 1 항은 ‘의료건강’을 생체인식, 종교신앙, 특정신분, 금융계좌, 행적정보 등과 나란히 민감개인정보로 열거한다. 민감개인정보의 판단기준에 관하여는 王利明:《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》, 载《当代法学》2022 年第 1 期 참조.

⁸「정보안전기술 건강의료데이터 안전지침」(GB/T 39725-2020) 제 3 장 ‘용어와 정의’는 ‘개인 건강의료데이터’를 단독으로 또는 다른 정보와 결합하여 특정 자연인을 식별할 수 있거나 특정 자연인의 생리적·심리적 건강을 반영하는 전자데이터로, ‘건강의료데이터’를 개인 건강의료데이터 및 이를 가공·처리하여 얻은 건강의료 관련 전자데이터를 포함하는 것으로 정의한다.

⁹《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》(国办发[2016]47 号)은 서두에서 “건강의료빅데이터는 국가의 중요한 기초적 전략자원”임을 명확히 하였고, 《国家健康医疗大数据标准、安全和服务管理办法(试行)》(国卫规划发[2018]23 号) 제 1 조는 이 자리매김을 이어받아 “건강의료빅데이터의 국가 중요 기초 전략자원으로서의 역할을 충분히 발휘”하는 것을 입법목적으로 한다.

¹⁰「인류유전자원관리조례」(국무원령 제 717 호, 2019 년 7 월 1 일 시행) 제 2 조; 「인류유전자원관리조례 실시세칙」(2023 년 7 월 1 일 시행) 제 2 조 제 3 항은 임상데이터, 영상데이터, 단백질데이터와 대사데이터를 인류유전자원정보에서 명문으로 제외한다.

G「중요데이터 식별지침」)이 그것이다¹¹. 각 층위 속성의 구체적 규범요건은 후술하는 관련 장에서 상세히 다룬다.

이에 따라 본 연구에서 말하는 ‘의료데이터’란, 의료·보건 및 건강 관련 활동에서 생성되어 단독으로 또는 다른 정보와 결합하여 특정 자연인을 식별하거나 그 생리적·심리적 건강상태를 반영할 수 있는 전자데이터와 그 파생데이터를 가리킨다.¹² 다만 강조할 점은, 이것이 단일 속성의 객체가 아니라 민감개인정보, 건강의료(빅)데이터, 인류유전자원정보, 그리고 중요데이터 또는 국가핵심데이터 등 다중적 속성을 동시에 가질 수 있는 복합적 객체라는 것이다. 동일한 데이터가 서로 겹치는 여러 규범적 평가 아래 동시에 놓이는 경우가 흔하다.

나. 본 사건이 관련된 구체적 자리매김

위 속성을 본 사건에 포섭하면 다음과 같다. 베이징우의병원과 암스테르담대학교 의학센터(Amsterdam UMC)가 공동으로 수행한 COLOR III·COLOR IV 국제 다기관 임상연구(COLOR III 는 베이징우의병원 단일기관 기준으로 본 사건 공시 시점까지 약 170 레 등록, COLOR IV 는 전 세계적으로 1,158 레 등록 계획)는 결장·직장암 환자의 진료 및 추적관찰 정보를 핵심으로 하여 특정 자연인을 식별하고 그 건강상태를 반영할 수 있으므로, 민감개인정보와 건강의료데이터에 해당함이 확실하며, 이것이 본 사건 데이터의 가장 확실한 속성 층위이다. 인류유전자원에 관하여 보면, 두 협약의

¹¹ 「중화인민공화국 데이터안전법」 제 21 조는 데이터 분류등급 보호제도를 확립하고 국가핵심데이터를 확정하며, 「네트워크데이터 안전관리조례」(2025 년 1 월 1 일 시행) 제 62 조는 ‘중요데이터’의 정의를 규정하고, 「데이터안전기술 데이터 분류등급 규칙」(GB/T 43697-2024) 부록 G ‘중요데이터 식별지침’은 동 표준의 규범성 부록으로서 중요데이터 식별의 방법론을 제공한다.

¹²이 획정은 GB/T 39725-2020 제 3 장의 ‘개인 건강의료데이터’와 ‘건강의료데이터’ 정의를 기초로 「개인정보보호법」 제 28 조 제 1 항의 민감개인정보 요소를 결합하여 구성한 것으로서, 분석의 편의를 위하여 본 연구가 채택한 작업적 정의이며 현행법상의 통일된 법정 개념이 아니다.

공개내용에 따를 때 본 사건의 연구데이터는 주로 임상 표현형, 영상의학적 평가, 수술 과정, 병리 평가, 수술 후 회복 및 추적관찰 데이터로서 유전자 시퀀싱이나 게놈 데이터의 수집을 명시적으로 포함하지 않는다. 「인류유전자원관리조례 실시세칙」(2023 년 7 월 1 일 시행)이 임상·영상·단백질·대사 데이터를 인류유전자원정보에서 제외한 점과 결합하면, 본 사건은 인류유전자원정보를 구성하지 않을 개연성이 크고 그에 따른 절차도 직접 발동되지 않는다(이는 2023 년 세칙을 사후적 참조로 삼은 추론이며, 심사 시점의 규범상태는 제 4 장에서 상술한다). 다만 연구에서 생물학적 시료(병리 표본 포함)의 국외제공이 있었는지는 추가 확인이 필요하다. 중요데이터 해당 여부는 단계를 나누어 관찰하여야 한다. 본 사건 심사 시점에는 중요데이터 목록과 의약산업 네거티브리스트가 모두 제정되기 전이었고, 본 사건이 중요데이터로 신고되었다는 기록도 공개자료에 없다. 컴플라이언스 지속 단계에서는 GB/T 43697-2024 부록 G 의 식별방법에 따르면 본 사건의 집적된 집단 진료데이터가 중요데이터로 식별될 여지가 있으나, 주관부처의 고지 또는 공개발표로 중요데이터로 지정되지 않은 한 「네트워크데이터 안전관리조례」상 중요데이터로 신고할 필요는 아직 없다. 시간축의 관점에서는, 본 사건의 COLOR III 참여가 2018 년 7 월, 데이터 국외이전 신고 개시가 2022 년 9 월, COLOR IV 는 2030 년까지 지속되므로, 각 단계에 적용되는 규범이 일치하지 않아 ‘언제 어떤 법이 적용되는가’에 따라 개별적으로 판단하여야 한다.

종합하면 본 사건 데이터는 다음과 같이 확정할 수 있다. 즉 결장·직장암 환자의 진료 및 추적관찰 정보를 핵심으로 하여 민감개인정보와 건강의료데이터에 해당함이 확실하고, 인류유전자원정보를 구성하지 않을 개연성이 크며, 주관부처의 고지 또는 공개발표로 중요데이터로 지정되지 않은 한 아직 중요데이터로 신고할 필요가 없는 복합적 데이터 집합이다. 그 속성은 사실관계와 시점에 따라 층층이 변동하며, 바로 이 점이 본 사건을

‘의료데이터의 다중적 속성이 구체적 국외이전 시나리오에서 어떻게 조합적용되는가’를 관찰하는 전형적 표본으로 만든다. 위 각 층위의 속성은 이후의 각 장과 하나하나 대응한다. 민감개인정보·건강의료데이터로서의 성질 결정은 제 4 장의 분류등급 식별 및 제 3 장의 국외이전 경로 선택에 대응하고, 중요데이터로서의 가능성은 제 4 장 컴플라이언스 지속 단계의 재판단에 대응하며, 인류유전자원정보의 배제는 제 7 장 규제관할 경계의 획정에 대응한다. 개념 획정은 이로써 이후 규범분석의 색인이 된다. 이른바 ‘조합적용’이란 동일한 데이터 집합이 다중적 속성에 동시에 포섭됨으로써 각 속성 아래의 규범의무를 중첩적으로 부담하고, 그 의무의 강도는 ‘높은 기준에 따른 엄격 적용’으로 확정되는 것을 말한다. 본 사건이 드러내는 난제는 주로 규범 간의 직접적 충돌이 아니라 규범 사이의 연계 공백이므로, 충돌규칙(상위법 우선, 특별법 우선)을 동원할 필요는 아직 없다. 이 판단은 제 6 장의 매트릭스에서 구체적으로 제시될 것이다.

4. 논문의 구성

본 연구를 일관하는 물음은 다음과 같다. 전국 최초로 데이터 국외이전 안전평가를 통과한 사건으로서, 본 사건은 장기 국제 임상연구라는 상황에서 중국 의료데이터 국외이전 규제의 실제 운용구조를 어떻게 보여주며, 그 안에 응답을 요하는 어떤 규범적 문제가 존재하는가. 이에 대한 본 연구의 핵심 논지는 다음과 같다. 본 사건은 ‘규범 구축이 앞서고 사실인정 규칙이 뒤처지는’ 구조적 긴장을 드러낸다. 즉 분류등급과 중요데이터 식별규칙이 아직 완비되지 않은 시기에 처리자의 내부 거버넌스가 사실상 규범 공백기의 식별 기능을 담당하였고(제 4 장에서 정리하는 ‘규범 미완성 — 사실 선행’이 그것이다), 동시에 2~3 년을 기한으로 하는 평가 유효기간과 10 년 단위로 헤아리는 국제 임상연구 주기 사이에 제도적 어긋남이 존재하여, ‘평가 통과’와 ‘지속적 컴플라이언스’가 각각 별도로 고찰하여야 할 두 개의 문제로 분리된다. 이후의

모든 사실 정리와 규범 분석은 이 논지의 검증과 전개에 봉사한다. 이 물음을 중심으로, 위의 연구대상·범위·개념 확정에 기초하여 본 연구는 ‘사실을 먼저, 규범을 나중에’의 순서로 전개하며, 본 사건의 핵심 절차인 데이터 국외이전 안전평가를 조직의 축으로 삼는다. 「데이터 국외이전 안전평가 방법」 제 5 조와 제 8 조에 열거된 평가사항이 바로 본 연구 각 장의 분석 차원을 구성한다. 제 2 장은 본 사건의 사실관계를 온전히 제시하여 모든 규범분석에 사실기반을 제공한다. 제 3 장은 위계에 따라 본 사건에 적용되는 법원(法源) 체계를 정리하며, 이는 국외이전의 적법성·정당성·필요성이라는 심사 차원에 대응한다. 제 4 장은 데이터 분류등급 보호제도를 본 사건에 적용하고 GB/T 43697-2024 를 진화 이후의 규범 참조계로 도입하며, 이는 국외이전 데이터의 종류·규모·민감정도라는 심사 차원에 대응한다. 제 5 장은 네트워크안전등급보호제도가 본 사건에 제공하는 국내 시스템 보장을 제시하며, 이는 데이터 처리자의 안전보장 능력이라는 심사 차원에 대응한다. 제 6 장은 ‘8 개 단계 적용규범 매트릭스’로 각 규범을 본 사건 데이터의 전생애주기에 집성하여 투영하며, 이는 국외이전 중·국외이전 후 위험이라는 심사 차원에 대응한다. 제 7 장은 중국과 EU 두 규제체계의 관할과 법적 책임으로 확장하며, 이는 국외 수령자 소재 법역의 법률환경이라는 심사 차원에 대응한다. 제 8 장은 본 사건의 표본가치와 핵심 발견을 정리한다. 바꾸어 말하면 각 장은 병렬적인 제도 나열이 아니라, 동일한 데이터 국외이전 안전평가의 법정 심사 차원을 항목별로 해부한 것이다. 덧붙여 ‘사실을 먼저, 규범을 나중에’는 사실 인정과 규범 평가의 선후 순서에 관한 것임을 밝혀 둔다. 공개자료가 밝히지 않은 사항은 모두 추론으로 표기하였으며, 평가의 법정 심사 차원으로 장을 조직한 것은 서술 틀의 선택일 뿐 각 차원 아래의 규범적 결론을 예단하지 않는다.

II. 사건의 사실관계

‘사실을 먼저, 규범을 나중에’의 분석순서에 따라, 본 장에서는 먼저 본

마붕초- 중국 의료데이터 국외이전 규제에 관한 연구
사건의 객관적 사실 — 사건 식별, 당사자, 협력 프로젝트, 핵심 시간선, 관련
데이터, 데이터 흐름과 신고 절차 — 을 온전히 제시하여 이후 각 장의
규범분석에 사실기반을 제공한다.

1. 사건 식별과 신고 경로

가. 사건번호와 공시

본 사건의 공식 공시번호는 20220001 로, 베이징시 인터넷정보판공실(이하 ‘베이징시 인터넷정보판공실’)이 부여하였다. 본 사건은 「데이터 국외이전 안전평가 방법」(2022 년 9 월 1 일 시행) 시행 이래 전국 최초로 데이터 국외이전 안전평가를 통과한 사례이다. 공시 시점은 2023 년 1 월 말부터 2 월 초이다.

나. 신고 경로

본 사건에 적용된 국외이전 경로는 「개인정보보호법」 제 38 조 제 1 호와 제 40 조가 규정한 국외이전 안전평가 경로이며, 그 근거는 「데이터 국외이전 안전평가 방법」이다. 수리기관은 베이징시 인터넷정보판공실(지방 인터넷정보 부서), 평가기관은 국가인터넷정보판공실(CAC)이다. 베이징시 인터넷정보판공실은 본 프로젝트를 ‘베이징시 선행시범(先行先试) 프로젝트’로 지정하였다.

다. 심사 통과 시점

심사 통과와 구체적 일자 는 공개 경로에서 직접 밝혀지지 않았다. 《재경(财经)》의 2023 년 2 월 보도는 “2022 년 9 월 베이징시 인터넷정보판공실이

..... 심사를 완료하였다”고 언급하나¹³, 이 표현은 ‘2022 년 9 월 1 일 「데이터 국외이전 안전평가 방법」 정식 시행’ 시점과 지나치게 근접하여 기술상의 오차 가능성이 있다.

2. 당사자

가. 중국 측 주체(데이터 처리자)

기관명칭	수도의과대학 부속 베이징우의병원
기관성격	사업단위(事业单位) ¹⁴
기관등급	3 급 갑등(三级甲等) 종합병원 ¹⁵
소속 분야	의료·보건 분야
주관부처	베이징시 보건위생위원회
업종 주관기관	국가보건위생위원회, 베이징시 보건위생위원회

본 연구에 대한 의의: 병원이 사업단위라는 법적 지위는 PIPL 상 ‘개인정보 처리자’의 식별에 영향을 미치고, ‘기업’을 적용주체로 하는 자유무역시험구 네거티브리스트의 범위에 포섭되는지와도 관련된다(제 3 장에서 상술). 또한 3 급

¹³《财经》:《数据合规出境倒计时:企业如何确定优先事项》, 2023 年 3 月 22 日。 https://www.mycaijin.com/article/detail/486209?source_id=40。

¹⁴ 中央编办关于批转《事业单位登记管理暂行条例实施细则》《事业单位法人年度报告公示办法(试行)》的通知 참조: “사업단위란 국가가 사회공익의 목적을 위하여 국가기관이 설립하거나 그 밖의 조직이 국유자산을 이용하여 설립한, 교육, 과학연구, 문화, 위생, 체육, 신문출판, 라디오·텔레비전, 사회복지, 구조·재해경감, 통계조사, 기술보급·실험, 공용시설관리, 물자비축, 관측, 탐사·측량, 측회(测绘), 검사·검측·감정, 법률서비스, 자원관리 사무, 품질기술 감독 사무, 경제 감독 사무, 지식재산권 사무, 공증·인증, 정보·컨설팅, 인재교류, 취업서비스, 기관 후생서비스 등 활동에 종사하는 사회서비스 조직을 말한다.”

¹⁵ 3 급 갑등(三级甲等) 병원은 약칭 ‘삼갑병원’으로, 중국이 「병원 등급관리방법」에 따라 시행하는 ‘3 급 6 등(三级六等)’ 등급구분 중 최고 등급의 병원이다.

갑등 종합병원이라는 규모는 실제 진료량이 「데이터 국외이전 안전평가 방법」 제 4 조 제 2 호의 ‘100 만 명 이상 개인정보’ 기준을 크게 초과할 수 있음을 의미한다.

나. 국외 수령자

기관명칭	네덜란드 암스테르담대학교 의학센터(Amsterdam University Medical Center)
기관 소재지	네덜란드 암스테르담
적용되는 국외 개인정보보호제도 ¹⁶ 이행입법	EU 「일반개인정보보호규정」(GDPR) 및 네덜란드 국내

본 연구에 대한 의의: 「데이터 국외이전 안전평가 방법」 제 8 조 제 2 호에 따라 CAC 는 평가 시 “국외 수령자가 소재한 국가 또는 지역의 데이터안전 보호 정책·법규 및 네트워크안전 환경”을 고려하여야 한다. 네덜란드에 GDPR 이 적용된다는 사실은 본 사건 안전평가의 통과 과정에서 이미 평가 고려요소에 반영되었을 것이나, 구체적인 평가 고려내용은 공개자료에 밝혀져 있지 않다.

¹⁶GDPR 적정성 결정 문제에 관한 설명: 지적하여 둘 것은, GDPR 제 45 조가 규정하는 ‘적정성 결정’(adequacy decision)은 EU 에서 제 3 국으로의 데이터 이전에 적용되며, 본 연구 작성 시점까지 EU 집행위원회는 중국에 대하여 적정성 결정을 내린 바 없다는 점이다. 본 사건의 기본 흐름은 ‘중국에서 EU 로’이므로 적정성 결정의 부재가 본 사건 데이터의 네덜란드 유입의 적법성에 직접 영향을 미치지 않는으나, EU 측에서 중국으로의 회송 또는 재이전이 발생하는 경우에는 표준계약조항(SCC) 등 GDPR 제 46 조 소정의 적절한 보호조치로 연계하여야 한다. 장래 본 사건 COLOR III/IV 의 후속 연구에서 네덜란드 측 데이터가 중국 측으로 역방향 전송되는 경우(다기관 합동분석 결과의 회송, 유럽 코호트 환자데이터의 회송 등)에는 EU 에서 중국으로의 데이터 이전이 성립하여, GDPR 제 5 장의 국경 간 이전 규칙에 따라 표준계약조항(SCC) 등 적절한 보호조치를 갖추어야 한다.

3. 관련 공동연구 프로젝트

본 사건은 두 개의 국제 다기관 임상연구를 합하여 다루며, 두 연구 모두 주체는 베이징우의병원과 Amsterdam UMC로서 동일 사건의 두 연구 하위항목을 구성한다.

가. COLOR III 연구

의뢰자	Amsterdam UMC(즉 국외 수령자)
베이징우의병원의 역할	참여기관(연구센터)
참여 시점	2018 년 7 월
본 사건 공시 시점까지의170 레(베이징우의병원은 전 세계 최다 등록 연구센터)	등록 수

나. COLOR IV 연구

의뢰자	베이징우의병원(즉 국내 측, COLOR III 와 반대)
공동 발기기관	Amsterdam UMC(즉 국외 수령자)
재원(중국 측)	국가중점연구개발계획 2017YFC0110904(2017 년 선정), 수도의과대학 결장직장암 임상센터 프로젝트 1192070313, 베이징시 병원관리국 임상의학발전 전문사업 ZLRK202302 등
준비 개시	2018 년부터
등록 예정	1,158 레(약 1,200 레, 3~5 년 내)
지속 기간	2030 년까지
참여기관(연구센터)	30~50 개소 예정

다. 두 연구의 본 사건에서의 병합 처리

두 연구의 국내 측은 모두 베이징우의병원, 해외 측은 모두 Amsterdam UMC 이며, 모두 중국 측 환자데이터의 네덜란드 측 전송을 수반한다. 본 연구는 주체와 데이터 흐름의 동일성에 근거하여 COLOR III 를 핵심 사실기반으로, COLOR IV 를 컴플라이언스 지속 시나리오로 함께 분석에 포함한다.

COLOR IV 의 중국 측 재원은 2017 년에 과제로 선정되었는데, 이때는 PIPL 과 「데이터안전법」이 아직 제정되지 않았고 「데이터 국외이전 안전평가 방법」도 공포되기 전이었다. 이 시점은 ‘각 시기별 적용법규’ 분석에 핵심적 의의를 가진다. 베이징우의병원의 COLOR III 참여는 2018 년 7 월로, 역시 PIPL 과 「데이터안전법」 제정 이전이다. 데이터 국외이전 신고는 2022 년 9 월에 개시되었는데, 「데이터 국외이전 안전평가 방법」이 막 시행된 직후였다. 이는 본 사건의 컴플라이언스 과정이 중국 데이터 국외이전 규제체계가 무에서 유로 구축되어 온 전 과정을 가로질렀음을 의미한다.

4. 사건의 핵심 시간선

아래 표는 본 사건의 핵심 분기점을 시간순으로 정리한 것이다.

시점	사건 경과 및 규범 시행
2017 년	COLOR IV 중국 측 재원 선정(국가중점연구개발계획 2017YFC0110904)
2017.6.1.	「네트워크안전법」 시행(네트워크안전등급보호제도, 제 37 조 CIIO 현지화 포함)
2018.7.	베이징우의병원, COLOR III 연구 참여
2018.9.13.	국가보건위생위, 「국가 건강의료빅데이터 표준·안전·서비스 관리방법(시행)」 발표
2019.7.1.	「인류유전자원관리조례」 시행(국무원령 제 717 호)
GB/T 22239-2019	GB/T 22239-2019 ¹⁷ 네트워크안전등급보호제도 2.0 시행(등급보호 1.0 대체)
2020 년	GB/T 35273-2020 시행(10.1.) ¹⁸ ; GB/T 39725-2020 ¹⁹ , GB/T 39335-2020 ²⁰ 발표(12.14., 11.19.)
2021.6.1./7.1.	GB/T 39335-2020, GB/T 39725-2020 순차 시행
2021.4.15.	「생물안전법」 시행
2021.9.1.	「데이터안전법」 시행; 「핵심정보인프라 안전보호조례」 시행
2021.11.1.	「개인정보보호법」 시행
2022.4.	베이징우의병원, COLOR III 전 세계 최초 100 레 등록 연구센터 달성
2022.7.22.	COLOR IV, ClinicalTrials.gov 등록
2022.8.29.	「의료보건기관 네트워크안전 관리방법」 인쇄·시행 「데이터 국외이전 안전평가 방법」 정식 시행; 베이징시
2022.9.1.	인터넷정보판공실, 전국 최초의 지방 신고수리 전용창구 개통; 베이징우의병원 신고 개시

¹⁷《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019) , 国家市场监督管理总局、国家

标准化管理委员会，2019年5月10日发布，2019年12月1日实施。

¹⁸《信息安全技术 个人信息安全规范》（GB/T 35273-2020），国家市场监督管理总局、国家标准化管理委员会，2020年3月6日发布，2020年10月1日实施。

¹⁹《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020），国家市场监督管理总局、国家标准化管理委员会，2020年12月14日发布，2021年7月1日实施。

²⁰《信息安全技术 个人信息安全影响评估指南》（GB/T 39335-2020），国家市场监督管理总局、国家标准化管理委员会，2020年11月19日发布，2021年6月1日实施。

시점	사건 경과 및 규범 시행
2022.9.	《재경》 보도에 따르면 베이징 인터넷정보판공실 심사 완료(구체적 일자 미공개)
2023.1.말~2.초	베이징시 인터넷정보판공실, 본 사건을 공시번호 20220001 전국 최초 통과 사례로 공시; 국가보건위생위 홈페이지 전재
2023.2.18.	「인간 대상 생명과학 및 의학연구 윤리심사 방법」(国卫科教发[2023]4 号) 발표
2023.6.1.	「개인정보 국외이전 표준계약 방법」 시행(본 사건 심사 후)
2023.7.1.	「인류유전자원관리조례 실시세칙」 시행(본 사건 심사 후)
2024.3.22.	「데이터 국경 간 이동 촉진 및 규범화 규정」 발표·시행(본 사건 심사 후)
2024.8.30.	베이징 자유무역시험구 데이터 국외이전 관리 네거티브리스트(2024 년판) 발표, 의약산업 포함(본 사건 심사 후)
2024.9.(추론)	본 사건 평가 유효기간 만료(「데이터 국외이전 안전평가 방법」 제 14 조의 원래 2 년 규칙에 따르면 이 시점에 만료; 2024 년 「데이터 국경 간 이동 촉진 및 규범화 규정」 제 9 조의 3 년 신규칙에 따르면 2025 년 9 월 만료로 연장)
2024 年 10 月 1 日	GB/T 43697-2024 「데이터안전기술 데이터 분류등급 규칙」 시행 ²¹ (본 사건 심사 후)
2025.1.1.	「네트워크데이터 안전관리조례」 시행(본 사건 심사 후)
2025.2.	COLOR IV 협약, Surgical Endoscopy 지에 정식 게재
2025.5.30.	GB/T 22239-2019 재심사 결과 계속 유효 확인(본 사건 컴플라이언스 지속 단계의 등급보호 기술근거 불변) ²²
2026.3.	COLOR III 단기 결과 공개 보도(1,103 례 무작위 등록)

시점

사건 경과 및 규범 시행

베이징 ‘양구(两区)’ 데이터 국외이전 네거티브리스트(2025 년판)
2026.5.11. 및 관리방법 발표, 적용범위가 베이징시 전역으로 확대되고
9 개 산업분야 포함(본 사건 심사 후)

본 사건의 시간적 범위는 2017 년부터 2030 년(COLOR IV 완료 예정)까지 이어지며, 그 사이 중국 데이터 국외이전 규제체계는 근본적인 구축을 겪었다. 본 사건의 심사는 2022 년 9 월부터 2023 년 초에 완료되었는데, 이는 PIPL 시행 후 1 년 미만, 「데이터안전법」 시행 후 약 1 년, 「데이터 국외이전 안전평가 방법」 시행 후 0~4 개월에 불과한 시점으로, 본 사건은 규제체계가 막 수립된 초창기에 심사가 완료된 것이다.

5. 관련 데이터

가. 데이터의 유형과 범위

COLOR III·COLOR IV 협약의 공개내용에 따르면, 본 사건이 관련된 데이터 차원에는 개인식별정보, 병력정보, 임상진단정보, 영상의학 데이터, 수술 및 수술 전후 데이터, 병리 평가 데이터, 수술 후 추적관찰 데이터가 포함된다. 다만 위는 병원이 연구 과정에서 관여·처리하는 데이터 차원을 가리키며, 그중 성명·입원번호 등 직접 식별 필드는 임상연구 실무상 통상 연구번호 등의 방식으로 코드화 처리되므로, 그것이 직접 식별 가능한 형태로 실제 국외이전되었는지는 공개자료에 밝혀져 있지 않다.

데이터 범주

구체적 내용(예시)

개인식별정보

환자 성명, 생년월일, 성별, 입원번호, 연구번호

²¹《数据安全技术 数据分类分级规则》，国家市场监督管理总局、中国国家标准化管理委员会，2024 年 3 月 15 日发布，2024 年 10 月 1 日实施。

²²《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019），国家市场监督管理总局、中国国家标准化管理委员会，2025 年 5 月 30 日复审确认继续有效。

데이터 범주	구체적 내용(예시)
병력정보	기왕력, 가족력, 알레르기력, 투약력
임상진단정보	병리 생검 결과, 종양 위치와 병기, TNM 병기, 수술 전 평가
영상의학 데이터	MRI, CT(COLOR III 협약은 중양화 MRI 재판독을 명문으로 요구)
수술 및 수술 전후 데이터	수술방식, 수술 중 데이터, 합병증, 수술 후 재원기간
병리 평가 데이터	중양화 병리 재판독
수술 후 추적관찰 데이터	1 차 평가변수, 2 차 평가변수, 3~5 년 추적관찰(EQ-5D-5L, EORTC-QLQ-C30, EORTC-QLQ-CR29 등 3 종의 삶의 질 척도 포함)

또한 COLOR IV 협약의 명문 규정에 따르면, 본 사건에서 국외이전되는 데이터에는 수술 동영상(unedited operative videos, CAT 점수에 의한 학습곡선 평가용), 중대한 이상반응 보고(SAE report form, 사건 인지 후 2 주 내에 조정센터로 전자 제출), 그리고 재발 보고(recurrence report form, 역시 2 주 내 제출)도 포함된다.

나. 데이터 민감도 분류

본 사건 데이터를 여러 규범의 관점에서 민감도 분류·식별한 결과를 아래 표로 정리한다.

규범의 관점	식별 결과
PIPL 제 28 조	민감개인정보(‘의료건강’류) — 진료기록, 검사, 영상, 수술, 추적관찰 등 전부 이에 해당
GB/T 39725-2020	건강의료데이터 4 등급 민감도(비교적 높음)

규범의 관점	식별 결과
「데이터안전법」 제 21 조 / GB/T 43697- 2024	‘중요데이터’ 해당 여부는 본 사건 심사 시점에 규범상 불명확; 2024 년 베이징 자유무역시험구 네거티브리스트는 ‘일정 규모 이상의 집단 진료’를 중요데이터로 열거
「인류유전자원관리조례」 제 2 조	인류유전자원정보를 구성하지 않을 개연성이 큼 — 협약 공개내용에 유전자 데이터 수집 언급 없음; 실시세칙(2023.7.1. 시행) 제 2 조 제 3 항은 ‘임상데이터, 영상데이터, 단백질데이터, 대사데이터’를 명문으로 제외

다. 데이터 규모

공개된 프로젝트 규모를 보면, COLOR III 연구에서 베이징우의병원 단일기관은 본 사건 공시 시점까지 약 170 레를 등록하였고(해당 연구의 전 세계 최다 등록 연구센터), 동 연구는 최종적으로 전 세계 28 개 센터에서 총 1,103 레를 무작위 등록하였다. COLOR IV 연구계획서는 전 세계 30~50 개 참여센터에서 합계 1,158 레(약 1,200 레)를 등록할 계획이다. 베이징우의병원 단일기관이 실제로 생성·국외이전한 데이터의 규모는 공개자료에 정확히 밝혀져 있지 않다.

국외이전 수량 자체로 판단하면, 두 연구의 전 세계 규모 합계(1,103 레와 1,158 레, 합계 약 2,300 레)를 본 사건 국외이전량의 상한으로 보더라도 「데이터 국외이전 안전평가 방법」 제 4 조 제 3 호가 규정하는 ‘1 만 명 민감개인정보’ 기준에 크게 미치지 못하며, 베이징우의병원 단일기관의 실제 국외이전량은 그보다 더 적을 수밖에 없으므로 위 상한 관찰은 보수적 추정에 해당한다. 공개된 데이터 규모로부터 추론하면, 본 사건이 안전평가를 촉발한 근거는

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

제 2 호일 가능성이 더 크다. 규범 자체의 논리에 따르면 “100 만 명 이상의 개인정보를 처리하는 데이터 처리자가 국외로 개인정보를 제공하는 경우, 단 한 건의 개인정보만 국외이전하더라도 데이터 국외이전 안전평가를 신고하여야 한다.” 즉 제 2 호는 처리자 주체 자체의 처리규모를 기준으로 하며 구체적인 국외이전 수량과는 무관하다. 베이징우의병원은 대형 3 급 갑등 종합병원으로서 장기간 다량의 환자 개인정보, 의료건강정보와 민감개인정보를 처리하여 왔으므로 ‘100 만 명 이상의 개인정보를 처리하는 데이터 처리자’로 평가될 가능성이 있다. 다만 병원이 동시에 CHIO 에 해당하는지, 어떤 방식으로 제 2 호 해당이 인정되었는지의 구체적 사실은 공개자료에 밝혀져 있지 않다.

6. 데이터 흐름

COLOR III: 베이징우의병원(국내 측) → Amsterdam UMC(국외 수령자)

COLOR IV: 베이징우의병원(국내 측/의뢰자) → Amsterdam UMC(국외 수령자; 그 밖에 전 세계 30~50 개 참여기관이 있으며, 이들이 중국 측 피험자의 개인 수준 데이터에 접근할 수 있는지는 공개자료에 밝혀져 있지 않음)

COLOR III 와 COLOR IV 는 주체의 위상이 서로 바뀌어 있다. COLOR III 는 ‘국외 측 주도·중국 측 참여’, COLOR IV 는 ‘중국 측 주도·국외 측 공동발기’이다. 그러나 두 연구 모두 중국 측 환자데이터의 네덜란드 측 전송을 수반하므로 모두 중국 데이터 국외이전 규제의 범위에 포섭된다. 따라서 국경 간 시나리오의 컴플라이언스 판단은 누가 의뢰자인지가 아니라 데이터의 물리적 흐름을 기준으로 한다.

COLOR IV 협약의 명문 규정에 따르면, 본 사건 데이터는 “COLOR IV secure digital case record form”이라는 중앙화 디지털 증례기록 시스템을 통하여 전송된다. CT 영상, 병리 보고 등 임상데이터는 이 시스템에서 집중적으로 평가되고, 수술 후 1 년과 2 년의 복부·골반 CT 영상은 “중앙화 재판독에

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구 업로드”되어야 하며, 중대한 이상반응과 재발 보고는 사건 인지 후 2 주 내에 조정센터로 전자 제출되어야 한다. 다만 이 시스템의 구체적 기술 형태(암호화 방식, 데이터센터의 물리적 위치, 접근통제, 전송 프로토콜 등), 수령자의 국외 저장 위치와 2 차 이전에 관하여는 공개자료에 밝혀져 있지 않다.

7. 신고 및 심사 절차

베이징시 보건위생위 공식 보도자료 원문에 따르면, 본 사건의 내부 심사 절차는 다음 네 단계로 구성된다.²³

제 1 단계는 병원 과학기술처의 내부 평가이다. 병원 과학기술처는 이 임상연구 프로젝트의 그간의 수행 상황, 과학적 의의와 산출 가치, 인류유전자원 등 측면의 상황을 심층 평가하고, 데이터 국외이전과 프로젝트 수행·산출 사이의 관계를 분석하여 데이터 국외이전의 필요성과 과학적 의의를 확인하였다. 이 단계는 사실상 「데이터 국외이전 안전평가 방법」 제 8 조 제 1 호의 ‘데이터 국외이전의 목적·범위·방식 등의 적법성·정당성·필요성’에 대한 사전 내부 논증을 완성하는 동시에, 프로젝트의 인류유전자원 관련 여부에 대한 분류 식별도 완료하였다.

제 2 단계는 병원 정보센터의 네트워크안전 평가이다. 병원 정보센터는 본 사건의 데이터 국외이전 신고에 앞서 병원의 네트워크안전·데이터안전을 다시 평가하여, 병원의 네트워크안전 제도가 완비되고 실효성 있게 이행되고 있으며 안전방어 기술능력이 등급보호 등 표준규범에 부합함을 확인하였다. 이 단계는 본 사건 데이터 국외이전 신고에서 국내 측의 안전보호 능력에 관한 컴플라이언스의 사전 기초를 제공한 것으로, 「데이터 국외이전 안전평가 방법」 제 8 조 제 5 호의 ‘본 방법이 규정한 절차 이행의 적법성, 중국의

²³北京市卫生健康委员会:《全国首个获批数据出境安全评估案例落地北京友谊医院》, 2023 年 2 月 2 日, https://wjw.beijing.gov.cn/xwzx_20031/jcdt/202302/t20230202_2910980.html 참조.

법률·행정법규·부문규장 규정예의 부합 여부’ 요건에 대응한다.

제 3 단계는 병원 내부 제도의 구축이다. 베이징우의병원은 병원 내부의 「데이터 국외이전 안전관리방법」을 제정하였는데, 공식 보도자료 원문의 표현에 따르면 동 방법의 내용은 “중요데이터 국외이전의 심사 메커니즘, 평가 메커니즘, 감독 메커니즘의 수립”을 포함하며, 사전 심사·안전평가·지속적 감독을 결합하는 원칙을 따른다. 이 단계는 데이터 처리자로서의 병원의 내부 컴플라이언스 제도 구축을 완성하였다.

제 4 단계는 베이징시 인터넷정보판공실에 대한 신고와 국가인터넷정보판공실의 평가 통과이다. 베이징우의병원은 최초 신고기관 중 하나로서 베이징시 인터넷정보판공실을 통하여 국가인터넷정보판공실에 데이터 국외이전 안전평가를 신고하였다. 본 프로젝트는 베이징시 인터넷정보판공실에 의하여 ‘베이징시 선행시범 프로젝트’로 지정되었고, 최종적으로 평가를 통과하여 공시번호 20220001 사건이 되었다.

위 네 단계 외에, 국가보건위생위원회가 업종 주관부처로서 본 사건 심사·평가에 병행 참여하였다. 공식 보도에 따르면 국가보건위생위는 본 사건 심사·평가에서 “관련 지도와 위탁 조사연구 업무를 수행”하였다. 베이징우의병원은 국가보건위생위의 위탁을 받아, 향후 의료데이터의 국경 간 수집·이용에 관한 안전관리방법의 기초(起草)를 위한 조사연구를 수행하기로 하였다.

8. 피험자 동의 문제

COLOR III 협약 원문에 따르면,²⁴ 동의서의 구체적 요건은 각 참여센터의

²⁴원

문: “Informed consent will be obtained from all eligible patients in accordance with the requirements of the local ethical committees.” Deijen CL, Velthuis S, Tsai A, et al. COLOR III: a multicentre randomised clinical trial comparing transanal TME versus laparoscopic TME for mid and low rectal cancer. Surg Endosc. 2016 Aug;30(8):3210-5 참조.

현지 윤리위원회가 정하도록 명시되어 있다. 베이징우의병원의 경우 중국 피험자의 동의서 내용은 베이징우의병원 자체 윤리위원회가 심사·승인한다. COLOR IV 협약 원문에 따르면,²⁵ COLOR III 보다 표현이 한 걸음 더 나아가, 현지 윤리위원회의 요구뿐만 아니라 현지 법규에도 부합할 것을 요구한다. 중국 측 피험자에 관하여 ‘현지 법규’는 PIPL 제 29 조(민감개인정보 단독 동의)와 제 39 조(국외 수령자 고지 후 단독 동의)를 포함하는 것으로 해석되어야 한다. 이 표현은 사실상 협약 차원에서 PIPL 적용의 규범적 접점을 열어 놓은 것이다. 협약 원문은 또한 두 가지 동의 요건을 명확히 구분한다. 즉 시험 개시 전 품질보증 단계(3 레의 수술 동영상)에는 별도의 동의가 요구되지 않으나, 시험 단계(정식 등록되는 모든 환자)에서는 반드시 충분한 설명에 근거한 동의를 취득하여야 한다.

베이징우의병원 자체 윤리위원회가 승인한 실제 동의서의 내용, 동의서가 PIPL 제 29 조와 제 39 조의 구체적 요건을 포괄하는지 여부, 사망 피험자 데이터의 처리, 동의 철회와 재동의 메커니즘 등 핵심 사항은 공개 경로에 밝혀져 있지 않다. 동의 철회 메커니즘에 관하여는, COLOR III 협약의 공개 문헌(Deijen 등이 2015 년 Surgical Endoscopy 에 발표한 프로토콜 논문)에 따르면 협약 차원에서 “환자는 연구의 어느 단계에서든 조건 없이 탈퇴할 수 있으며, 이미 수집된 데이터는 환자가 명시적으로 요구하지 않는 한 보존되어 분석에 포함된다”고 명시적으로 규정한다. 이러한 철회 메커니즘의 협약 차원 규정은 철회권 고지에 관한 ICH-GCP E6(R2) 제 4.8.10(m)항의 요건에 부합하고, PIPL 제 15 조가 규정하는 동의 철회권에도 부합한다. 다만 본 사건의 구체적 집행 차원 — 베이징우의병원 자체 윤리위원회의 해당 조항에 대한 현지화 처리,

²⁵ 원문 1: “All patients ... must provide informed consent in accordance with local regulations.” 원문 2: “The operative videos of the quality assessment phase will be evaluated ...” Wu S, Wei P, Gao J, Shu W, Zhao H, Bonjer H, Tuynman J, Yao H, Zhang Z; COLOR IV study group. COLOR IV: a multicenter randomized clinical trial comparing intracorporeal and extracorporeal anastomosis after laparoscopic right colectomy for right colon cancer. Surg Endosc. 2025 Feb;39(2):1182-1190 참조.

중국 측 피험자의 실제 철회 사례 유무, 철회 후 이미 국외이전된 데이터에 대한 소급 삭제 메커니즘의 가동 여부 등 — 은 모두 공개 경로에 밝혀져 있지 않다.

피험자 동의 단계에는 네 가지 규범 체계의 병행적용이 동시에 관련된다. 첫째, PIPL 제 29 조에 따라 민감개인정보(의료건강류)의 처리에는 단독 동의가 필요하다. 둘째, PIPL 제 39 조에 따라 국외로 개인정보를 제공하는 경우 국외 수령자의 명칭, 연락처, 처리목적, 처리방식, 개인정보의 종류 및 권리행사의 방식과 절차를 고지하고 단독 동의를 취득하여야 한다. 셋째, 인간 대상 연구의 윤리심사 규범으로서, 위계위(卫计委) 11 호령(2016)과 国卫科教发[2023]4 号 방법이 동의서에 대하여 실질적 요건을 정한다. 넷째, 국제 다기관 임상연구 협약으로서, COLOR IV 협약은 ‘현지 법규에 따라’ 동의를 취득할 것을 요구하는데, 이는 사실상 협약 차원에서 PIPL 제 29 조와 제 39 조를 승계한 것이다. 네 규범 체계의 동의 요건은 일부는 중첩되고 일부는 각각 독립적이며, 처리자는 그 전부를 동시에 충족하여야 비로소 컴플라이언스가 성립한다. 본 사건은 이러한 ‘조합적용’이 실무에서 구체적으로 어떻게 작동하는지를 관찰하는 전형적 표본이다.

9. 공개자료상 확인되지 않는 사항

앞에서 사실의 유형별로 본 사건의 객관적 사실을 정리하였으나, 공개자료의 한계로 인하여 일부 사실은 아직 규명되지 않았다. 본 연구의 사실기반을 투명하게 검증 가능하도록 하기 위하여, 본 절에서는 이들 미확인 사항을 그 소속 단계별로 전체적으로 설명하고 후속 연구의 확인 경로를 제시한다. 본 연구의 핵심 미확인 사항은 우선순위에 따라 세 층으로 정리할 수 있다. 제 1 층(가장 핵심적이며 컴플라이언스 판단을 좌우)은 동의 문제의 구체적

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구
컴플라이언스 설계이고, 제 2 층은 심사의 구체적 시점과 촉발 사유이며,
제 3 층은 기술적 세부사항이다.

규제 측면에서, 공개자료는 본 사건 심사 통과와 구체적 일자, 데이터 국외이전 안전평가를 촉발한 구체적 사유(즉 「데이터 국외이전 안전평가 방법」 제 4 조의 몇 호가 적용되었는지), 평가의 구체적 개시·종료일, 그리고 2024 년 9 월 평가 유효기간 만료 후의 처리 상황을 직접 밝히지 않았다. 베이징시 인터넷정보판공실의 본 사건에 대한 원(原) 통보 문건도 공개 경로에 직접 제시된 바 없으며, 본 연구가 인용하는 사실은 주로 베이징시 보건위생위원회 공식 홈페이지와 주요 매체의 전제 기사에 의한 것이다. 이러한 사실의 공백으로 인하여, 본 사건이 ‘핵심정보인프라 운영자의 국외이전 + 100 만 명 이상 규모 처리자의 국외이전’에 동시에 해당하는지에 대한 본 연구의 판단은 결론이 아닌 추론에 머무를 수밖에 없다.

병원 측면에서, 본 사건의 데이터 처리자인 베이징우의병원이 내부적으로 제정한 「데이터 국외이전 안전관리방법」의 전문, 병원이 보건위생 주관부처에 의하여 핵심정보인프라 운영자로 정식 인정되었는지 여부, 병원 각 정보시스템의 구체적인 네트워크안전등급보호 등급 결정 결과, PIPL 제 55 조가 요구하는 개인정보보호 영향평가 문서, 그리고 자체 윤리위원회의 COLOR III·COLOR IV 에 대한 심사 결정은 모두 공개 경로에 제시된 바 없다. 그중 병원 자체의 등급보호 등급 결정과 윤리심사 결정 두 가지가 특히 핵심적이다. 전자는 본 사건에 「데이터 국외이전 안전평가 방법」 제 4 조의 촉발 사유를 적용하는 판단 기초와 관련되고, 후자는 본 사건 피험자 동의 취득의 컴플라이언스 판단 기초와 관련된다.

프로젝트 측면에서, 미확인 사항은 다시 두 부류로 나눌 수 있다. 첫째 부류는 피험자 동의의 구체적 컴플라이언스 설계로서, 이는 개인정보 국외이전 컴플라이언스의 실무 운용상 가장 핵심적인 단계 중 하나이다. 베이징우의병원

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구 자체 윤리위원회가 승인한 실제 동의서의 내용, 동의서가 PIPL 제 29 조의 단독 동의와 제 39 조의 국외이전 고지 후 단독 동의 요건을 포괄하는지, 사망 피험자 데이터 처리, 동의 철회와 재동의 메커니즘의 본 사건에서의 구체적 설계는 공개 경로에 밝혀져 있지 않다.

둘째 부류는 데이터 전송의 기술적 세부사항이다. COLOR IV 협약은 중앙화 디지털 증례기록 시스템으로서 “secure digital case record form”을 명문으로 언급하나, 동 시스템의 암호화 방식, 데이터센터의 물리적 위치, 접근통제와 전송 프로토콜, 국외 수령 측의 저장 위치와 2 차 이전 등 기술적 세부사항은 공개자료에 밝혀져 있지 않다.

이로써 본 사건의 사실관계는 온전히 제시되었다. 이하에서는 규범 차원으로 전환한다. 제 3 장부터는 ‘사실을 먼저, 규범을 나중에’라는 기정 순서에 따라, 위 각 단계의 사실에 적용되는 중국법 규범을 층위별로 확정한다.

III. 법원(法源)

본 장에서는 규범의 위계 순서에 따라 본 사건에 적용되는 중국법 규범을 정리한다. 본 사건의 시간적 범위가 2017 년부터 현재까지 이어지고 COLOR IV 연구에 따라 2030 년까지 지속될 것이며, 그 사이 중국 데이터 거버넌스 입법이 근본적인 체계 구축을 겪었으므로, 본 장은 각 규범을 소개할 때 그 발포일·시행일 및 본 사건 각 단계와의 시점 대응관계를 명확히 표기한다.

1. 법률

가. 「네트워크안전법」

본 사건 COLOR IV 연구의 중국 측 재원은 2017 년에 선정되었고(국가중점연구개발계획 2017YFC0110904), 베이징우의병원의 COLOR

III 연구 참여는 2018 년 7 월이다. 두 시점 모두 본 법은 이미 시행 중이었다.

본 사건 관련 조문	관련성
제 21 조 국가는 네트워크안전등급보호제도를 시행한다. 네트워크 운영자는 네트워크안전등급보호제도의 요구에 따라 다음의 안전보호 의무를 이행하여 네트워크가 간섭·파괴되거나 무단으로 접근되지 않도록 보장하고 네트워크 데이터의 유출 또는 절취·변조를 방지하여야 한다. (1) 내부 안전관리제도와 운영규정을 제정하고 네트워크안전 책임자를 확정하며 네트워크안전 보호책임을 이행할 것, (2) 컴퓨터 바이러스와 네트워크 공격, 네트워크 침입 등 네트워크안전을 해치는 행위를 방지하는 기술조치를 취할 것, (3) 네트워크 운영상태와 네트워크안전 사건을 감시·기록하는 기술조치를 취하고 규정에 따라 관련 네트워크 로그를 6 개월 이상 보존할 것, (4) 데이터 분류, 중요데이터 백업 및 암호화 등의 조치를 취할 것, (5) 법률·행정법규가 규정하는 그 밖의 의무.	제 21 조가 확립한 네트워크안전등급보호제도는, 본 사건 데이터 국외이전 신고에서 “병원 정보센터가 네트워크안전·데이터안전을 다시 평가하여 병원의 네트워크안전 제도가 완비되고 실효성 있게 이행되며 안전방어 기술능력이 등급보호 등 표준규범에 부합함을 확인”한 것의 법률적 기초이다.

본 사건 관련 조문	관련성
	제 37 조가 확립한
제 37 조 핵심정보인프라의 운영자가 중화인민공화국 역내에서 운영 중 수집·생성한 개인정보와 중요데이터는 역내에 저장하여야 한다. 업무상 필요로 국외에 제공할 필요가 확실히 있는 경우에는 국가 인터넷정보 부서가 국무원 관련 부서와 함께 제정한 방법에 따라 안전평가를 실시하여야 한다. 법률·행정법규에 달리 규정이 있는 경우에는 그 규정에 따른다.	‘핵심정보인프라 운영자 데이터 현지화 원칙 + 예외적 안전평가’ 메커니즘은 본 사건 데이터 국외이전 신고의 가장 이른 법률적 기초이다. 다만 베이징우의병원이 핵심정보인프라 운영자로 인정되었는지는 공개자료에 명확히 나타나 있지 않다.

나. 「데이터안전법」

본 사건의 데이터 국외이전 신고는 2022 년 9 월에 개시되었고, 이때 본 법은 시행된 지 약 1 년이 경과한 상태였다.

본 사건 관련 조문	관련성
제 21 조 국가는 데이터 분류등급 보호제도를 수립하여, 데이터가 경제·사회 발전에서 가지는 중요도와 그것이 변조·파괴·유출되거나 불법으로 취득·이용될 경우 국가안전, 공공이익 또는 개인·조직의 적법한 권익에 초래할 위해의 정도에 따라 데이터를 분류등급하여 보호한다. 국가 데이터안전업무 조정기구는 관련	제 21 조가 확립한 ‘데이터 분류등급 보호제도’는 본 사건의 데이터 차원에서의 규제의 출발점이다.

본 사건 관련 조문	관련성
부서를 총괄·조정하여 중요데이터 목록을 제정하고 중요데이터에 대한 보호를 강화한다. 국가안전, 국민경제의 명맥, 중요한 민생, 중대한 공공이익 등과 관련되는 데이터는 국가핵심데이터로서 더욱 엄격한 관리제도를 시행한다. 각 지역·각 부서는 데이터 분류등급 보호제도에 따라 해당 지역·해당 부서 및 관련 업종·분야의 중요데이터 구체적 목록을 확정하고, 목록에 포함된 데이터를 중점적으로 보호하여야 한다. 제 31 조 핵심정보인프라의 운영자가 중화인민공화국 역내에서 운영 중 수집·생성한 중요데이터의 국외이전 안전관리에는 「네트워크안전법」의 규정을 적용한다. 그 밖의 데이터 처리자가 중화인민공화국 역내에서 운영 중 수집·생성한 중요데이터의 국외이전 안전관리방법은 국가 인터넷정보 부서가 국무원 관련 부서와 함께 제정한다.	제 31 조는 ‘중요데이터 국외이전’을 독립된 규제대상으로 삼는다. 본 사건이 관련된 의료데이터에 중요데이터가 존재한다면(2024 년 베이징 자유무역시험구 네거티브리스트의 의약산업 인정기준에 따르면 집단 진료, 특정 의약품 실험 데이터, 대규모 생체특징 데이터 등이 중요데이터에 해당한다²⁶), PIPL 제 38 조의 개인정보 국외이전 경로와는 별도로

²⁶《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局联合发布，2024 年 8 月 30 日，<https://www.beijing.gov.cn/zhengce/zhengcefagui/202409/W020240902597001758234.pdf>.

본 사건 관련 조문

관련성

「데이터안전법」 제 31 조의 중요데이터 국외이전 관리를 독립적으로 적용하여야 한다. 다만 본 사건의 심사는 2022 년 9 월에 완료되었고, 위 인정기준은 본 사건 심사 이후(2024 년 8 월)에 발표되었다.

다. 「개인정보보호법」

본 사건의 데이터 국외이전 신고는 2022 년 9 월에 개시되었고, 이때 본 법은 시행된 지 약 10 개월이 경과한 상태였다.

본 사건 관련 조문

제 28 조 민감개인정보란 일단 유출되거나 불법으로 사용되면 자연인의 인격존엄이 침해되거나 신체·재산의 안전이 위해를 받기 쉬운 개인정보로서, 생체인식, 종교신앙, 특정신분, 의료건강, 금융계좌, 행적정보 등의 정보 및 14 세 미만 미성년자의 개인정보를 포함한다. 개인정보 처리자는 특정한 목적과 충분한 필요성이 있고 엄격한 보호조치를 취하는 경우에 한하여 민감개인정보를 처리할 수 있다.

제 29 조 민감개인정보를 처리하는 경우에는 개인의 단독 동의를 취득하여야 한다. 법률·행정법규가 민감개인정보의 처리에 서면 동의를 취득하도록 규정한 경우에는 그 규정에 따른다.

제 38 조 개인정보 처리자가 업무 등의 필요로 중화인민공화국 역외에 개인정보를 제공할 필요가 확실히 있는 경우에는 다음 중 하나의 요건을 갖추어야 한다. (1) 본 법 제 40 조의 규정에 따라 국가 인터넷정보 부서가 조직하는 안전평가를 통과할 것, (2) 국가 인터넷정보 부서의 규정에 따라

전문기관의 개인정보보호 인증을 받을 것, (3) 국가 인터넷정보 부서가 제정한 표준계약에 따라 국외 수령자와 계약을 체결하여 쌍방의 권리와 의무를 약정할 것, (4) 법률·행정법규 또는 국가 인터넷정보 부서가 규정하는 그 밖의 요건.

제 39 조 개인정보 처리자가 중화인민공화국 역외에 개인정보를 제공하는 경우에는 국외 수령자의 명칭 또는 성명, 연락처, 처리목적, 처리방식, 개인정보의 종류 및 개인이 국외 수령자에 대하여 본 법이 규정하는 권리를 행사하는 방식과 절차 등의 사항을 개인에게 고지하고 개인의 단독 동의를 취득하여야 한다.

제 40 조 핵심정보인프라 운영자 및 국가 인터넷정보 부서가 규정하는 수량에 달하는 개인정보를 처리하는 개인정보 처리자는 중화인민공화국 역내에서 수집·생성한 개인정보를 역내에 저장하여야 한다. 국외에 제공할 필요가 확실히 있는 경우에는 국가 인터넷정보 부서가 조직하는 안전평가를 통과하여야 한다. 법률·행정법규 및 국가 인터넷정보 부서가 안전평가를 실시하지 아니할 수 있다고 규정한 경우에는 그 규정에 따른다.

제 55 조 다음 중 하나에 해당하는 경우, 개인정보 처리자는 사전에 개인정보보호 영향평가를 실시하고 처리 상황을 기록하여야 한다. (1) 민감개인정보를 처리하는 경우, (2) 개인정보를 이용하여 자동화된 의사결정을 하는 경우, (3) 개인정보의 처리를 위탁하거나 다른 개인정보 처리자에게 개인정보를 제공하거나 개인정보를 공개하는 경우, (4) 국외에 개인정보를 제공하는 경우, (5) 그 밖에 개인의 권익에 중대한 영향을 미치는 개인정보 처리활동.

본 사건과의 관련성: 첫째, 본 사건이 관련된 의료데이터에는 진료기록, 검사, 영상, 수술 후 추적관찰 등의 내용이 포함되며, 제 28 조에 따라 민감개인정보(‘의료건강’류)에 해당한다. 둘째, 제 29 조에 따라 민감개인정보의

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

처리에는 개인의 단독 동의가 필요하고, 제 39 조에 따라 국외에 개인정보를 제공하는 경우에도 개인의 단독 동의를 취득하여야 한다. 본 사건에서 피험자 동意的 취득 방식, 범위, 형식 등 구체적 세부사항은 공개 경로에 밝혀져 있지 않아 추가 확인이 필요하다. 셋째, 본 사건은 제 38 조 제 1 호의 ‘국외이전 안전평가’ 경로를 선택하였다. 구체적으로 어느 사유가 촉발되었는지(CIIO 지위, 100 만 명 이상 규모, 누적 1 만 명 이상 민감개인정보)는 공개자료에 밝혀져 있지 않다. 넷째, 제 55 조에 따라 본 사건은 개인정보보호 영향평가를 이미 완료하였을 것이나, 그 평가 문서는 공개되지 않았다.

라. 「생물안전법」

본 사건의 데이터 국외이전 신고는 2022 년 9 월에 개시되었고, 이때 본 법은 시행된 지 약 1 년 반이 경과한 상태였다.

본 사건 관련 조문

제 53 조 국가는 우리나라 인류유전자원과 생물자원에 대한 보호를 강화한다.
국가는 우리나라 인류유전자원과 생물자원에 대하여 주권을 가진다.

제 55 조 우리나라 인류유전자원의 채집·보존·이용·국외제공은 윤리원칙에 부합하여야 하며, 공중보건, 국가안전과 사회공공이익을 해쳐서는 아니 된다.

본 사건과의 관련성: 본 법은 「인류유전자원관리조례」의 상위법적 근거이다. 본 사건이 인류유전자원(즉 유전자/게놈 데이터)과 관련되는지를 현재의 공개자료로 판단하면 다음과 같다. COLOR III·COLOR IV 협약의 공개내용에 따르면 연구데이터는 주로 임상 표현형, 영상의학적 평가(CT, MRI), 수술 과정 데이터, 병리 평가, 수술 후 회복 지표, 추적관찰 데이터를 포함한다.²⁷ 두

²⁷Wu S, Wei P, Gao J, Shu W, Zhao H, Bonjer H, Tuynman J, Yao H, Zhang Z; COLOR IV study group. COLOR IV: a multicenter randomized clinical trial comparing intracorporeal and extracorporeal anastomosis after laparoscopic right colectomy for right colon cancer. Surg Endosc. 2025 Feb;39(2):1182-1190 참조.

마붕초- 중국 의료데이터 국외이전 규제에 관한 연구

협약의 공개 문서에는 유전자 시퀀싱이나 게놈 데이터의 수집이 명시적으로 언급되어 있지 않다. 「인류유전자원관리조례 실시세칙」 제2조 제3항의 제외적 획정(후술)에 따르면 임상데이터, 영상데이터, 단백질데이터와 대사데이터는 인류유전자원정보에 속하지 않는다. 따라서 본 사건은 「생물안전법」과 「인류유전자원관리조례」의 절차를 직접 촉발하지 않을 개연성이 크다. 다만 최종 판단을 위하여는 연구에서 생물학적 시료(병리 표본 포함)의 국외제공이 있었는지를 추가로 확인할 필요가 있다.

2. 행정법규

가. 「인류유전자원관리조례」

본 사건의 COLOR III 참여 시점(2018 년 7 월)에는 본 조례가 아직 시행되기 전이었고, 데이터 국외이전 신고 개시 시점(2022 년 9 월)에는 시행된 지 약 3 년이 경과한 상태였다.

본 사건 관련 조문

제 2 조 중화인민공화국 역내에서 중국 인류유전자원의 채집·보존·이용·국외제공 활동에 종사하는 경우 본 조례를 적용한다. 본 조례에서 말하는

인류유전자원은 인류유전자원 재료와 인류유전자원 정보를 포함한다.

인류유전자원 재료란 인체 게놈·유전자 등 유전물질을 함유한 장기·조직·세포 등의 유전 재료를 말한다. 인류유전자원 정보란 인류유전자원 재료를 이용하여 생성된 인류 유전자·게놈 데이터 등의 정보자료를 말한다.(주: 여기서 ‘인류 유전자·게놈 데이터’라는 한정은 2023 년 7 월 1 일 시행된

「인류유전자원관리조례 실시세칙」의 기준에 따른 것이며, 2019 년 조례 원문의 표현은 ‘인류유전자원 재료를 이용하여 생성된 데이터 등 정보자료’이다.)

제 7 조 외국의 조직·개인 및 그가 설립하거나 실질적으로 지배하는 기관은 우리나라 역내에서 우리나라 인류유전자원을 채집·보존하여서는 아니 되며,

우리나라 인류유전자원을 국외에 제공하여서는 아니 된다.

제 21 조 우리나라 인류유전자원 재료를 운송·우송·휴대하여 출국시키는 경우에는 다음의 요건에 부합하여야 하며 국무원 과학기술 행정부서의 허가를 받아야 한다. (1) 우리나라 공중보건, 국가안전과 사회공공이익을 해치지 아니할 것, (2) 법인 자격을 가질 것, (3) 명확한 국외 협력 상대방과 합리적인 출국 용도가 있을 것, (4) 인류유전자원 재료의 채집이 적법할 것, (5) 윤리심사를 통과할 것. 우리나라 인류유전자원 정보를 국외의 조직·개인 및 그가 설립하거나 실질적으로 지배하는 기관에 제공하거나 개방하여 사용하게 하는 경우에는 국무원 과학기술 행정부서에 사전에 보고하고 정보의 사본을 제출하여야 한다.

본 사건과의 관련성: 본 조례의 인류유전자원 규제는 인터넷정보 부서가 주도하는 데이터 국외이전 규제와는 독립적이다. 베이징시 보건위생위 공식 홈페이지의 보도자료 원문은 본 사건 심사에서 “병원 과학기술처가 이 임상연구 프로젝트의 그간의 수행 상황, 과학적 의의와 산출 가치, 인류유전자원 등 측면의 상황을 심층 평가하였다”고 명시적으로 언급한다. 이 표현은 병원이 내부 심사 단계에서 인류유전자원 관련 상황을 심사하였음을 보여준다. 다만 그 심사 결론이 인류유전자원관리조례 제 21 조의 과기부 허가 절차를 발동시켰는지는 공개자료에 밝혀져 있지 않다.

나. 「핵심정보인프라 안전보호조례」

본 사건의 데이터 국외이전 신고 개시 시점(2022 년 9 월)에 본 조례는 시행된 지 만 1 년이 경과한 상태였다.

본 사건 관련 조문

제 2 조 본 조례에서 말하는 핵심정보인프라란 공공통신과 정보서비스, 에너지, 교통, 수리(水利), 금융, 공공서비스, 전자정부, 국방과학기술공업 등 중요 업종·분야의, 그리고 그 밖에 일단 파괴되거나 기능을 상실하거나 데이터가 유출될 경우 국가안전, 국민경제와 민생, 공공이익을 중대하게 해칠 수 있는 중요 네트워크 시설, 정보시스템 등을 말한다.

제 8 조 본 조례가 규정하는 중요 업종·분야의 주관부서·감독관리부서는 핵심정보인프라 안전보호 업무를 담당하는 부서(이하 ‘보호업무부서’)이다.

본 사건과의 관련성: 본 사건에서 베이징우의병원이 핵심정보인프라 운영자로 인정되었는지는 공개자료에 명확히 나타나 있지 않다. 베이징우의병원은 대형 3 급 갑등 병원이자 국가소화기질환 임상의학연구센터의 수행기관으로서 의료 분야에서 상당한 규모를 가지나, 구체적으로 CIIO 인정이 완료되었는지와 그 인정 시점은 추가 확인이 필요하다.

다. 「네트워크데이터 안전관리조례」

본 조례는 본 사건의 2022~2023 년 최초 심사에는 직접 적용되지 않으나, 2025 년 1 월 이후의 컴플라이언스 지속에 대하여 규범적 의의를 가진다. 아래 조문은 본 사건의 후속 컴플라이언스 지속 단계(2025 년 1 월 1 일 이후)와 구체적으로 관련된다.

본 사건 관련 조문

관련성

제 12 조 네트워크데이터 처리자가 본 조는 제공자와 수령자 사이의 계약 다른 네트워크데이터 처리자에게 약정, 수령자의 의무 이행에 대한 감독, 개인정보와 중요데이터를 제공하거나 그리고 처리기록 3 년 보존 의무를

본 사건 관련 조문	관련성
그 처리를 위탁하는 경우에는 계약 등을 통하여 네트워크데이터 수령자와 처리목적·방식·범위 및 안전보호 의무 등을 약정하고, 네트워크데이터 수령자의 의무 이행 상황을 감독하여야 한다. 다른 네트워크데이터 처리자에게 개인정보와 중요데이터를 제공하거나 그 처리를 위탁한 처리 상황의 기록은 3 년 이상 보존하여야 한다. 네트워크데이터 수령자는 네트워크데이터 안전보호 의무를 이행하여야 하며, 약정된 목적·방식·범위 등에 따라 개인정보와 중요데이터를 처리하여야 한다.	행정법규 차원에서 처음으로 명확히 규정하였다. 본 사건의 베이징우의병원과 Amsterdam UMC 사이의 협력 협약은 2025 년 이후 본 조의 요건에 부합하여야 한다. 다른 네트워크데이터 처리자에게 개인정보와 중요데이터를 제공하거나 그 처리를 위탁한 처리 상황의 기록은 3 년 이상 보존하여야 한다. 네트워크데이터 수령자는 네트워크데이터 안전보호 의무를 이행하여야 하며, 약정된 목적·방식·범위 등에 따라 개인정보와 중요데이터를 처리하여야 한다.
제 22 조 네트워크데이터 처리자가 개인의 동의에 기초하여 개인정보를 처리하는 경우에는 다음의 규정을 준수하여야 한다. (1) 개인정보의 수집은 제품 또는 서비스의 제공에 필요한 범위로 한정하고, 범위를 초과하여 개인정보를 수집하지 아니하며, 오도·사기·강박 등의 방식으로 개인의 동의를 취득하지	본 조 제 2 호는 ‘의료건강’류 민감개인정보의 처리에 단독 동의를 필요함을 재확인하여 PIPL 제 29 조를 행정법규 차원에서 승계한다. 본 조 제 6 호는 처리목적·방식·종류가 변경되는 경우 동의를 다시 취득하도록 규정하여, 본 사건 컴플라이언스 지속 단계(예컨대 국외이전 데이터의 범위 또는 종류가 변경되는 경우)의 ‘재동의’ 의무를 명확히

본 사건 관련 조문	관련성
아니할 것, (2) 생체인식, 종교신앙, 규정한다. 특정신분, 의료건강, 금융계좌, 행정정보 등 민감개인정보를 처리하는 경우에는 개인의 단독 동의를 취득할 것, (3) 14 세 미만 미성년자의 개인정보를 처리하는 경우에는 미성년자의 부모 또는 그 밖의 후견인의 동의를 취득할 것, (4) 개인이 동의한 개인정보의 처리목적·방식·종류·보존기간을 초과하여 개인정보를 처리하지 아니할 것, (5) 개인이 자신의 개인정보 처리에 동의하지 아니함을 명확히 표시한 후 빈번하게 동의를 구하지 아니할 것, (6) 개인정보의 처리목적·방식·종류가 변경되는 경우에는 개인의 동의를 다시 취득할 것.	
제 27 조 네트워크데이터 처리자는 본 조는 개인정보 처리자에게 정기적 정기적으로 스스로 또는 전문기관에 컴플라이언스 감사 의무를 신설하였다. 위탁하여 개인정보 처리의 법률·행정법규 준수 상황에 대한 컴플라이언스 감사를 실시하여야 한다.	본 사건의 데이터 국외이전은 지속적이므로(COLOR IV 는 2030 년까지 지속 예정), 베이징우의병원은 2025 년 이후 본 조에 따라 정기적 컴플라이언스

본 사건 관련 조문	관련성
제 28 조 1,000 만 명 이상의 개인정보를 처리하는 네트워크데이터 편입시킨다. 베이징우의병원이 대형 3 급 처리자는 본 조례 제 30 조, 제 32 조가갑등 종합병원으로서 1,000 만 명 기준에 중요데이터를 처리하는 네트워크데이터 처리자(이하 ‘중요데이터 처리자’)에 대하여 규정한 사항도 준수하여야 한다.	감사 의무를 이행하여야 한다. 본 조는 ‘1,000 만 명 이상의 개인정보를 처리하는 네트워크데이터 처리자’를 중요데이터 처리자의 의무체계에 도달하는지는 공개자료에 밝혀져 있지 않으나, 도달한다면 중요데이터 처리자에 준하여 제 30 조(안전책임자, 안전관리기구)와 제 32 조(합병·분할·해산·파산 시 보고의무)의 규정을 부담하여야 한다.
제 35 조 다음 중 하나의 요건에 부합하는 경우, 네트워크데이터 처리자는 국외에 개인정보를 제공할 수 있다. (1) 국가 인터넷정보 부서가 조직하는 데이터 국외이전 안전평가를 통과한 경우, (2) 국가 인터넷정보 부서의 규정에 따라 전문기관의 개인정보보호 인증을 받은 경우, (3) 국가 인터넷정보 부서가 제정한 개인정보 국외이전 표준계약에 관한 규정에 부합하는 경우, (4) 개인이 일방 당사자인	본 조는 PIPL 제 38 조가 규정한 세 가지 경로를 여덟 가지 컴플라이언스 사유로 확장한다. 본 사건은 본래 제 1 호의 국외이전 안전평가 경로를 적용하였으나, 2024 년 9 월 평가 유효기간 만료 후의 컴플라이언스 지속에서는 본 조에 기초하여 다른 경로(표준계약, 인증, 또는 제 6 호의 법정 직책 경로 등)의 적용을 선택할 수 있다.

본 사건 관련 조문	관련성
계약의 체결·이행을 위하여 국외에 개인정보를 제공할 필요가 확실히 있는 경우, (5) 법에 따라 제정된 노동규칙제도와 법에 따라 체결된 단체협약에 따라 국경 간 인적자원 관리를 실시하기 위하여 국외에 근로자의 개인정보를 제공할 필요가 확실히 있는 경우, (6) 법정 직책 또는 법정 의무의 이행을 위하여 국외에 개인정보를 제공할 필요가 확실히 있는 경우, (7) 긴급상황에서 자연인의 생명·건강과 재산의 안전을 보호하기 위하여 국외에 개인정보를 제공할 필요가 확실히 있는 경우, (8) 법률·행정법규 또는 국가 인터넷정보 부서가 규정하는 그 밖의 요건.	
제 37 조 네트워크데이터 처리자가 본 조는 ‘중요데이터 국외이전 신고’에 중화인민공화국 역내에서 운영 중 관하여 ‘사전 공표·고지’ 원칙을 수집·생성한 중요데이터를 국외에 채택한다. 즉 관련 주관부처로부터 제공할 필요가 확실히 있는 경우에는 고지받거나 공개발표로 중요데이터로 국가 인터넷정보 부서가 조직하는 지정되지 않은 경우에는 중요데이터로 데이터 국외이전 안전평가를 신고할 필요가 없다. 본 사건 심사 통과하여야 한다. 네트워크데이터 시(2022 년)에는 ‘중요데이터 관련 처리자는 국가의 관련 규정에 따라 여부’의 판단이 규범 차원에서	

본 사건 관련 조문	관련성
중요데이터를 식별·신고하되, 관련 지역·부서로부터 중요데이터로 고지받거나 공개발표되지 아니한 경우에는 이를 중요데이터로 하여 데이터 국외이전 안전평가를 신고할 필요가 없다.	불명확하였으나, 본 조는 2025 년 이후 이 문제에 명확한 판단규칙을 제공한다. 즉 주관부처가 사전에 고지하거나 공개적으로 공표하지 않는 한 본 사건 데이터는 ‘중요데이터’를 구성하지 않으며, 중요데이터 신고 경로를 밟을 필요가 없다.
제 38 조 데이터 국외이전 안전평가를 통과한 후, 네트워크데이터 처리자가 국외에 개인정보와 중요데이터를 제공하는 경우에는 평가 시 명확히 한 데이터 국외이전의 목적·방식·범위와 종류·규모 등을 초과하여서는 아니 된다.	본 사건의 원 심사는 2022 년에 이루어졌고, 그 시점에 COLOR III 는 베이징우의병원 단일기관 170 례 등록, COLOR IV 는 전 세계 1,158 례 등록 계획이었다. 본 사건에서 2025 년 이후 실제 국외이전의 목적·방식·범위, 데이터의 종류 또는 규모가 2022 년 원 평가의 범위를 초과하는 경우에는 데이터 국외이전 안전평가를 다시 신고하여야 한다.

3. 부문규장

가. 「국가 건강의료빅데이터 표준·안전·서비스 관리방법(시행)」

본 사건의 COLOR III 참여 시점(2018 년 7 월)에는 본 방법이 아직 발표되기 전이었고, COLOR IV 의 준비 및 신고 시점(2022 년)에는 이미 시행 중이었다.

본 사건 관련 조문

제 16 조 건강의료빅데이터 안전관리란 데이터의 채집·저장·발굴·응용·운영·전송

등 여러 단계에서의 안전과 관리를 말하며, 국가전략 안전, 인민 생명 안전, 개인정보 안전에 관한 권한·책임 관리 업무를 포함한다.

제 17 조 책임단위는 관련 안전관리제도·운영규정과 기술규범을 수립·정비하고, ‘최고책임자’ 책임제를 이행하며, 안전보장체계의 구축을 강화하고, 총괄관리와 조정·감독을 강화하여 건강의료빅데이터의 안전을 보장하여야 한다.

본 방법은 의료데이터 전생애주기 관리의 가장 이른 완결적 표현이다. 본 방법 제 16 조에 열거된 ‘채집·저장·발굴·응용·운영·전송’의 여섯 단계는 이후 중국 의료데이터 거버넌스 체계의 기초 골격이 되었다. 본 방법은 본 사건 각 단계의 의료데이터 처리활동에 직접적인 규범력을 가진다.

나. 「의료보건기관 네트워크안전 관리방법」

본 방법은 본 사건의 데이터 국외이전 신고 개시(2022년 9월 1일) 불과 며칠 전에 시행되었다. 본 사건의 베이징우의병원은 의료보건기관 주체로서 본 방법에 따라 업종상의 의무를 이행하여야 한다.

본 사건 관련 조문	관련성
제 2 조 네트워크안전은 인민을 위한 것이고 인민에 의거한다는 원칙을 견지하고, 네트워크안전 교육·기술·산업의 융합 발전을 견지하며, 발전 촉진과 법에 따른 관리의 통일을 견지하고, 안전·통제가능성과 개방·혁신의 병행을 견지한다.	본 조는 의료보건기관 네트워크안전의 중점 보호대상 — CIIO, 네트워크안전등급보호 제 3 급 이상의 네트워크, 중요데이터와 개인정보의 네 부류 — 를 명확히 한다.
등급별 보호와 중점의 부각을	베이징우의병원은 대형 3 급 갑등 종합병원이자 국가급 임상의학연구센터의 수행기관으로서, 그 핵심 정보시스템은 업계 관행상 제 3 급

본 사건 관련 조문	관련성
견지한다. 핵심정보인프라, 네트워크안전등급보호 제 3 급(이하 ‘제 3 급’) 이상의 네트워크 및 중요데이터와 개인정보의 안전을 중점적으로 보장한다. 제 5 조 각 의료보건기관은 네트워크안전·정보화 업무 영도소조를 구성하고, 기관의 주요 책임자가 영도소조 조장을 맡으며, 매년 1 회 이상 네트워크안전 업무회의를 개최하여 안전 중점업무를 배치하고, 「핵심정보인프라 안전보호조례」와 네트워크안전등급보호제도의 요구를 이행하여야 한다. 제 2 급 이상의 네트워크를 보유한 의료보건기관은 네트워크안전 관리업무를 담당하는 직능부서를 명확히 하고, 안전 주관자·안전 관리자 등의 직책을 담당하는 직위를 명확히 하며, 네트워크안전 관리제도 체계를 수립하고 네트워크안전 방어를 강화하며 비상대응을 강화하고, 그 기초 위에서 핵심정보인프라에 대하여 중점 보호를 실시하여 네트워크안전	이상으로 등급이 결정되어 본 방법의 중점 보호를 받아야 할 것이다. 본 조는 의료보건기관에 전문적인 네트워크안전 거버넌스 조직의 설치를 요구한다. 베이징우의병원의 본 사건 데이터 국외이전 신고에서는 ‘병원 정보센터’가 네트워크안전·데이터안전의 재평가를 담당하였는데, 이 업무 조직이 곧 본 조에서 말하는 직능부서에 해당할 것이다.

본 사건 관련 조문

사건의 발생을 방지하여야 한다.

제 6 조 각 의료보건기관은 ‘주관하는

자가 책임지고, 운영하는 자가

책임지며, 사용하는 자가 책임진다’는

원칙에 따라 네트워크 구축 과정에서

해당 기관 각 네트워크의

주관부서·운영부서·정보화부서·사용부서

등의 관리책임을 명확히 하고, 해당

기관 운영범위 내의 네트워크에 대하여

등급보호 등급

결정·비안(备案)·측정평가·안전구축

시정 등의 업무를 수행하여야 한다.

(4) 각 의료보건기관은 이미 등급이 결정되어 비안된 네트워크의 안전성에 대하여 검측·평가를 실시한다. 제 3 급 또는 제 4 급의 네트워크는 등급보호 측정평가기관에 위탁하여 매년 1 회 이상 네트워크안전 등급측정평가를 실시하여야 한다. 제 2 급의 네트워크는 등급보호 측정평가기관에 위탁하여

정기적으로 네트워크안전

등급측정평가를 실시하되, 그중 10 만

명 이상의 개인정보가 관련되는

네트워크는 3 년에 1 회 이상, 그 밖의

관련성

본 조는 의료기관의

네트워크안전등급보호 등급 결정과

측정평가 주기에 대하여 구체적인

요구를 정한다. 베이징우의병원은 본

사건 데이터 국외이전 신고 전에

네트워크안전등급보호 컴플라이언스

재평가를 완료하였는데, 그 평가는 본

조의 요구에 따라 수행되었을 것이다.

본 사건에 관한 베이징시 보건위생위

공식 보도자료 원문에 따르면 병원

정보센터는 “안전방어 기술능력이

등급보호 등 표준규범에 부합”함을

확인하였는데, 이 표현은 사실상 본

조가 규정하는 ‘등급측정평가’ 의무에

대응한다. 베이징우의병원 각

정보시스템의 구체적인 등급 결정과

측정평가 결과는 공개자료에 밝혀져

있지 않다.

본 사건 관련 조문

네트워크는 5 년에 1 회 이상
네트워크안전 등급측정평가를
실시하여야 한다.

관련성

본 조는 의료보건기관의 데이터
분류등급에 대하여 강행적 요구 —

제 20 조 각 의료보건기관은 매년 데이터 자산을 전면적으로 정리하고, 네트워크안전등급보호제도의 이행을 기초로 데이터의 중요도와 파괴 시의 위해 정도에 따라 해당 기관의 데이터 분류등급 기준을 수립하여야 한다. 데이터 분류등급은 적법·준법 원칙, 실행가능성 원칙, 시효성 원칙, 자율성 원칙, 차등성 원칙 및 객관성 원칙을 따라야 한다.

매년 정리 + 자체 등급기준 수립 — 를 정한다. 베이징우의병원이 본 사건 심사에서 식별한 의료데이터 민감도(GB/T 39725-2020 의 4 등급 민감도 기준)와 ‘중요데이터’ 판정은 사실상 본 조를 업종규범상의 근거로 한다. 본 사건 데이터의 ‘중요데이터’ 관련 여부는 공개자료에 밝혀져 있지 않으나, 본 조가 병원 스스로 분류등급 기준을 수립하도록 요구하므로 그 판단은 병원 내부에서 이미 완료되었을 것이다.

제 21 조 각 의료보건기관은 데이터 안전관리제도·운영규정 및 기술규범을 수립·정비하고, 관련 관리제도를 매년 1 회 이상 개정하며, 관련 인원이 매년 비밀유지협약을 체결할 것을 권장한다. 매년 해당 기관의 데이터에 대하여 데이터안전 위험평가를 실시하여

본 조는 의료기관에 매년 데이터안전 위험평가의 실시를 요구한다. 본 사건의 COLOR IV 는 2030 년까지 지속되므로, 병원은 본 조에 따라 매년 데이터안전 상태를 평가하여야 한다.

본 사건 관련 조문

데이터안전 상태를 적시에 파악한다.

데이터안전 교육·훈련을 강화하고
안전의식 교육과 데이터 안전관리제도
홍보·훈련을 조직한다. 해당 기관의
실정에 맞추어 데이터 사용 신청 및
승인 절차를 수립·정비하고, ‘주관하는
자가 심사한다’는 원칙과 사전
신청·승인, 과정 중 감독, 사후 심사의
원칙을 따르며, 업무관리부서의 동의와
의료보건기관 책임자의 승인이라는
업무절차를 엄격히 집행하여 데이터
활동 절차의 컴플라이언스를 지도한다.

제 22 조 각 의료보건기관은 데이터의
수집·저장·전송·처리·사용·교환·파기
전생애주기 안전관리 업무를
강화하여야 하고, 데이터 전생애주기
활동은 역내에서 수행하여야 하며,
업무상 국외에 제공할 필요가 확실히
있는 경우에는 관련 법령 및 관련
요구에 따라 안전평가 또는 심사를
실시하여야 하고, 국가안전에 영향을
미치거나 미칠 수 있는 데이터
처리활동에 대하여는 국가안전심사에
회부하여 데이터안전 사건의 발생을

관련성

본 조는 본 방법 가운데 본 사건과
가장 직접 관련되는 조문이다. 본 조는
두 가지 규칙을 명문으로 확립한다.

첫째, 의료보건기관의 데이터
전생애주기 활동은 역내에서
수행하여야 한다는 것으로, 이는
의료업종 차원에서 ‘데이터 현지화’
원칙을 명문화한 표현이다. 둘째,
업무상 국외에 제공할 필요가 확실히
있는 경우에는 관련 법령 및 관련
요구에 따라 안전평가 또는 심사를
실시하여야 한다는 것으로, 본 사건의

본 사건 관련 조문

방지하여야 한다.

(1) 각 의료보건기관은 데이터 수집의 적법성 관리를 강화하고, 데이터 수집의 적법성에 관한 업무부서와 관리부서의 주체적 책임을 명확히 하여야 한다. 데이터 마스킹, 데이터 암호화, 링크 암호화 등의 통제조치를 취하여 데이터 수집 과정에서의 데이터 유출을 방지한다.

(2) 데이터 분류등급의 기초 위에서 서로 다른 안전등급 데이터의 암호화 전송 요건을 더욱 명확히 한다. 전송 과정의 인터페이스 안전통제를 강화하여 인터페이스를 통한 전송 시의 안전성을 확보하고 데이터의 절취를 방지한다.

(3) 각 의료보건기관은 관련 법규·표준에 따라 적합한 데이터 저장 아키텍처와 매체를 선택하여 역내에 저장하고, 백업·암호화 등의 조치로 데이터의 저장 안전을 강화하여야 한다. 클라우드 저장이 관련되는 경우에는 초래될 수 있는 안전위험을 평가하여야 한다. 데이터 저장기간은

관련성

데이터 국외이전은 바로 본 조가 지시하는 ‘안전평가’ 경로(즉 「데이터 국외이전 안전평가 방법」)에 따라 신고가 개시된 것이다.

본 사건 관련 조문

관련성

데이터 사용규칙이 정한 보존기간을
초과하여서는 아니 된다. 저장 과정의
접근통제 안전, 데이터 사본 안전,
데이터 아카이브 안전 관리를
강화한다.

(4) 각 의료보건기관은 인원별 권한을
엄격히 정하고, 데이터 사용 과정의
신청·승인 절차 관리를 강화하여
데이터가 통제 가능한 범위에서
사용되도록 하며, 로그 보존·관리
업무를 강화하고 로그의 변조·삭제
현상을 근절하여 데이터의 월권 사용을
방지하여야 한다. 각 데이터
사용부서와 사용자는 신청서에 기재된
용도와 범위에 따라 엄격히 데이터를
사용하여야 하며 데이터의 안전에
책임을 진다. 승인 없이는 어떠한
부서·개인도 대외에 공개되지 아니한
정보·데이터를 부서 밖으로
전달하여서는 아니 되며, 어떠한
방식으로도 이를 유출하여서는 아니
된다.

(5) 각 의료보건기관은 데이터를
공표·공유할 때 초래될 수 있는

본 사건 관련 조문

관련성

안전위험을 평가하고 필요한 안전통제 조치를 취하여야 한다. 데이터 상부 보고가 관련되는 경우에는 보고 제기 측이 보고 요구의 해석을 담당하고 보고 범위와 보고 규칙을 확정하여 데이터 보고의 안전·통제가능성을 확보한다.

(6) 각 의료보건기관이 안면인식 또는 안면식별을 실시하는 경우에는 비(非)안면인식 신원확인 방식을 함께 제공하여야 하며, 정보주체가 안면인식 데이터의 수집에 동의하지 아니한다는 이유로 정보주체의 기본 업무기능 사용을 거부하여서는 아니 되고, 안면인식 데이터는 신원확인 이외의 목적 — 정보주체의 업무성과, 경제상황, 건강상태, 선호, 관심 등에 대한 평가 또는 예측을 포함하되 이에 한하지 아니한다 — 에 사용하여서는 아니 된다. 각 의료보건기관은 안면인식 데이터의 저장·전송에 안전조치를 취하여야 하며, 여기에는 안면인식 데이터의 암호화 저장·전송, 안면인식 데이터와 개인 신원정보의

본 사건 관련 조문

관련성

물리적 또는 논리적 분리 저장 등이

포함되되 이에 한하지 아니한다.

(7) 데이터를 파기할 때에는 데이터의

복원이 불가능함을 보장하는 파기

방식을 채택하여야 하며, 데이터 잔존

위험과 데이터 백업 위험에 중점적으로

주의한다.

다. 「데이터 국외이전 안전평가 방법」

본 방법은 본 사건의 직접적인 신고 근거이다. 본 사건의 신고 개시 시점(2022 년 9 월)은 본 방법의 시행 시점과 완전히 겹친다.

본 사건 관련 조문

제 4 조 데이터 처리자가 국외에 데이터를 제공하는 경우로서 다음 중 하나에 해당하는 때에는 소재지 성급 인터넷정보 부서를 통하여 국가 인터넷정보 부서에 데이터 국외이전 안전평가를 신고하여야 한다. (1) 데이터 처리자가 국외에 중요데이터를 제공하는 경우, (2) 핵심정보인프라 운영자 및 100 만 명 이상의 개인정보를 처리하는 데이터 처리자가 국외에 개인정보를 제공하는 경우, (3) 전년 1 월 1 일부터 누적하여 10 만 명의 개인정보 또는 1 만 명의 민감개인정보를 국외에 제공한 데이터 처리자가 국외에 개인정보를 제공하는 경우, (4) 국가 인터넷정보 부서가 규정하는 그 밖에 데이터 국외이전 안전평가의 신고가 필요한 경우.

제 8 조 데이터 국외이전 안전평가는 데이터 국외이전 활동이 국가안전, 공공이익, 개인 또는 조직의 적법한 권익에 초래할 수 있는 위험을 중점적으로 평가하며, 주로 다음의 사항을 포함한다. (1) 데이터 국외이전의 목적·범위·방식

등의 적법성·정당성·필요성, (2) 국외 수령자가 소재한 국가 또는 지역의 데이터안전 보호 정책·법규와 네트워크안전 환경이 전송되는 데이터의 안전에 미치는 영향, 국외 수령자의 안전보호 수준이 중화인민공화국 법률·행정법규의 규정과 강제성 국가표준의 요구에 도달하는지 여부, (3) 국외이전 데이터의 규모·범위·종류·민감정도, 데이터의 국외이전 중 및 국외이전 후의 변조·파괴·유출·분실·이전 또는 불법 취득·불법 이용 등의 위험, (4) 데이터 처리자와 국외 수령자가 체결하는 법률문서에 데이터안전 보호의 책임·의무가 충분히 약정되어 있는지 여부, (5) 본 방법이 규정한 절차 이행의 적법성, 중국의 법률·행정법규·부문규장 규정예의 부합 여부, (6) 그 밖에 데이터 국외이전의 안전에 영향을 미칠 수 있는 사항.

제 14 조 데이터 국외이전 안전평가 결과의 유효기간은 2 년으로 하며, 평가 결과가 나온 날부터 기산한다.

본 방법은 본 사건 신고의 법정 근거이다. 본 사건이 어느 사유(제 4 조의 몇 호)를 촉발하였는지는 공개자료에 명확히 밝혀져 있지 않다. 베이징우의병원은 핵심정보인프라 운영자 지위와 ‘100 만 명 이상 개인정보’ 규모 기준에 동시에 해당할 가능성이 있으나, 이는 외부 관찰에 의한 추론일 뿐 규제기관이 공개한 사실이 아니다.

본 사건의 평가 유효기간은 2 년이며 평가 결과가 나온 날부터 기산한다. 본 사건이 2022 년 9 월에 승인되고 2023 년 1 월에 공시된 점을 고려하면, 본 방법 제 14 조의 유효기간 규칙에 따라 평가의 유효기간은 늦어도 2024 년 9 월에 만료되며, 그 시점에 본 사건은 이미 재신고를 하였거나 유효기간 연장을 받았어야 한다. 그 연장 또는 재신고 상황은 공개 경로에 밝혀져 있지 않아 추가 확인이 필요하다.

라. 「데이터 국경 간 이동 촉진 및 규범화 규정」

본 규정은 데이터 국외이전 규제에 여러 정책적 조정을 가하였고, 자유무역시험구가 데이터 국외이전 네거티브리스트를 제정할 수 있도록 수권하였다(이는 2024 년 8 월 베이징 자유무역시험구 네거티브리스트의 정책적 수권 근거이다). 본 규정의 시행 시점(2024 년 3 월 22 일)에 본 사건의 원 심사는 이미 약 1 년 반 전에 통과되었으므로, 본 규정은 본 사건의 원 심사에 소급 적용되지 않는다. 다만 본 사건의 컴플라이언스가 2024 년 3 월 22 일 이후의 컴플라이언스 지속 단계에 들어선 뒤에는 본 규정이 본 사건에 적용되는 핵심 규범이 된다.

본 사건 관련 조문	관련성
제 2 조 데이터 처리자는 관련 규정에 따라 중요데이터를 식별·신고하여야 한다. 관련 부서·지역으로부터 중요데이터로 고지받거나 공개발표되지 아니한 경우, 데이터 처리자는 이를 중요데이터로 하여 데이터 국외이전 안전평가를 신고할 필요가 없다.	본 사건 심사 시(2022 년)에는 ‘중요데이터 관련 여부’의 판단이 불명확하였다. 본 조는 2024 년에, 주관부처가 사전에 고지하거나 공개적으로 공표하지 않는 한 중요데이터 신고 경로를 밟을 필요가 없음을 명확히 하였다. 본 사건의 컴플라이언스 지속 단계에는 본 조가 적용된다.
제 6 조 자유무역시험구는 국가 데이터 분류등급 보호제도의 틀 안에서, 구역 내에서 데이터 국외이전 안전평가, 개인정보 국외이전 표준계약, 개인정보보호 인증의 관리범위에 포함시킬 필요가 있는 데이터 목록(이하 ‘네거티브리스트’)을	본 조는 2024 년 8 월 베이징 자유무역시험구 네거티브리스트의 정책적 수권 근거이다. 베이징우의병원이 사업단위로서 베이징 자유무역시험구의 적용범위에 포섭되는지는 확인이 필요하다. 적용된다면 본 사건의 2024 년 8 월

본 사건 관련 조문

관련성

자체적으로 제정할 수 있으며, 성급 네트워크안전·정보화위원회의 기준을 거쳐 국가 인터넷정보 부서, 국가 데이터관리 부서에 비안한다.

자유무역시험구 내의 데이터 처리자가 네거티브리스트 외의 데이터를 국외에 제공하는 경우에는 데이터 국외이전 안전평가의 신고, 개인정보 국외이전 표준계약의 체결, 개인정보보호 인증의 통과를 면제받을 수 있다.

제 7 조 데이터 처리자가 국외에 데이터를 제공하는 경우로서 다음 중 하나의 요건에 해당하는 때에는 소재지 성급 인터넷정보 부서를 통하여 국가 인터넷정보 부서에 데이터 국외이전 안전평가를 신고하여야 한다. (1) 핵심정보인프라 운영자가 국외에 개인정보 또는 중요데이터를 제공하는 경우, (2) 핵심정보인프라 운영자 이외의 데이터 처리자가 국외에 중요데이터를 제공하거나, 당해 연도 1 월 1 일부터 누적하여 100 만 명 이상의 개인정보(민감개인정보 제외) 또는 1 만 명 이상의 민감개인정보를

이후의 컴플라이언스 지속은 본 조가 제공하는 간소화 경로의 혜택을 받을 수 있다.

본 조는 「데이터 국외이전 안전평가 방법」 제 4 조에 중요한 조정을 가하여, ‘100 만 명 이상 개인정보 처리자’ 기준을 ‘주체 요건’(국외이전량을 불문하고 병원의 총 처리규모 기준)에서 ‘당해 연도 1 월 1 일부터 누적하여 100 만 명 이상을 국외에 제공’(실제 국외이전량 기준)으로 변경하였다. 본 사건 심사 시(2022 년)에는 구(舊)기준이 적용되었고, 2024 년 3 월 이후의 갱신 신고에는 신(新)기준이 적용된다.

신규칙에 따르면, 관련 연구의 전 세계 규모 합계(합계 약 2,300 레)를 상한으로 추정하더라도 본 사건의 누적

본 사건 관련 조문	관련성
국외에 제공하는 경우.	국외이전량은 ‘누적 100 만 명 이상 개인정보’ 기준에 크게 미치지 못하고 ‘1 만 명 이상 민감개인정보’ 누적 기준에도 이르지 못하므로, 본 사건의 컴플라이언스 지속 단계에서 여전히 국외이전 안전평가가 촉발되는지는 신규칙에 따라 다시 판단할 필요가 있다.
제 8 조 핵심정보인프라 운영자 이외의 데이터 처리자가 당해 연도 1 월 1 일부터 누적하여 10 만 명 이상 100 만 명 미만의 개인정보(민감개인정보 제외) 또는 1 만 명 미만의 민감개인정보를 국외에 제공하는 경우에는 법에 따라 국외 수령자와 개인정보 국외이전 표준계약을 체결하거나 개인정보보호 인증을 통과하여야 한다.	본 사건의 컴플라이언스 지속 단계에서 실제 누적 국외이전량이 제 7 조의 안전평가 기준에 이르지 못하는 경우에는 본 조에 따라 표준계약 또는 인증 경로를 선택하여야 하며, 더 이상 국외이전 안전평가를 계속할 것이 아니다. 본 사건에서 누적 국외이전된 민감개인정보(전 세계 규모 합계 약 2,300 레를 상한으로 추정)는 바로 본 조의 ‘1 만 명 미만 민감개인정보’ 구간에 해당하므로, 규범 차원에서 본 사건의 컴플라이언스 지속 단계는 안전평가 경로에서 표준계약 또는 인증 경로로 하향 전환될 가능성이 있다.
제 9 조 데이터 국외이전 안전평가를 통과한 결과의 유효기간은 3 년으로	본 조는 본 사건의 컴플라이언스 지속과 직접 관련된다. 본 사건은

본 사건 관련 조문	관련성
하며, 평가 결과가 나온 날부터 기산한다. 유효기간이 만료되어 데이터 국외이전 활동을 계속할 필요가 있고 데이터 국외이전 안전평가를 다시 신고하여야 할 사유가 발생하지 아니한 경우, 데이터 처리자는 유효기간 만료 60 근무일 전까지 소재지 성급 인터넷정보 부서를 통하여 국가 인터넷정보 부서에 평가 결과 유효기간의 연장 신청을 제출할 수 있다. 국가 인터넷정보 부서의 비준을 거쳐 평가 결과의 유효기간을 3 년 연장할 수 있다.	2022 년 9 월에 2 년의 유효기간으로 승인되었으므로 본래 2024 년 9 월에 만료되어야 한다. 본 규정이 2024 년 3 월 22 일 시행된 후 평가 유효기간은 2 년에서 3 년으로 연장되었다. 다만 본 규정 시행 전에 이미 승인되어 당시 유효기간 내에 있던 기존 평가 결과에 대하여 유효기간을 당연히 3 년으로 다시 계산할 수 있는지는 규범 문언에 명시되어 있지 않다. 국가인터넷정보판공실의 기자문답도 “이미 데이터 국외이전 안전평가를 통과한 데이터 국외이전 활동은 데이터 처리자가 신고사항에 따라 계속 수행할 수 있다”고 확인하였을 뿐²⁸, 기존 결과의 유효기간 환산에는 미치지 않는다. 신규칙이 본 사건에 적용될 수 있다는 전제하에 2022 년 9 월의 승인 시점을 기준으로 추산하면 본 사건의 유효기간은 약 2025 년 9 월에 만료되며, 평가 결과가 나온 날이 공개되지 않았으므로 실제 만료 시점은 그만큼

²⁸국가인터넷정보판공실 관계자의 「데이터 국경 간 이동 촉진 및 규범화 규정」 기자문답, 2024 년 3 월 22 일, 中国网信网 게재. 그중 “이미 데이터 국외이전 안전평가를 통과한 데이터 국외이전 활동은 데이터 처리자가 신고사항에 따라 계속 수행할 수 있다”고 명시한다.

본 사건 관련 조문

관련성

늦추어질 수 있다. 이러한 기간 연장은
컴플라이언스 논리상의 추론이지
규제의 소급효에 대한 사실 인정이
아니다. 본 연구 작성 시점(2026 년
5 월)까지 어느 규칙에 의하더라도 본
사건의 유효기간은 이미 만료되었으며,
현재의 컴플라이언스 지속 상태(연장
신청 완료 / 재신고 완료 / 경로 변경
완료 / 미연장)는 공개자료에 밝혀져
있지 않다. 국가인터넷정보판공실과
베이징시 인터넷정보판공실의 공개
경로를 검색한 결과, 본 연구 작성
시점까지 본 사건에 관한 후속 공시는
확인되지 않았다.

제 10 조 데이터 처리자가 국외에 개인정보를 제공하는 경우에는 법률·행정법규의 규정에 따라 고지, 개인의 단독 동의 취득, 개인정보보호 영향평가의 실시 등의 의무를 이행하여야 한다.	본 조는 PIPL 제 39 조(고지 + 단독 동의)와 제 55 조(개인정보보호 영향평가)의 의무를 재확인하는 것으로, 본 사건 피험자 동의 단계의 컴플라이언스 요건에 대하여 지속적인 규범적 의의를 가진다.
---	---

마. 「인류유전자원관리조례 실시세칙」

본 세칙은 본 사건의 심사 통과 후 약 반년 뒤에 시행되었다. 본 사건의
심사 시점에 본 세칙은 아직 공포되지 않았다.

본 사건 관련 조문

제 2 조 우리나라 인류유전자원의 채집·보존·이용·국외제공은 본 실시세칙을 준수하여야 한다. 「조례」 제 2 조에서 말하는 인류유전자원 정보는 인류유전자원 재료를 이용하여 생성된 인류 유전자·게놈 데이터 등의 정보자료를 포함한다. 전항에서 말하는 인류유전자원 정보에는 임상데이터, 영상데이터, 단백질데이터와 대사데이터가 포함되지 아니한다.

제 2 조 제 3 항의 제외적 획정은 본 사건에 대하여 해석상의 의의를 가진다. COLOR III/IV 협약의 공개자료에 기술된 연구데이터는 주로 임상 표현형, 영상 평가, 병리 평가, 수술 후 추적관찰 등을 포함하는데, 본 항의 제외적 획정에 따르면 이들 데이터는 인류유전자원정보에 속하지 않으므로 본 사건은 인류유전자원관리조례 제 21 조의 과기부 심사 절차를 밟을 필요가 없을 개연성이 크다. 다만 이 제외적 획정은 본 사건의 심사 통과 이후에 비로소 부문규장의 형식으로 정식 확립된 것이며, 그 전의 2019 년 조례 자체의 인류유전자원정보 정의는 임상·영상·단백질·대사 데이터를 명시적으로 제외하지 않았다. 이는 본 사건 심사 시점(2022 년 9 월)에 ‘인류유전자원정보 해당 여부’의 판단이 규범 차원에서 일정한 불확실성을 안고 있었음을 의미하며, 병원 과학기술처의 ‘심층 평가’가 사실상 이 획정 기능을 담당한 것이다.

4. 지방성법규와 규범성 문건

가. 본 사건 심사 기간(2022~2023 년) 베이징시의 상황

본 사건의 심사 통과 시점(2023 년 초)까지 베이징시 차원에서 데이터 국외이전을 전문적으로 규율하는 지방성법규 또는 규범성 문건은 존재하지 않았다. 베이징시 인터넷정보판공실은 본 사건의 추진을 위하여 ‘전국 최초의 지방 신고수리 상담 전용창구’를 개통하였으나, 이는 행정서비스 조치이지

지방입법이 아니다.

나. 베이징 자유무역시험구 데이터 국외이전 관리

네거티브리스트(2024 년판)

이 리스트는 본 사건의 심사 통과 후 약 1 년 반 뒤에 발표되었다. 이 리스트는 전국 최초의 ‘시나리오화·필드 수준’ 데이터 국외이전 네거티브리스트로서, 1 차로 자동차, 의약, 소매, 민간항공, 인공지능의 5 개 분야를 포괄하고 23 개 업무 시나리오, 198 개 구체적 필드를 명시한다²⁹. 그중 의약산업 부분은 ‘의약데이터’를 명확히 정의한다. 즉 의약품 연구개발, 의약품 안전성 감시, 의약제조업 기업의 일상 생산·경영 등 과정에 관련되는 개인정보 데이터와 중요데이터가 이에 포함된다.

리스트는 다음 세 부류의 의약산업 데이터를 중요데이터로 열거한다. (i) 일정 규모 이상의 집단 진료, 건강·생리 상태, 의료구호 보장 데이터, 특정 의약품 실험 데이터 등, (ii) 일정 규모 이상의 특정 분야·특정 집단·특정 지역의 생체특징 데이터, 의료자원 데이터, (iii) 수출통제 또는 기술수출 관리사항에 포함되는 데이터.

이 리스트는 베이징 자유무역시험구 내에 등기·등록된 기업에 적용된다. 베이징우의병원이 사업단위로서 이 리스트의 적용범위에 포섭되는지는 확인이 필요하다. 이 리스트는 본 사건의 심사 통과 이후에 발표되었으나, 본 사건의 컴플라이언스 지속(평가 유효기간 만료 후의 갱신 신고)에 대하여 참조적 의의를 가진다. 2026 년 5 월 11 일 베이징시 인터넷정보판공실 등 3 개 부서는 나아가 ‘양구(两区)’ 데이터 국외이전 네거티브리스트(2025 년판) 및 부속 관리방법(시행)을 발표하여, 네거티브리스트 관리 메커니즘을 자유무역시험구에서 국가 서비스업 확대개방 종합시험구(즉 베이징시 전역)로

²⁹北京市互联网信息办公室等:《中国(北京)自由贸易试验区数据出境管理清单(负面清单)(2024 版)》, 2024 年 8 月 30 日.

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구 확대하고, 적용 분야를 5 개에서 9 개로 확대하였으며, 기존 의약 분야 리스트는 그대로 이관되었다.³⁰ 적용범위가 베이징시 전역으로 확대됨에 따라, 베이징시 역내에 소재한 베이징우의병원이 컴플라이언스 지속 단계에서 리스트의 적용범위에 포섭될 가능성은 현저히 높아졌다.

다. 「베이징시 디지털경제 촉진조례」

본 조례의 시행 시점은 본 사건의 공시 시점과 거의 겹친다.

본 사건 관련 조문	관련성
제 56 조 디지털경제 분야의 국제협력 확대를 장려하고, 국제규칙·표준·협정의 제정 참여를 지원하며, 국제 전시·포럼·통상·경기·연수 등 협력 플랫폼을 구축하고, 데이터의 국경 간 이동, 디지털서비스 시장 개방, 디지털제품 안전인증 등의 분야에서 호혜·상생과 협력·공영을 실현한다.	본 조는 산업정책의 방향을 제시하는 조문으로서 ‘데이터의 국경 간 이동’이 베이징시가 장려하는 국제협력 분야의 하나임을 긍정한다. 전국 최초의 데이터 컴플라이언스 국외이전 사례가 베이징에서 실현된 본 사건은 본 조가 구현하는 정책 방향과 일치한다. 다만 본 조가 본 사건의 구체적 컴플라이언스 의무의 근거를 구성하는 것은 아니다.

라. 「베이징시 의학윤리심사 상호인정연맹 업무규칙(2020 년판)」³¹ 및 2023 년 심화조치³²

³⁰ 北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局：《关于印发中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境负面清单（2025 版）及管理暂行办法的通知》，2026 年 5 月 11 日发布，载首都之窗（www.beijing.gov.cn）。

³¹ 《北京市卫生健康委员会关于进一步加强医学伦理管理和审查能力建设的通知》，北京市卫健委，2020 年 11 月 27 日。<https://wjw.beijing.gov.cn> 참조.

³² 《北京市卫生健康委员会关于印发北京市深化医学伦理审查结果互认有关工作的若干措施的通知》，北京卫健委，2023 年 10 月 31 日。<https://wjw.beijing.gov.cn> 참조.

본 규칙은 본 사건의 심사 통과 2 년여 전에 발표·시행되었다. 본 사건의 심사 시점에 본 규칙은 이미 안정적으로 운영되고 있었다.

2020 년 12 월 1 일 베이징시 보건위생위원회의 제창에 따라 베이징 지역 의료보건기관들이 발기하여 ‘베이징시 의학윤리심사 상호인정연맹’(이하 ‘상호인정연맹’)을 결성하였고, 같은 날 「베이징시 의학윤리심사 상호인정연맹 업무규칙(2020 년판)」을 내놓았다. 상호인정연맹 업무규칙 제 4 조에 따르면, 동일한 연구계획에 따라 둘 이상의 연맹 회원기관에서 다기관 임상연구를 수행하는 경우 연맹 회원기관은 본 규칙에 따라 윤리심사를 상호인정하며, 다기관 임상연구에는 의약품·의료기기 임상시험과 연구자 주도 임상연구가 포함된다.

베이징우의병원은 상호인정연맹의 회원기관 중 하나이다(베이징우의병원 공식 홈페이지의 연맹 업무규칙 공개 게재에 따르면 동 병원은 상호인정 메커니즘에 편입되어 있다). 본 사건의 COLOR III/IV 는 국제 다기관 임상연구이므로, 베이징우의병원의 중국 국내 협력기관이 역시 상호인정연맹의 회원이라면 국내 구간의 윤리심사에 상호인정 메커니즘을 적용할 수 있다.

본 사건과의 관련성: 상호인정연맹 업무규칙은 국내 다기관 연구의 윤리심사 상호인정만을 규율할 뿐 국경 간 데이터 국외이전의 윤리심사에는 미치지 않는다. 즉 본 사건이 국내 구간에서 상호인정 메커니즘을 적용하더라도, 국외에 데이터를 제공하는 것과 관련된 윤리심사는 여전히 베이징우의병원 자체 윤리위원회가 독립적으로 수행하여야 한다. 상호인정연맹 업무규칙과 본 사건의 데이터 국외이전 컴플라이언스 사이에는 ‘국내 구간 간소화, 국외이전 구간 독립’이라는 병행관계가 성립한다. 본 사건에서 상호인정 메커니즘이 실제로 가동되었는지, 가동되었다면 상호인정의 범위와 국경 간 데이터 국외이전 구간이 어떻게 구분되었는지는 공개 경로에 밝혀져 있지 않다. 지적하여 둘 것은, 이러한 구분은 상호인정 규칙의 문언이 국경 간 시나리오에

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구
대하여 아무런 언급을 하지 않은 데에서 비롯한 것으로, 규범이 미치지 않은
것이지 명문으로 배제한 것이 아니라는 점이다. 국경 간 다기관 연구의 경우
국내 구간의 윤리 간소화가 국외이전 구간으로 당연히 전이되는 것은 아니므로,
양자는 별도로 설계되어야 한다.

2023년 10월 31일 베이징시 보건위생위원회는 「베이징시 의학윤리심사 결과
상호인정 심화에 관한 약간의 조치 인쇄·발포에 관한 통지」를 발표하여, 2020년
업무규칙을 기초로 다기관 임상연구 윤리심사의 질적 제고와 효율화를 한층
추진하였다. 이 조치는 본 사건의 심사 통과 후 약 9개월 뒤에 발표되어 본
사건의 최초 심사에는 직접적인 영향이 없으나, 본 사건의 컴플라이언스 지속
단계에서 관련될 수 있는 국내 다기관 구간의 윤리심사에 대하여 규범적
의의를 가진다.

본 장에서 위계에 따라 정리한 각 규범은 본 사건에 적용되는 규범 좌표계를
구성한다. 그중 본 사건과 가장 직접 관련되는 데이터 분류등급 보호제도(그
기술표준 체계 포함)와 네트워크안전등급보호제도는 각각 제 4장과 제 5장에서
구체적으로 전개한다.

IV. 데이터 분류등급 보호제도의 본 사건에서의 적용과 전개

데이터 분류등급은 중국 데이터 거버넌스 체계의 기초적 제도이자 본 사건
데이터 국외이전 컴플라이언스 사슬의 출발점이다. 국외이전 경로의 선택,
안전평가의 촉발 여부, 보호조치의 강도는 모두 데이터가 어떤 범주로
식별되고 어떤 등급으로 판정되는지를 전제로 한다. 평가의 구조에서 본 장이
대응하는 것은 평가사항 중 국외이전 데이터의 종류·규모·민감정도에 대한
심사 차원이다. 본 장의 전개 순서는 다음과 같다. 먼저 이 제도의 규범적
기초와 본 사건 심사 시점의 분류등급 프레임워크를 제시하고, 이어서 병원
내부 3단계라는 관찰 가능한 사실을 복원한다. 그 위에서 GB/T 43697-2024 와

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

관련 기술표준을 진화 이후의 규범 참조계로 도입하여 그 방법에 따라 본 사건 데이터를 단계별로 식별하고, 나아가 심사 후 신설된 규칙 아래에서 컴플라이언스 지속 단계의 재정성(再定性)을 다루며, 분류등급과 등급보호의 연계로써 다음 장으로 넘어간 뒤 마지막으로 본 장을 소결한다. 구체적 식별 결과와 관련하여 공개자료에 밝혀지지 않은 것은 모두 추론으로 표기하며 본 연구의 사실적 결론을 구성하지 않는다.

1. 데이터 분류등급 보호제도의 규범적 기초

데이터 분류등급 보호제도가 중국 데이터 거버넌스 체계에서 가지는 규범적 기초는 법률·행정법규·부문규장·국가표준의 네 층위를 관통한다.

법률 차원에서 「데이터안전법」 제 21 조는 국가가 데이터 분류등급 보호제도를 수립하여, 데이터가 경제·사회 발전에서 가지는 중요도와 그것이 변조·파괴·유출되거나 불법으로 취득·이용될 경우 국가안전, 공공이익 또는 개인·조직의 적법한 권익에 초래할 위해의 정도에 따라 데이터를 분류등급하여 보호하도록 규정하고, ‘국가핵심데이터·중요데이터·일반데이터’의 3 등급 분급 프레임워크를 확립하였다.³³ 「개인정보보호법」 제 28 조는 개인정보의 차원 안에서 일반개인정보와 민감개인정보를 더 구분하고 ‘민감개인정보’를 열거적으로 확정하는데, 그중 ‘의료건강’과 ‘생체인식’의 두 부류가 본 사건과 가장 관련된다. 두 규범은 각각 ‘데이터’와 ‘개인정보’라는 두 차원에서 본 사건 분류등급 판단의 법률 층위 기초를 구성한다.

행정법규 차원에서 「인류유전자원관리조례」는 인류유전자원 재료와 인류유전자원 정보에 대하여 개인정보 체계와는 독립적인 분류관리를 정한다. 2023 년 7 월 1 일 시행된 「인류유전자원관리조례 실시세칙」 제 2 조 제 3 항은 나아가 인류유전자원정보를 제외적으로 확정하여 임상데이터, 영상데이터, 단백질데이터와 대사데이터가 인류유전자원정보에 속하지 않음을 명확히

³³洪延青：《国家安全视野中的数据分类分级保护》，载《中国法律评论》2021年第5期 참조.

하였다. 이 제외적 획정은 본 사건의 분류 판단에 직접적인 의의를 가진다.

부문규장 차원에서, 국가보건위생위원회·국가중의약관리국·국가질병예방통제국이 2022 년 8 월 29 일 공동으로 인쇄·발포한 「의료보건기관 네트워크안전 관리방법」 제 20 조는 의료보건기관이 매년 데이터 자산을 전면적으로 정리하고, 네트워크안전등급보호제도의 이행을 기초로 데이터의 중요도와 파괴 시의 위해 정도에 따라 해당 기관의 데이터 분류등급 기준을 수립하도록 명확히 요구한다. 동 방법의 시행 시점은 본 사건 데이터 국외이전 신고 개시 시점(2022 년 9 월 1 일)과 거의 겹치며, 이는 본 사건의 신고 개시 시점에 의료기관의 데이터 분류등급 의무가 막 행정규범으로 구체화되었음을 의미한다.

국가표준 차원에서, 통용 방법론은 GB/T 43697-2024 「데이터안전기술 데이터 분류등급 규칙」(2024 년 10 월 1 일 시행)이 확립하고, 의료업종의 세부화는 GB/T 39725-2020 「정보안전기술 건강의료데이터 안전지침」(2021 년 7 월 1 일 시행)이 제공하며, 개인정보 차원의 통용 표준은 GB/T 35273-2020 「정보안전기술 개인정보 안전규범」(2020 년 10 월 1 일 시행)이다. 세 층위의 표준은 시간적으로 앞뒤로 연결된다. 본 사건의 심사 시(2022~2023 년)에는 뒤의 둘이 적용되었고, 본 사건의 컴플라이언스 지속 단계(2024 년 10 월 이후)에는 GB/T 43697-2024 가 추가로 적용된다.

2. 본 사건 심사 시점에 적용된 분류등급 프레임워크

본 사건의 심사는 2022 년 9 월부터 2023 년 초 사이에 완료되었다. 심사 시점에 적용된 분류등급 프레임워크는 법률 층위, 업종규장 층위, 국가표준 층위의 세 층으로 구성되며, 세 층은 본 사건의 구체적 식별에서 중첩적용 관계를 형성한다.

법률 층위의 프레임워크에서 보면, PIPL 제 28 조와 「데이터안전법」 제 21 조가 두 차원에서 본 사건 데이터를 식별한다. 개인정보 차원에서, 본 사건이 관련된 환자 성명·입원번호·연락처 등은 일반개인정보에 속하고, 주민신분증번호는 PIPL 제 28 조에 열거된 ‘특정신분’ 및 신분증번호에 대한 국가표준의 특별취급 규칙에 따라 민감개인정보에 속하며, 진료기록·검사·영상·수술 후 추적관찰 등의 데이터는 ‘의료건강’류 민감개인정보에 속한다. 학계의 통설은 ‘민감개인정보’의 식별은 ‘인격존엄의 침해 또는 신체·재산 안전의 위해를 초래할 수 있는지’를 실질적 판단기준으로 하여야 한다고 보며, 의료건강정보는 개인의 신체상태, 생명상태, 질병이력 등 깊은 사적 영역을 직접 반영하므로 민감개인정보의 전형적 유형을 구성한다.³⁴

데이터 차원에서, 개별 환자의 임상데이터는 일반데이터에 속한다. 대규모·다기관·국경 간 전송되는 임상데이터가 ‘중요데이터’를 구성하는지는 본 사건 심사 시점에 규범 차원에서 명확하지 않았다. ‘중요데이터’ 식별의 구체적 업종기준은 2024 년 8 월 베이징 자유무역시험구 네거티브리스트가 나온 뒤에야 체계화되었다.

업종규장 층위의 프레임워크에서 보면, 본 사건의 데이터 국외이전 신고 개시 시점에 「의료보건기관 네트워크안전 관리방법」이 막 시행되었다(2022 년 8 월 29 일). 동 방법 제 20 조는 의료보건기관이 매년 데이터 자산을 전면적으로 정리하고 자체 데이터 분류등급 기준을 수립하도록 요구한다. 베이징시 보건위생위원회 공식 홈페이지가 공개한 본 사건 정보에 따르면, 베이징우의병원은 본 사건 심사 과정에서 내부 「데이터 국외이전

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구
안전관리방법」을 제정하였고, 동 방법은 “중요데이터 국외이전의 심사
메커니즘, 평가 메커니즘, 감독 메커니즘”의 수립을 명확히 하였다. 이 병원
내부 방법의 제정은 사실 차원에서 병원 단위의 데이터 분류등급 내부 식별
프레임워크 구축을 완성한 것이다.

국가표준 층위의 프레임워크에서 보면, 본 사건 심사 시점에는 GB/T 39725-
2020 이 적용되어 건강의료데이터의 6 대 분류(개인속성데이터, 건강상태데이터,
의료응용데이터, 의료지불데이터, 위생자원데이터, 공공위생데이터)와 5 등급
민감도 구분(1 급~5 급)에 따라 구체적 식별이 이루어졌다. 제 2 장 제 5 절에서
확인한 데이터 필드 범위에 따르면, 본 사건 데이터는 주로 대분류 (1)
개인속성데이터, (2) 건강상태데이터, (3) 의료응용데이터에 해당하고, 5 등급
민감도 구분상 주로 4 급(비교적 높은 민감도)에 해당하며, 주민신분증번호도
민감개인정보 규범에 따라 4 급에 속한다. 본 사건에는 5 급(최고 민감도)
데이터가 관련되지 않는데, COLOR III 와 COLOR IV 협약의 공개내용 모두
유전자 데이터, 생체인식 데이터의 수집을 언급하지 않기 때문이다.

3. 본 사건 분류등급 판정의 관찰 가능한 사실: 병원 내부 3 단계

베이징시 보건위생위원회 공식 홈페이지가 공개한 본 사건 정보에 따르면,
본 사건의 분류등급 판정은 병원 내부의 세 단계를 통하여 사실상
완성되었다.³⁵

제 1 단계는 병원 과학기술처에 의한 인류유전자원의 식별이다. 과학기술처는
프로젝트의 “그간의 수행 상황, 과학적 의의와 산출 가치, 인류유전자원 등

³⁵ 본 사건 병원 내부 3 단계의 사실은
北京市卫生健康委员会：《全国首个获批数据出境安全评估案例落地北京友谊医院》，2023 年 2 月 2
日，https://wjw.beijing.gov.cn/xwzx_20031/jcdt/202302/t20230202_2910980.html 의 공개내용에 따라
정리한 것이다. 이하 같다.

측면의 상황을 심층 평가”하였는데, 그 실질적 기능은 본 사건이 인류유전자원과 관련되는지를 판단하는 것이다. COLOR III·COLOR IV 협약의 공개내용에 유전자 데이터 수집이 언급되지 않은 사실에, 그 후 2023 년 7 월 1 일 시행된 「인류유전자원관리조례 실시세칙」 제 2 조 제 3 항의 제외적 획정을 결합하면 평가 결론은 ‘관련되지 않음’이었을 것이다. 다만 지적할 점은, 본 사건 심사 시(2022 년 9 월)에는 이 제외적 획정이 아직 부문규장으로 정식 확립되지 않았고 2019 년 「인류유전자원관리조례」 자체의 인류유전자원정보 정의도 임상데이터·영상데이터 등을 명시적으로 제외하지 않았다는 것이다. 이는 병원 과학기술처의 ‘심층 평가’가 규범이 불확실한 상황에서 분류 식별의 기능을 실제로 담당하였음을 의미한다.

제 2 단계는 병원 정보센터에 의한 네트워크안전 보호능력의 식별이다. 정보센터는 “네트워크안전·데이터안전을 다시 평가하여 병원의 네트워크안전 제도가 완비되고 실효성 있게 이행되며 안전방어 기술능력이 등급보호 등 표준규범에 부합함을 확인”하였는데, 그 실질적 기능은 병원의 네트워크안전등급보호 등급과 네트워크안전 능력이 본 사건 데이터 국외이전이 요구하는 보호수준에 부합함을 확인하는 것이다. 이 단계의 규범적 기초는 본 사건의 네트워크안전등급보호제도 적용과 연계되며, 제 5 장에서 상술한다.

제 3 단계는 병원에 의한 내부 「데이터 국외이전 안전관리방법」의 제정이다. 동 방법은 “중요데이터 국외이전의 심사 메커니즘, 평가 메커니즘, 감독 메커니즘”을 수립하여, 사실 차원에서 병원 단위의 중요데이터 식별 메커니즘 구축을 완성하였다. 다만 그 구체적인 식별 기준과 식별 결과는 공개자료에 밝혀져 있지 않다.

4. GB/T 43697-2024 「데이터안전기술 데이터 분류등급 규칙」의 체계적 해석

미리 밝혀 둘 것은, 본 절이 GB/T 43697-2024 를 도입하는 것은 2022 년

심사의 당부를 평가하기 위함이 아니라는 점이다. 본 사건 심사 시에는 동 표준이 아직 나오지 않았고, 당시 의료데이터 분급의 주된 기술적 근거는 GB/T 39725-2020 이었다. 본 절은 동 표준을 진화 이후의 규범 참조계로 삼아, 본 사건이 컴플라이언스 지속 단계에서 직면할 수 있는 재정성을 추론하기 위한 것이다.

국가표준 차원에서, 통용 방법론은 GB/T 43697-2024 「데이터안전기술 데이터 분류등급 규칙」(2024 년 10 월 1 일 시행)이 확립하고, 의료업종의 세부화는 GB/T 39725-2020 「정보안전기술 건강의료데이터 안전지침」(2021 년 7 월 1 일 시행)이 제공하며, 개인정보 차원의 통용 표준은 GB/T 35273-2020 「정보안전기술 개인정보 안전규범」(2020 년 10 월 1 일 시행)이고, 개인정보보호 영향평가의 기술지침은 GB/T 39335-2020 「정보안전기술 개인정보 안전영향평가 지침」(2021 년 6 월 1 일 시행)이 제공한다. 네 표준은 시간적으로 앞뒤로 연결된다. 본 사건의 심사 시(2022~2023 년)에는 뒤의 셋이 적용되었고, 컴플라이언스 지속 단계(2024 년 10 월 이후)에는 GB/T 43697-2024 가 추가로 적용된다.

국가표준	기능적 위상	시행일	심사 시점	컴플라이언스 지속
			(2022.9.~2023. 초)	단계 (2024.9. 이후)
GB/T 43697-2024 데이터 분류등급 규칙	통용 분류등급 방법론(산업영역+업무속성 분류, 3 등급 분급, 중요데이터 식별)	2024-10-01	미시행, 적용되지 않음	적용, 재신고/평가 연장의 분류등급 근거
GB/T 39725-2020 건강의료데이터 안전지침	의료업종 세부화(6 대 분류, 5 등급 민감도, 전생애주기 안전요구)	2020-11-19	적용, 심사 시의 주된 기술적 근거	계속 적용, 43697 과 연계
GB/T 35273-2020 개인정보 안전규범	개인정보 차원 통용 표준(개인민감정보 획정, PIPL 제 28 조와 상호 확인)	2020-10-01	적용	계속 적용
GB/T 39335-2020 개인정보 안전영향평가 지침	PIPL 제 55 조 영향평가의 기술지침	2021-06-01	적용(실시되었 을 것이나 문서 미공개)	계속 적용

GB/T 43697-2024(이하 본 절에서 「규칙」)는 전국네트워크안전표준화기술위원회가 명칭 변경 후 발표한 최초의 ‘데이터안전기술’ 명칭 국가표준으로서, 이후 각 업종·각 지역 데이터 분류등급 업무의 통용 방법론을 확립하였고, 본 사건 분류등급 판단을 이해하는 방법론적 모체를 구성한다. 「규칙」은 본 사건의 심사 이후에 비로소 시행되었으나, 본 사건 컴플라이언스 지속 단계의 재신고 또는 평가 연장은 이를 근거로 하여야 하므로 본 사건에 대하여 전망적인 규범적 의의를 가진다. 본 절은 「규칙」 본문 조항과 그 규범성 부록을 근거로 핵심 정의 부분에서는 원문을 짧게 인용하고 조항을 표기하며, 나머지는 분석적 서술로 제시한다.

가. 제정 배경, 법적 근거와 문서의 위상

「규칙」은 국가시장감독관리총국·국가표준화관리위원회가 2024 년 3 월 15 일 발표하고 2024 년 10 월 1 일 시행하였으며, 표준번호는 GB/T 43697-2024, 소관기관은 전국네트워크안전표준화기술위원회이다.³⁶ 일부 업계 해설 기사는 발표일을 2024 년 3 월 21 일로 기재하나, 이는 네트워크안전표준위가 대외 공고한 날로서 국가표준 전문공개시스템에 기재된 발표일(3 월 15 일)과 다르며, 본 연구는 국가표준 전문공개시스템에 기재된 일자를 기준으로 한다.

법적 근거의 측면에서 「규칙」은 「데이터안전법」 제 21 조의 ‘국가는 데이터 분류등급 보호제도를 수립한다’는 요구를 직접 이행하여, 동 조의 제도 선언을 조작 가능하고 점검 가능한 기술적 과정으로 전환한다. 「규칙」이 나오기 전 「네트워크안전법」과 「데이터안전법」은 중요데이터·핵심데이터의 개념을 확립하였으나 그 식별에 관한 통일된 기술적 기준을 제시하지 않아 ‘중요데이터’는 장기간 ‘개념은 섰으되 기준은 미정’인 상태에 놓여 있었다.

³⁶ 국가표준 전문공개시스템: GB/T 43697-2024《数据安全技术 数据分类分级规则》, 표준번호 GB/T 43697-2024, 발표일 2024-03-15, 시행일 2024-10-01, 소관기관 전국네트워크안전표준화기술위원회.

「규칙」의 의의는 바로 원칙에서 조작으로 가는 이 공백을 메우는 데 있다.³⁷

문서의 연혁 측면에서 「규칙」은 무에서 창설된 것이 아니라 두 건의 선행 의견수렴안을 병합·흡수한 것이다. 하나는 네트워크안전표준위가 2022 년 9 월 14 일 발표한 「정보안전기술 네트워크데이터 분류등급 요구(의견수렴안)」이고, 다른 하나는 「정보안전기술 중요데이터 식별규칙(의견수렴안)」이다. 「규칙」은 본문 부분에서 전자의 분류등급 원칙·프레임워크·방법에 관한 내용을 기본적으로 이어받는 동시에 후자의 ‘중요데이터 식별지침’을 규범성 부록 G로 편입하여, 데이터 분류등급·중요데이터 식별·국가핵심데이터 식별을 아우르는 완결적 체계를 형성하였다. 이 연혁을 정리하는 것은 본 사건 심사 시(2022~2023 년)의 규범상태를 이해하는 데 도움이 된다. 당시 위 내용은 의견수렴안 단계에 머물러 정식 국가표준으로 승격되지 않았으며, 이것이 바로 본 사건의 ‘규범 미완성 — 사실 선행’ 특징의 표준 층위에서의 원인이다.

나. 적용범위와 기본원칙

「규칙」 제 1 장은 적용범위를 확정하고 제 4 장은 다섯 가지 기본원칙을 확립한다.

표준 원문(제 1 장, 제 4 장)	해석과 본 사건에의 적용
제 1 장 범위: 본 문서는 데이터 분류등급의 원칙·프레임워크·방법과 절차를 규정하고 중요데이터 식별지침을 제시한다. 본 문서는 산업영역 주관(감독)부서가 해당 업종·분야의 데이터 분류등급 표준규범을 제정할 때 참고하는 데	「규칙」은 세 부류의 적용주체 — 산업 주관부서, 각 지역·각 부서, 데이터 처리자 — 를 설정한다. 베이징우의병원은 세 번째 부류인 ‘데이터 처리자’에 속한다. 보건위생 산업 주관부서가 업종 세칙을 발표하기 전에는 처리자가 「규칙」을 참조하여

³⁷ 중요데이터 식별이 장기간 미해결 상태에 있던 문제에 대한 분석으로는 洪延青:《国家安全视野中的数据分类分级保护》, 载《中国法律评论》2021 年第 5 期 참조.

표준 원문(제 1 장, 제 4 장)	해석과 본 사건에의 적용
적용되고, 각 지역·각 부서가 데이터 분류등급을 먼저 수행하고, 업종 목록 분류등급 업무를 수행하는 데에도 또는 식별규범이 발표된 후에 다시 적용되며, 아울러 데이터 처리자의 연계할 수 있다. 본 사건 데이터는 데이터 분류등급에 참고를 제공한다. 국가비밀·군사데이터와 무관하므로 본 문서는 국가비밀에 관련되는 제외범위에 속하지 않는다. 데이터와 군사데이터에는 적용되지 아니한다.	
4 기본원칙 a) 과학·실용 원칙: 데이터의 관리·사용에 편리한	다섯 원칙 중 c) 상향 엄격적용과 d) 점·면 결합이 본 사건에 결정적 의의를
관점에서 흔하고 안정적인 속성 또는 특징을 데이터 분류의 근거로 과학적으로 선택하고, 실제 필요에 맞추어 데이터를 세분화한다. b) 경계	점·면 결합이 본 사건에 결정적 의의를 가진다. 상향 엄격적용은, 본 사건 데이터의 어느 한 요소(예컨대 집단 규모)만 중요데이터 기준에 도달하여도 중요데이터로 등급이 결정됨을 의미한다.
명확 원칙: 데이터 등급의 각 등급 경계를 명확히 하고, 서로 다른 등급의 데이터에 상응하는 보호조치를 진료기록은 일반데이터일 수 있으나	점·면 결합은 본 사건의 다기관 데이터 집적 상황을 직접 겨냥한다. 개별
취한다. c) 상향 엄격적용(就高从严) 원칙: 높은 쪽을 따르고 낮은 쪽을 따르지 않는 원칙으로 데이터 등급을 결정하여야 하며, 이것이 바로 본 사건의	다기관 집적·융합 후에는 안전 영향을
영향을 미칠 수 있는 경우에는 각 데이터와 구별되는 규범적 근거이다. e) 영향대상에 미칠 수 있는 최고의 영향동태 갱신 원칙은 본 사건의 COLOR	다시 평가하여 종합적으로 등급을
정도에 따라 데이터 등급을 확정한다. IV 가 2030 년까지 지속되는 반면 평가	확정하며, 여러 요소가 데이터 등급에 ‘집단 진료 규모 데이터’가 개별
d) 점·면 결합(点面结合) 원칙: 데이터 유효기간은 2~3 년에 불과하다는	영향을 미칠 수 있는 경우

표준 원문(제 1 장, 제 4 장)

해석과 본 사건에의 적용

분급은 개별 데이터의 분급을 장기성에 대응하여, 업무와 규모의 고려하는 동시에 여러 분야·집단 또는 변화에 따라 등급을 심사·갱신할 것을 지역의 데이터가 집적·융합된 후의 요구한다.

안전 영향을 충분히 고려하여 데이터

등급을 종합적으로 확정한다. e) 동태

갱신 원칙: 데이터의 업무속성,

중요도와 초래할 수 있는 위해 정도의

변화에 따라 데이터 분류등급,

중요데이터 목록 등을 정기적으로

심사·갱신한다.

다. 용어체계: 핵심데이터, 중요데이터, 일반데이터와 공공데이터,

파생데이터

「규칙」 제 3 장이 획정하는 용어 중 3 등급 데이터의 정의가 분급의 논리적 출발점을 구성한다.

표준 원문(제 3 장 용어와 정의)

해석과 본 사건에의 적용

3.2 중요데이터: 특정 분야, 특정 집단, 특정 지역의 것이거나 일정한 정밀도와 규모에 도달'이 본 사건 집단 정밀도와 규모에 달한 것으로서, 일단 진료데이터 등급 결정의 핵심 척도이며, 유출되거나 변조·훼손되면 국가안전, '공중의 건강과 안전'이 바로 본 사건 경제운영, 사회 안정, 공중의 건강과 안전을 직접 위해할 수 있는 데이터. 대상이다. '주'가 정한 '개인에게만 영향을 주: 조직 자체 또는 공민 개인에게만 영향을 미치는 데이터는 일반적으로 중요데이터로 하지 않는다'는 한정은

표준 원문(제 3 장 용어와 정의)	해석과 본 사건에의 적용
중요데이터로 하지 아니한다.	개별 환자의 임상데이터가 중요데이터를 구성하지 않는다고 판단하는 직접적 근거로서, 본 사건에 ‘개인 — 집단’의 층위별 판단 구조를 형성시킨다.
3.3 핵심데이터: 분야·집단·지역에 대하여 비교적 높은 포괄도를 가지거나 비교적 높은 정밀도, 비교적 핵심데이터는 ‘정치안전에 직접 영향’을 큰 규모, 일정한 심도에 달한 것으로서, 일단 불법으로 사용되거나 공유되면 정치안전에 직접 영향을 미칠 수 있는 중요데이터. 주: 핵심데이터는 주로 국가안전 중점 분야에 관련되는 데이터, 국민경제의 명맥·중요한 민생·중대한 공공이익에 관련되는 데이터, 국가 관련 부서의 평가로 확정된 그 밖의 데이터를 포함한다.	문턱으로 하므로 그 기준은 본 사건 의료데이터가 도달할 수 있는 범위를 훨씬 넘는다. 본 사건 데이터는 정치안전, 국민경제의 명맥과 무관하므로 핵심데이터의 적용을 배제할 수 있으며, 본 사건의 분류 판단은 ‘중요데이터/일반데이터’ 사이에 집중된다.
3.4 일반데이터: 핵심데이터, 중요데이터 이외의 그 밖의 데이터.	일반데이터는 보충적 범주이다. 본 사건에서 개인 차원의 임상데이터는 중요데이터의 문턱에 이르지 못하는 한 일반데이터로 귀속되며, 더 세분화할 필요가 있으면 자료성 부록 H를 참고할 수 있다.
3.8 공공데이터: 각급 정부부서,	베이징우의병원은 공립 의료기관으로서

표준 원문(제 3 장 용어와 정의)

해석과 본 사건에의 적용

공공관리·서비스 직능을 가진 조직과 그 기술지원 단위가 법에 따라 공공사무 관리직책을 이행하거나 공공서비스를 제공하는 과정에서 수집·생성한 데이터.

진료활동에서 생성한 데이터가 동시에 ‘공공데이터’로 식별되는지가 데이터 거버넌스 의무의 중첩에 영향을 미칠 수 있다. 본 사건의 공개자료는 이에 관하여 인정한 바 없으므로, 여기서는 그러한 식별 차원의 존재만을 지적하고 결론은 내리지 않는다.

3.10 파생데이터: 통계, 연계, 마이닝, 집계, 비식별화 등 가공활동을 거쳐 생성된 데이터.

본 사건 COLOR III 협약이 요구하는 중앙화 병리 재판독, 중앙화 MRI 재판독, 그리고 다기관 데이터 병합 후 형성되는 집단 차원의 통계 결과는 모두 파생데이터에 속한다. 그 분급은 §6.6 f)에 따라 원본 데이터 등급을 기초로 가공 후의 ‘심도’ 등 요소를 종합적으로 고려하여 확정하여야 하는데, 이 점은 심사 시점의 구(旧)프레임워크에서는 명확하지 않았다.

라. 분류규칙: 산업영역 우선, 업무속성 후속

「규칙」 제 5 장은 ‘먼저 산업영역으로 분류하고, 다음에 업무속성으로 분류한다’는 사고를 확립한다.

표준 원문(제 5 장 데이터 분류규칙)

해석과 본 사건에의 적용

5.1 데이터 분류 프레임워크: 데이터는 제 1 단계 산업영역 분류: 본 사건 먼저 산업영역으로 분류하고 다음에 데이터는 진료와 임상연구 활동에서

표준 원문(제 5 장 데이터 분류규칙)

해석과 본 사건에의 적용

업무속성으로 분류하는 사고에 따라 생성되었으므로 ‘보건의료데이터’에

분류한다. a) 산업영역에 따라 귀속된다. 제 2 단계 업무속성 분류: 아홉 데이터를 공업데이터, 전신데이터, 가지 업무속성 차원 중 본 사건은 금융데이터, 에너지데이터, ‘데이터 용도’(임상연구데이터와 의료서비스데이터의 구분), ‘기술 대상’ 교통운수데이터, 자연자원데이터, 등의 차원으로 세분화하기에 적합하다. 보건의료데이터, 교육데이터, 과학데이터 등으로 분류한다. b) 각 c)항의 ‘법령에 특별한 관리 요구가 있는 업종·각 분야 주관(감독)부서는 해당 데이터 범주’는 본 사건에서 업종·분야의 업무속성에 따라 해당 민감개인정보(PIPL 제 28 조)의 중첩 업종·분야의 데이터를 세분화하여 식별과 인류유전자원정보 배제 판단의 분류한다. 흔한 업무속성에는 기준 근거로서, 제 4 절의 제 3 단계에 업무영역, 책임부서, 기술(记述)대상, 대응한다.

절차 단계, 데이터 주체, 내용 주제,

데이터 용도, 데이터 처리, 데이터

출처 등이 포함되되 이에 한하지

아니한다. c) 법령에 특별한 관리

요구가 있는 데이터 범주(개인정보

등)가 관련되는 경우에는 관련 규정과

표준에 따라 식별·분류하여야 한다.

5.2 데이터 분류방법: a) 데이터 범위의이 4 단계 방법은 처리자 측의 분류 조작

명확화, b) 업무 분류의 세분화(부서별 경로이다. 본 사건은 이에 따라

직책 분담에 맞추어 업무 라인 분류를 ‘보건의료 — 임상연구 — COLOR III/IV

명확히 하고, — 중앙화 재판독 데이터/추적관찰

업무범위·운영모델·업무절차에 따라 데이터’ 등으로 단계별 표지를 부여할 수

표준 원문(제 5 장 데이터 분류규칙)

해석과 본 사건에의 적용

핵심업무 분류를 세분화), c) 업무속성 있다. 「규칙」은 처리자가 자신의 데이터 분류(적합한 업무속성을 선택하여 특성에 맞추어 업무속성을 유연하게 핵심업무의 데이터를 세분화하여 선택하도록 허용하므로, 본 사건의 2 차 분류), d) 분류규칙의 확정(‘업무 라인 분류에는 합리적인 탄력의 여지가 있다. — 핵심업무 — 업무속성 분류’의 방식으로 데이터 분류규칙을 제시할 수 있다).

마. 등급규칙: 3 등급 프레임워크, 등급 절차, 등급 요소와 영향 분석

「규칙」 제 6 장은 데이터 등급규칙을 확립한다.

표준 원문(제 6 장 데이터 분급규칙)

해석과 본 사건에의 적용

6.1 데이터 분급 프레임워크: 데이터가

경제·사회 발전에서 가지는 중요도와 그것이 일단 유출·변조·훼손되거나 불법으로 취득·사용·공유될 경우 국가안전, 경제운영, 사회질서, 공공이익, 조직권익, 개인권익에 초래하는 위해의 정도에 따라, 데이터를 높은 것부터 낮은 것까지 핵심데이터, 중요데이터, 일반데이터의 세 등급으로 나눈다.

6.2 데이터 분급방법: a) 분급대상의 확정(데이터 항목, 데이터셋, 파생데이터, 산업영역을 넘는 데이터 등. 주: 데이터 항목은 통상 데이터베이스 테이블의 한 열 필드로 나타나고, 데이터셋은 여러 데이터 레코드로 구성된 집합으로서 데이터베이스 테이블, 데이터베이스의 한 행 또는 여러 행의 레코드 집합, 데이터 파일 등이 그 예이다), b) 분급 요소의 식별, c) 데이터 영향 분석, d) 등급의 종합적 확정.

3 등급 분급의 판단구조는

‘중요도 + 위해 정도’이다. 본 사건 의료데이터의 위해 정도 판단은 ‘공공이익’, ‘공중의 건강과 안전’, ‘개인권익’의 세 영향대상 사이에 집중되며, 데이터가 개인 차원인지 집단 차원인지에 따라 달라진다.

a) 분급대상의 확정은 본 사건에서 건너뛴 수 없는 관건이다. 개별 환자의 임상데이터 항목(데이터셋 안의 필드/단건 레코드)과 다기관 집적된 집단 진료 데이터셋은 서로 다른 분급대상에 속하므로 각각 판단하여야 하며 서로 다른 등급에 이를 수 있다. 본 사건에 대한 제 4 절의 단계별 식별은 바로 이 4 단계를 엄격히 따라 전개된다.

표준 원문(제 6 장 데이터 분급규칙)

해석과 본 사건에의 적용

6.3 데이터 분급 요소: 데이터 분급에 영향을 미치는 요소에는 데이터의 분야, 집단, 지역, 정밀도, 규모, 심도, 포괄도, 중요성 등이 포함된다. 그중 분야, 집단, 지역, 중요성은 통상 정성적으로 기술되는 분급 요소이고, 정밀도, 규모, 포괄도는 정량적으로 기술되는 분급 요소이며, 심도는 통상 파생데이터의 분급 요소가 된다.

6.4.1 영향대상: 통상 국가안전, 경제운영, 사회질서, 공공이익, 조직권익, 개인권익을 포함한다. 그중 공공이익이란 사회 공중의 공공서비스·공공시설·공공자원 이용에 영향을 미치거나 공중의 건강·안전 등에 영향을 미치는 공공이익을 말하고, 개인권익이란 자연인의 인신권, 재산권, 프라이버시권, 개인정보 권익 등 개인의 권익에 영향을 미치는 것을 말한다.

본 사건의 집단 진료 데이터셋에

관련되는 요소는 다음과 같다.

집단(결장·직장암 환자라는 특정 질환 집단), 규모(COLOR IV 계획상 1,158 레 등록이며 전 세계 다기관 합계 규모), 포괄도(30~50 개 기관, 다기관·복수 지역), 심도(중앙화 통계 재판독으로 형성되는 파생데이터).

이들 요소의 중첩이 그것이

중요데이터의 문턱에 도달한다고

추론하는 사실적 기초이다.

본 사건의 영향대상 판단은

‘개인권익’과 ‘공공이익/공중의 건강·안전’ 사이에서 층위가 나뉜다.

단건 임상데이터의 유출은 주로

개인권익(프라이버시권, 개인정보

권익)에 영향을 미치고, 집단

진료데이터는 공중의 건강과 안전에

영향을 미칠 수 있어 영향대상의

층위가 위로 이동한다.

표준 원문(제 6 장 데이터 분급규칙)

해석과 본 사건에의 적용

6.4.2 영향 정도: 높은 것부터 낮은 것까지

특히 중대한 위해, 중대한 위해, 일반적 위해로 나뉜다. 영향대상이 국가안전, 경제운영, 사회질서 또는 공공이익인 경우에는 국가·사회 또는 업종·분야의 전체 이익을 판단기준으로 하고, 조직 또는 개인의 권익에 불과한 경우에는 조직 또는 공민 개인의 권익을 판단기준으로 한다. 영향대상이 개인 또는 조직의 권익인 경우, 대규모의 개인 또는 조직의 권익에 영향을 미친다면 국가안전, 경제운영, 사회질서 또는 공공이익에 영향을 미치는지 여부와 그 영향 정도를 함께 검토하여야 한다.

끝 문장은 본 사건에 극히 중요하다. 개인정보의 ‘대규모로’ 영향을 받는 경우에는 공공이익에 대한 영향으로 상승하는지를 추가로 검토하여야 한다. 본 사건의 다기관·대규모 환자데이터 집적은 바로 ‘대규모 개인정보’의 상황에 해당하므로 이 규칙에 따라 공공이익의 층위에서 검토되어야 하며, 이로써 집단 데이터의 등급 상향 이동이라는 추론이 뒷받침된다.

표준 원문(제 6 장 데이터 분급규칙)

해석과 본 사건에의 적용

6.5 등급 확정규칙 b)(중요데이터): 다음

중 어느 하나의 조건을 충족하면

중요데이터로 식별한다. 1) 데이터가 일단

유출·변조·훼손되거나 불법으로

취득·사용·공유되면 국가안전에 일반적
위해를 직접 초래하는 경우, 2) 경제운영에

중대한 위해를 직접 초래하는 경우, 3)

사회질서에 중대한 위해를 직접 초래하는

경우(사회 안정에 영향 등), 4) 공공이익에

중대한 위해를 직접 초래하는 경우(공중의

건강과 안전에 대한 위해 등), 5) 데이터가

국가안전, 경제운영, 사회 안정, 공중의

건강과 안전에 직접 관련되는 특정 분야,

특정 집단 또는 특정 지역의 것인 경우, 6)

데이터가 일정한 정밀도·규모·심도 또는

중요성에 달하여 국가안전, 경제운영,

사회 안정, 공중의 건강과 안전에 직접

영향을 미치는 경우, 7) 업종·분야

주관(감독)부서의 평가로 확정된

중요데이터.

b)4), 5), 6)의 세 항이 본 사건과 직접

대응한다. 본 사건의 집단

진료데이터는 ‘공중의 건강과

안전’에 관련되고 ‘특정

집단’(결장·직장암 환자)을 포함하며

‘일정한 규모에 도달’하여

중요데이터의 식별조건에 부합한다.

b)7)은 최종 인정 권한이 보건위생

산업 주관부서에 있음을 시사하며,

본 사건의 확정적 결론은 업종

목록이 마련되기를 기다려야 한다.

표준 원문(제 6 장 데이터 분급규칙)

해석과 본 사건에의 적용

6.6 등급의 종합적 확정: a) 6.5 에 따라 핵심데이터·중요데이터·일반데이터를 식별한다. b) 중요데이터의 식별은 6.5 b)에 부합하는 것을 기초로 부록 G 에 따라 집행하여야 한다. c) 여러 요소, 여러 영향대상 또는 영향 정도가 관련되는 경우에는 상향 엄격적용 원칙에 따라 등급을 확정한다. d) 데이터셋의 등급은 데이터 항목 등급을 기초로 상향 엄격적용 원칙에 따라 데이터셋에 포함된 데이터 항목의 최고 등급을 데이터셋의 기본 등급으로 할 수 있되, 분급 요소(데이터 규모 등)의 변화로 등급을 높일 필요가 있는지도 함께 고려하여야 한다. f) 파생데이터의 등급은 상향 엄격적용 원칙에 따라 원본 데이터 등급을 기초로 가공 후의 데이터 심도 등 분급 요소를 종합적으로 고려하여 확정할 수 있다.

b)항은 본문과 부록 G 를 연결하는 중추이다. 중요데이터의 식별은 6.5 b)의 조건을 충족하는 동시에 부록 G 에 따라 집행되어야 한다(다음 항에서 상술). d)항은 본 사건의 ‘데이터셋 상향’을 확인한다. 다기관 데이터셋의 등급은 그에 포함된 데이터 항목의 최고 등급을 취하며 규모 증대에 따라 더 높아질 수 있는데, 이것이 집단 데이터의 등급이 단건 데이터보다 높은 규범적 근거이다. f)항은 본 사건의 중앙화 재판독 등 파생데이터의 등급 결정에 경로를 제공한다.

바. 규범성 부록 G ‘중요데이터 식별지침’

부록 G 는 「규칙」의 유일한 규범성 부록으로서 그 효력은 본문과 동일하다. GB/T 1.1-2020 에 따르면 규범성 부록은 표준이 반드시 집행하여야 하는 기술요소로서, 참고용에 그치는 자료성 부록(부록 A~F, H~J)과 구별된다.

표준 원문(부록 G, 규범성)	해석과 본 사건에의 적용
부록 G 중요데이터 식별지침(서두 부분): 중요데이터의 식별은 6.5 b)에 부합하는 것을 기초로 다음의 요소를 고려하여야 한다. 위 요소 중 하나를 갖춘 데이터는 중요데이터로 식별될 수 있다.	부록 G의 식별 메커니즘은 ‘6.5 b)의 기초조건 + 부록 G의 열거 요소, 그중 하나를 갖추면 식별 가능’이다. 부록 G는 a)부터 q)까지 17개 요소를 열거하며 국토·군사, 경제운영, 문화, 핵심정보인프라, 과학기술, 수출통제, 생태자원, 핵 안전, 해외 이익, 생물안전, 금융산업, 공중보건 등의 차원을 포괄한다. 본 사건의 판단은 의료와 직접 관련되는 제 o)항에 집중된다. 제 o)항은 본 사건 등급 결정의 가장 직접적인 규범 근거이다. 본 사건 COLOR III/IV 연구의 다기관·집단 차원 결장·직장암 진료 및 추적관찰 데이터는 바로 ‘대량 인구의 진료와 건강관리’가 기술하는 범주에 해당한다(COLOR III·COLOR IV는 모두 외과 수술방식 비교 연구로서 ‘특정 의약품 실험’에는 속하지 않는다). 이에 따라 부록 G의 ‘하나를 갖추면 중요데이터로 식별 가능’ 규칙상, 본 사건의 집적된 집단 진료 규모 데이터는 방법론상 중요데이터의 실질적 특징을 갖춘다. 다만 그것이 최종적으로 중요데이터를 구성하는지는 여전히 주관부처의 고지 또는 목록·리스트의 공표를 기준으로 한다.
부록 G 제 o)항: 국가 또는 지역의 집단 건강·생리 상태를 반영하거나, 질병의 전파·방역과 관련되거나, 식품·의약품 안전과 관련되는 것으로서, 예컨대 건강의료자원, 대량 인구의 진료와 건강관리, 질병통제·방역, 건강구호 보장, 특정 의약품 실험, 식품안전 이력추적에 관련되는 데이터.	

표준 원문(부록 G, 규범성)

해석과 본 사건에의 적용

부록 G 제 n)항: 전국적 또는

중점 분야의 경제운영·금융활동
상황을 반영하거나, 산업경쟁력과
관련되거나, 공공안전 사고를
초래하거나 국민의 생명안전에
영향을 미칠 수 있거나, 집단적
활동을 유발하거나 집단의
감정·인식에 영향을 미칠 수 있는
것으로서, 예컨대 미공개
통계데이터, 중점기업의 영업비밀.

제 n)항은 주변부에서 의료 분야와
관련되나(‘국민의 생명안전에 영향을 미치는’
통계데이터 등), 본 사건과의 관련 정도는
제 o)항에 분명히 미치지 못하므로 본 사건은
이를 주된 근거로 하지 않는다. 대조를
위하여 열거한 것은 부록 G 요소들 사이의
경계를 보이기 위함일 뿐이다.

사. 데이터 분류등급 절차: 산업 측과 처리자 측

「규칙」 제 7 장은 산업영역 주관(감독)부서와 데이터 처리자라는 두 역할의
절차를 구분한다.

표준 원문(제 7 장 데이터 분류등급
절차)

해석과 본 사건에의 적용

7.1 산업영역 데이터 분류등급 절차: 산업 측 절차는 보건위생 주관부서의

a) 업종 표준규범의 제정(업종 직책에 대응한다. 본 연구 작성 시점까지
데이터 분류 세칙의 명확화; 분급 보건의료 업종의 중요데이터 식별 세칙은
요소를 분석하여 중요데이터 식별 순차적으로 제정되고 있으며, 이미
세칙을 명확히 하고 어떤 데이터가 단체표준 T/GDWJ 024-2024 「건강의료정보
중요데이터로 확정될 수 있는지 중요데이터 식별 및 관리지침」이 각
확정; 핵심데이터 식별 세칙의 기관에 중요데이터 목록의 작성을
명확화; 일반데이터 범위의 명확화), 요구하고 등급 확정은 GB/T 43697-2024

표준 원문(제 7 장 데이터 분류등급

해석과 본 사건에의 적용

절차)

b) 데이터 분류등급의 수행(해당 제 6.5 조를 참조할 수 있다고 규정한다. 본 업종·분야의 데이터 처리자를 사건 데이터의 최종 등급은 업종 조직하여 업무를 수행하고, 중요데이터 목록이 마련된 뒤에 중요데이터와 핵심데이터 목록 확정되어야 한다(6.5 b)7)과 호응). 정보를 정확히 식별하고 적시에 보고하도록 지도).

7.2 처리자 데이터 분류등급 절차: a) 처리자 측의 5 단계 방법(동태 갱신 데이터 자산 정리, b) 내부 규칙의 포함)은 베이징우의병원의 실제 업무에 제정, c) 데이터 분류의 대응한다. 병원은 과학기술처 평가와 실시(공공데이터, 개인정보 등 특수 정보센터 평가를 통하여 a) 자산 정리와 범주 데이터의 식별과 분류), d) 초보적 식별을 완성하였고, 내부 「데이터 데이터 등급의 실시(핵심데이터, 국외이전 안전관리방법」을 통하여 b) 내부 중요데이터와 일반데이터의 범위 규칙 제정과 d) 중요데이터 식별 메커니즘 확정), e) 목록의 심사·보고(데이터 구축을 완성하였다. 이는 처리자 측 분류등급 리스트, 절차가 의료 실무에 적용된 초기 표본을 중요데이터·핵심데이터 목록을 구성하나, e) 목록 보고와 f) 동태 갱신의 작성하여 절차에 따라 보고), f) 구체적 집행은 공개자료에 밝혀져 있지 동태적 갱신 관리. 않다.

위 여섯 개의 표를 종합하면, 「규칙」은 본 사건에 조작 가능한 분류등급 방법론 일습을 제공한다. 제 1 장 범위와 제 4 장 원칙으로 위상을 정하고, 제 3 장 용어에 따라 3 등급 프레임워크를 확정하며, 제 5 장에 따라 분류를, 제 6 장에 따라 등급을 완성하고, 중요데이터 식별에서는 제 6.6 b)가 규범성 부록 G 를

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

지시한다. 제 7 장의 양측 절차는 위 방법을 산업 주관부서와 처리자라는 두 주체에 배분하여 집행하게 한다. 그중 제 4 장의 ‘상향 엄격적용’, ‘점·면 결합’ 원칙, 제 6.4.2 조의 ‘대규모 개인정보의 공공이익 영향을 검토하여야 한다’는 규칙, 그리고 부록 G 제 o)항이 함께, 본 사건의 집단 진료 규모 데이터가 중요데이터로 식별되어야 한다는 규범적 사슬을 구성한다. 또한 제 6.6 d)의 ‘데이터셋 상향’과 f)의 ‘파생데이터 상향’은 집단 데이터셋의 등급이 그에 포함된 단건 데이터보다 높은 이유를 설명한다.

GB/T 43697-2024 가 제공하는 것은 업종을 가로지르는 통용 방법론이다. 밝혀 둘 것은, 동 표준은 권고성 국가표준에 속하고 그 부록 G 가 표준 문서 내에서는 규범성 부록이지만 당연히 행정법상의 강제적 효력을 가지는 것은 아니며, 본 사건에서 그 의의는 데이터 분류등급과 중요데이터 식별에 방법론적 참조를 제공하고 규제 신고 실무를 거쳐 사실상의 컴플라이언스 기준으로 전화되는 데 있다는 점이다. 본 사건의 구체적 적용에서는 의료업종의 세부화 표준과 개인정보 차원의 통용 표준이 추가로 중첩 적용되어야 한다.

5. 본 사건과 관련된 그 밖의 데이터안전 기술표준

GB/T 39725-2020 은 2020 년 12 월 14 일 발표되어 2021 년 7 월 1 일 시행되었으며, 본 사건 심사보다 1 년여 앞서 시행되어 본 사건 심사 시 의료데이터 분류등급의 주된 기술적 근거였다. 동 표준은 건강의료데이터를 6 대 분류와 5 등급 민감도로 구분하고, 데이터 전생애주기 각 단계에 기술적 안전통제 요건을 제시한다.

6 대 분류에서 동 표준은 건강의료데이터를 개인속성데이터, 건강상태데이터, 의료응용데이터, 의료지불데이터, 위생자원데이터, 공공위생데이터로 나눈다.

5 등급 민감도 구분에서는 낮은 것부터 높은 것까지 1 급에서 5 급으로 나누며, 각 등급은 서로 다른 안전통제 요건에 대응한다.³⁸

가. GB/T 35273-2020 「정보안전기술 개인정보 안전규범」

GB/T 35273-2020 은 2020 년 10 월 1 일 시행된 개인정보 안전 분야의 핵심 통용 기술표준이다. 동 표준의 ‘개인민감정보’ 획정은 PIPL 제 28 조와 상호 확인된다. 표준은 ‘개인 건강생리정보’, ‘유전자’, ‘개인 생체인식정보’ 등을 개인민감정보로 명시적으로 열거한다. 본 사건의 데이터 범위에 따르면 진료기록, 검사, 영상, 수술 후 추적관찰 등의 데이터는 표준에서 말하는 ‘개인 건강생리정보’에 속하여 개인민감정보를 구성하며, 이는 PIPL 제 28 조의 ‘의료건강’류 민감개인정보 인정과 일치한다.

민감개인정보의 실질적 판단기준에 관하여 학계의 통설은 ‘자연인의 인격존엄이 침해되기 쉬운지 여부와 개인의 신체·재산 안전을 위해하는지 여부’를 판단기준으로 하여야 한다고 보며, 의료건강정보는 개인의 신체상태, 생명상태, 질병이력 등 깊은 사적 영역을 직접 반영하므로 민감개인정보의 전형적 유형을 구성한다.³⁹ 이러한 실질적 판단은 GB/T 35273-2020 의 열거식 획정과 상호 보완하여, 본 사건에서 임상데이터를 민감개인정보로 식별하는 결론을 함께 뒷받침한다.

나. GB/T 39335-2020 「정보안전기술 개인정보 안전영향평가 지침」

GB/T 39335-2020 은 2021 년 6 월 1 일 시행되었으며, PIPL 제 55 조 ‘개인정보보호 영향평가’의 구체적 기술지침이다. PIPL 제 55 조 제 1 호(민감개인정보의 처리)와 제 4 호(국외에 개인정보 제공)에 따라 본 사건은 개인정보보호 영향평가 요건을 이중으로 촉발한다.

³⁸GB/T 39725-2020 의 건강의료데이터 6 대 분류(개인속성데이터, 건강상태데이터, 의료응용데이터, 의료지불데이터, 위생자원데이터, 공공위생데이터)와 5 등급 민감도 구분에 관한 규정.

³⁹王利明:《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》,载《当代法学》2022年第1期 참조.

동 표준의 영향평가 프레임워크에 따르면 본 사건은 다음을 평가하여야 한다. 처리목적의 적법성·정당성·필요성, 처리활동이 개인의 적법한 권익에 초래할 수 있는 위험(데이터 유출, 남용, 2 차 이용 등), 이미 취한 안전보호 조치의 유효성, 개인의 처리활동에 대한 통제 가능 정도. 본 사건의 개인정보보호 영향평가 문서는 공개 경로에 밝혀져 있지 않으며, 여전히 미규명 사항에 속한다.

다. 네 표준의 본 사건에서의 분담관계

종합하면 네 국가표준은 본 사건에서 층위가 분명한 분담을 형성한다. GB/T 43697-2024 는 통용 분류등급 방법론을 제공하고(방법론 층위), GB/T 39725-2020 은 의료업종의 6대 분류·5등급 세부화를 제공하며(업종 세부화 층위), GB/T 35273-2020 은 개인정보 차원의 민감정보 식별을 제공하고(개인정보 층위), GB/T 39335-2020 은 영향평가의 기술지침을 제공한다(영향평가 층위). 아래 표는 그 분담과 본 사건에서의 역할을 표시한다.

층위	표준	본 사건에서의 역할	대응 법률조항
방법론 층위	GB/T 43697-2024	산업영역+업무속성 분류, 3 등급 데이터안전법 분급, 중요데이터 식별(부록 G) 제 21 조	
업종 세부화 층위	GB/T 39725-2020	건강의료데이터 6 대 분류, 5 등급 민감도, 전생애주기 안전요구	데이터안전법 제 21 조(업종 구체화)
개인정보 층위	GB/T 35273-2020	개인민감정보 식별(건강생리정보, 유전자, 생체인식)	개인정보보호법 제 28 조
영향평가 층위	GB/T 39335-2020	개인정보보호 영향평가의 기술 프레임워크	개인정보보호법 제 55 조

위 표준들은 본 사건 분류등급 판단의 방법론과 근거를 구성한다. 이하의 두 절에서는 이 표준 방법을 본 사건 데이터에 적용한다. 먼저 GB/T 43697-2024 에 따라 본 사건 데이터를 단계별로 식별하고, 다음으로 컴플라이언스 지속 단계에서 규범 변화로 생기는 차이를 다룬다.

6. GB/T 43697-2024 방법에 따른 본 사건 데이터의 단계별 식별

이하에서는 본 장 제 4 절에서 서술한 GB/T 43697-2024 의 ‘산업영역 우선, 업무속성 후속’이라는 분류 사고와 ‘분급대상 — 요소 식별 — 영향 분석 — 등급의 종합적 확정’이라는 분급 절차에 따라 본 사건 데이터를 단계별로 식별한다. 밝혀 둘 것은, 공개자료는 본 사건 컴플라이언스 지속 단계의 실제 식별 결과를 공개하지 않았으므로 아래 각 단계의 결론은 모두 추론이며 사실적 결론을 구성하지 않는다는 점이다.

제 1 단계, 산업영역 분류. 베이징우의병원은 의료보건기관이고 본 사건 데이터는 진료와 임상연구 활동에서 생성되었으므로, 산업영역 분류상 ‘보건의료’ 업종에 귀속된다. 이 단계는 정성적 귀류로서 결론이 비교적 확실하다.

제 2 단계, 업무속성 분류. ‘보건의료’ 산업영역 아래에서 업무속성 차원 중 ‘데이터 용도’, ‘기술 대상’에 따라 세분화한다. 본 사건 데이터는 용도에 따라 ‘임상연구데이터’(COLOR III/IV 연구 전용의 중앙화 재판독, 추적관찰, 통계 데이터)와 ‘의료서비스데이터’(진료활동에서 생성된 진료기록, 검사, 영상 등)의 두 부류로 더 나눌 수 있다.

제 3 단계, 특수 범주 식별의 중첩. 분류 과정에서 두 가지 식별을 중첩한다. 첫째, 「개인정보보호법」 제 28 조와 GB/T 35273-2020 에 따라 ‘민감개인정보’ 속성을 식별한다. 본 사건의 진료기록, 검사, 영상, 수술 후 추적관찰 등의

데이터는 ‘의료건강’류 민감개인정보에 속하고, 주민신분증번호는 ‘특정신분’류 민감개인정보에 속한다. 둘째, 「인류유전자원관리조례 실시세칙」 제 2 조 제 3 항에 따라 인류유전자원정보 해당 여부를 판단한다. 본 사건 협약의 공개내용에 유전자 데이터 수집이 언급되지 않았고 임상데이터·영상데이터 등이 동 항에 의하여 인류유전자원정보에서 명시적으로 제외되므로, 본 사건은 인류유전자원정보를 구성하지 않는다고 추론된다. 이 단계의 의의는, 민감개인정보 속성이 ‘상향 엄격적용’ 원칙을 통하여 이후의 분급에 영향을 미치고, 인류유전자원정보의 배제가 본 사건을 인류유전자원관리조례 아래의 더 엄격한 심사 궤도에 들어가지 않도록 한다는 데 있다.

제4단계, 분급. 이 단계는 분급 절차에 따라 항목별로 전개되어야 한다. 첫째, 분급대상의 확정. 본 사건 데이터에는 분급상 적어도 두 부류의 서로 다른 분급대상이 존재한다. 하나는 개별 환자의 임상데이터 항목 또는 단건 진료기록이고, 다른 하나는 다기관 집적 후의 집단 진료 규모 데이터셋과 중앙화 재판독으로 형성되는 파생데이터이다. 양자는 서로 다른 분급대상에 속하므로 각각 판단하여야 한다. 둘째, 분급 요소의 식별. 개별 환자 데이터 항목은 규모·포괄도가 모두 낮다. 집단 진료 규모 데이터셋에 대하여는 ‘규모’(COLOR IV 계획상 1,158 레 등록, 참여기관 30~50 개소, 전 세계 다기관 합계 규모), ‘집단’(결장·직장암 환자라는 특정 질환 집단), ‘포괄도’(다기관·복수 지역) 등의 요소를 고려하여야 하고, 중앙화 통계 재판독이 관련되므로 파생데이터의 ‘심도’ 요소도 고려하여야 한다.

셋째, 데이터 영향 분석. 개별 환자 데이터는 일단 유출되더라도 영향대상이 주로 개인권익이고 영향 정도는 개인 차원에 그친다. 집단 진료 규모 데이터셋에 대하여는, 부록 G 제 o)항에 따라 ‘국가 또는 지역의 집단 건강·생리 상태를 반영’하고 ‘대량 인구의 진료와 건강관리’, ‘특정 의약품 실험’에 관련되는 데이터가 중요데이터로 명시적으로 열거되어 있다. 본 사건의

다기관 집적된 결장·직장암 집단 진료 및 추적관찰 데이터는 성질상 동 항의 기술에 대응하므로 그 영향대상은 ‘개인권익’에서 ‘공중의 건강과 안전’으로 상승할 수 있고, 영향 정도도 그에 따라 높아진다. 넷째, ‘상향 엄격적용’에 따른 등급의 종합적 확정. 개별 환자 데이터 항목은 중요데이터 정의 중 ‘공민 개인에게만 영향을 미치는 데이터는 일반적으로 중요데이터로 하지 않는다’는 획정에 따라 일반데이터로 정하여야 한다. 집단 진료 규모 데이터셋은 부록 G 제 6)항에 열거된 데이터 유형에 대응하고 일정한 규모에 도달하므로, 부록 G의 ‘열거 요소 중 하나를 갖추면 중요데이터로 식별 가능’ 규칙과 ‘상향 엄격적용’ 원칙을 결합하면 방법론상 중요데이터로 식별되어야 한다.

이상을 종합하여 추론하면, 본 사건 데이터의 등급은 ‘층위별 결론’을 보인다. 개인 차원의 임상데이터는 일반데이터이고(그중 민감개인정보 부분은 비교적 높은 세부 등급에 속한다), 다기관 집적된 집단 진료 규모 데이터는 방법론상 중요데이터의 특징을 갖춘다. 이 결론의 최종 확인은 여전히 업종 중요데이터 목록과 주관부처의 ‘일정 규모’ 임계치에 대한 구체적 인정에 달려 있으며, 본 사건 컴플라이언스 지속 단계의 실제 식별 결과는 공개자료에 밝혀져 있지 않다.

7. 본 사건 심사 후 신설된 분류등급 규칙과 컴플라이언스 지속 단계

본 사건의 심사 통과 후 순차적으로 나온 분류등급 규칙은 본 사건의 최초 심사에는 소급 적용되지 않으나, 본 사건의 컴플라이언스 지속 단계(평가 유효기간 만료 후의 갱신 신고)에 대하여 규범적 의의를 가진다. 본 사건의 안전평가 유효기간은 「데이터 국외이전 안전평가 방법」 제 14 조에 따라 2 년으로서 2024 년 9 월에 만료된다. 2024 년 3 월 22 일 시행된 「데이터 국경 간 이동 촉진 및 규범화 규정」 제 9 조는 이 유효기간을 3 년으로 연장하였는데,

2022 년 9 월의 승인을 기준으로 추산하면 신규칙에 따른 본 사건의 유효기간은 약 2025 년 9 월에 만료된다(평가 결과가 나온 날이 공개되지 않았으므로 실제 만료 시점은 그만큼 늦추어질 수 있다). 구규칙과 신규칙 중 어느 것을 적용하더라도 본 연구 작성 시점(2026 년 5 월)까지 본 사건의 원 평가 유효기간은 이미 만료되었으며, 그 컴플라이언스 지속 상태는 공개 경로에 밝혀져 있지 않다.⁴⁰

본 사건이 컴플라이언스 지속 단계에서 재신고 또는 평가 연장을 개시한다면, 심사 시점과 비교하여 적어도 세 가지 규범 차원에서 서로 다른 판단 틀을 마주하게 된다. 첫째, GB/T 43697-2024 가 통일된 분류 방법론과 3 등급 분급체계를 확립하고 규범성 부록 G 로 중요데이터 식별 요소를 세분화하였으므로, 본 사건이 재분급을 하게 되면 동 표준(부록 G 포함)에 따라 앞서 본 4 단계 식별을 다시 수행하여야 한다. 둘째, 「데이터 국경 간 이동 촉진 및 규범화 규정」이 데이터 국외이전 규제에 일련의 조정 — 평가 유효기간의 3 년 연장, 국외이전 안전평가 촉발 사유의 계산방식 조정 등 — 을 가하여, 본 사건 컴플라이언스 지속 단계의 경로 선택과 기준 판단에 직접 관련된다.

셋째, 「중국(베이징)자유무역시험구 데이터 국외이전 관리 리스트(네거티브리스트)(2024 년판)」(2024 년 8 월 30 일 발표)은 의약산업의 ‘중요데이터’를 필드 수준에서 구체화하여, 일정 규모 이상의 집단 진료, 건강·생리 상태, 의료구호 보장 데이터, 특정 의약품 실험 데이터 등을 중요데이터로 열거하였다. 이 리스트의 표현은 부록 G 제 o)항과 고도로 대응한다. ‘집단 진료’, ‘건강·생리 상태’, ‘특정 의약품 실험’은 부록 G 제 o)항과 거의 축자적으로 호응하므로, 부록 G 제 o)항의 지방 차원 필드 수준 세부화로

⁴⁰ 丁晓东：《数据跨境流动的法理反思与制度重构——兼评〈数据出境安全评估办法〉》，载《行政法学研究》2023 年第 1 期，第 62—77 页 참조.

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

볼 수 있으며, 앞서 본 사건의 집단 진료 규모 데이터가 중요데이터로 식별되어야 한다는 추론을 한층 확인하여 준다. 본 사건의 베이징우의병원이 사업단위로서 베이징 자유무역시험구 리스트의 적용범위에 포섭되는지는 확인이 필요하다. 자유무역시험구 리스트가 적용되지 않는다면 국가 차원의 통일 규칙에 따라 처리되며, 결론의 방향은 일치한다.⁴¹

주목할 점은, 본 사건의 심사 시점(2022~2023 년)부터 본 연구 작성 시점(2026 년 5 월)까지 분류등급 규칙이 국가 차원에서 ‘원칙적 프레임워크’로부터 ‘조작적 세부화’로 실질적 변화를 겪었다는 것이다. 이러한 규범 차원의 동태적 변화는 본 사건 컴플라이언스 지속 단계가 직면하는 분류등급 판단이 원 심사 시점과 이미 다르다는 것을 결정짓고, 본 사건을 이 제도의 진화를 관찰하는 종단적 표본으로 만든다.

8. 분류등급과 네트워크안전등급보호의 본 사건에서의 연계

본 사건의 분류등급 판단과 네트워크안전등급보호제도는 사실 차원에서 서로 연계된다. 앞서 본 병원 정보센터의 네트워크안전·데이터안전 재평가(병원 내부 3 단계 중 제 2 단계)의 실질은 곧 병원의 네트워크안전등급보호 등급과 방어능력이 본 사건 데이터 국외이전이 요구하는 보호수준에 부합함을 확인하는 것이다. 바꾸어 말하면, 분류등급은 ‘데이터가 어떤 등급이고 어떤 강도의 보호가 필요한가’의 문제를 해결하고, 등급보호는 ‘데이터를 담는 네트워크와 정보시스템이 상응하는 방어능력을 갖추었는가’의 문제를 해결한다. 전자는 데이터 차원, 후자는 시스템 차원으로서 본 사건에서 함께 데이터 국외이전의 국내 안전기반을 구성한다. 네트워크안전등급보호제도 2.0 의 본 사건에 대한 구체적 적용은 제 5 장에서 상술한다.

⁴¹ 동 네거티브리스트의 의약산업 중요데이터에 대한 필드 수준 획정은 GB/T 43697-2024 부록 G(규범성) 제 o)항 ‘중요데이터 식별지침’에 열거된 고려요소와 고도로 대응한다.

9. 소결: 규범 미완성 — 사실 선행

본 장의 사실 제시와 규범 분석을 종합하면, 본 사건을 관통하는 하나의 특징을 관찰할 수 있다. 즉 분류등급 차원에서 본 사건의 컴플라이언스 과정은 ‘규범 미완성 — 사실 선행’의 양상을 보인다. ‘규범 미완성’이란 본 사건 심사 시(2022~2023 년) 국가 차원의 통일된 분류등급 방법론이 아직 의견수렴안 단계에 머물러 있었고, 중요데이터 식별지침과 자유무역시험구 네거티브리스트의 필드 수준 획정이 모두 나오기 전이었으며, 의료기관의 데이터 분류등급 의무가 「의료보건기관 네트워크안전 관리방법」에 의하여 막 명확해진, 규범 공급이 무에서 유로 가는 구축기에 있었음을 가리킨다. ‘사실 선행’이란 이러한 배경에서 본 사건의 처리자인 베이징우의병원이 내부 조직(과학기술처, 정보센터)과 내부 방법(「데이터 국외이전 안전관리방법」)을 통하여 인류유전자원 식별, 네트워크안전 등급 식별, 중요데이터 식별 메커니즘 구축이라는 분류등급 판단 업무를 사실상 완성하였음을 가리킨다.

이 ‘사실 선행’형 컴플라이언스 모델은 이중적 의의를 가진다. 실증의 차원에서, 그것은 제도 구축기에 처리자의 내부 거버넌스 능력이 규범 공백기의 식별 기능을 실제로 담당하였음을 보여 주며, 의료데이터 국경 간 컴플라이언스의 선행시범 표본을 구성한다. 규범의 차원에서, 그것은 하나의 구조적 문제를 드러낸다. 즉 최초 심사가 근거한 분류등급 프레임워크와 컴플라이언스 지속 단계에 적용되는 새 프레임워크 사이에 실질적 차이가 존재할 때, 장기 임상연구의 데이터 국외이전 컴플라이언스는 ‘동일한 데이터, 서로 다른 시점, 서로 다를 수 있는 등급’이라는 긴장에 직면한다. 본 사건의 COLOR IV 가 2030 년까지 지속되는 반면 평가 유효기간은 2~3 년에 불과하다는 사정이 바로 이 긴장을 본 사건이 장기간 마주하여야 할 현실 문제로 만든다. 나아가 본 사건에 관하여 말하면, ‘규범의 완성’은 적어도 세 가지 요건의 구비를 요구한다. 즉 보편적 구속력을 가지는 데이터 분류등급 규칙, 효력이

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

발생한 중요데이터 목록, 그리고 인류유전자원정보 경계의 명확한 획정이 그것인데, 심사 시점에 첫째 것은 권고성 업종표준(GB/T 39725-2020)만이 참조 가능하였고 뒤의 둘은 결여되어 있었다. ‘사실 선행’은 따라서 이중의 의미를 가진다. 인정의 순서에서는 처리자의 사실적 식별이 규범적 확인에 앞섰고, 제도의 생성에서는 이러한 개별 사안이 드러낸 식별의 곤란과 그 후 규범의 체계화 과정(GB/T 43697-2024, 네거티브리스트와 인류유전자원 실시세칙의 순차적 등장)이 시간적으로 앞뒤로 이어졌다. 본 연구는 시간 순서의 관찰에 그치며 인과의 단언은 하지 않는다. 이러한 양상은 의료데이터 분야에 고유한 것은 아니나, 규범 밀도와 데이터 민감도가 모두 높은 의료 분야에서 가장 집중적으로 나타난다.

V. 네트워크안전등급보호제도에 의한 본 사건의 국내 시스템 보장

앞 장에서 본 바와 같이, 데이터 분류등급과 네트워크안전등급보호는 본 사건에서 서로 연계된다. 전자는 데이터 차원에, 후자는 시스템 차원에 작용한다. 본 장에서는 네트워크안전등급보호제도의 규범적 기초와 본 사건에 대한 구체적 적용을 제시한다. 평가의 구조에서 이 제도는 국내 데이터 처리자의 안전보장 능력 심사에 대한 사실적 기초를 구성한다.

1. 네트워크안전등급보호제도의 규범적 기초

네트워크안전등급보호제도가 중국 법체계에서 가지는 규범적 기초는 법률 층위, 행정법규 층위, 국가표준 층위의 세 층을 포함한다.

법률 층위의 기초는 「네트워크안전법」 제 21 조와 제 31 조로 구성된다. 「네트워크안전법」 제 21 조는 국가가 네트워크안전등급보호제도를 시행함을 규정하고, 네트워크 운영자에게 등급보호제도의 요구에 따라 다섯 가지

안전보호 의무 — 내부 안전관리제도의 제정, 컴퓨터 바이러스·네트워크 공격을 방지하는 기술조치, 네트워크 운영상태를 감시·기록하는 기술조치와 6 개월 이상의 네트워크 로그 보존, 데이터 분류와 중요데이터 백업·암호화 조치, 그리고 법률·행정법규가 정하는 그 밖의 의무 — 를 이행하도록 요구한다. 「네트워크안전법」 제 31 조는 등급보호제도를 기초로 핵심정보인프라에 대하여 중점 보호를 시행한다.

행정법규 층위에서는,公安부가 주도하여 기초한 「네트워크안전등급보호조례」가 본 연구 작성 시점까지 여전히 의견수렴안 단계에 있어 정식 공포되지 않았으며, 동 조례가 정식으로 나오기 전까지 등급보호제도의 구체적 시행은 주로 국가표준을 매개로 이루어진다. 2021 년 9 월 1 일 시행된 「핵심정보인프라 안전보호조례」는 핵심정보인프라에 대한 중점 보호를 시행하여 등급보호제도와 연계를 형성한다.

국가표준 층위에서는,公安부가 주도하여 네트워크안전등급보호제도 2.0 표준체계를 제정하였으며, 그 핵심은 GB/T 22239-2019 「정보안전기술 네트워크안전등급보호 기본요구」(2019 년 5 월 10 일 발표, 2019 년 12 월 1 일 시행)이다. 부속 표준에는 GB/T 22240-2020 등급결정지침, GB/T 25058-2020 실시지침, GB/T 25070-2019 안전설계 기술요구, GB/T 28448-2019 측정평가요구, GB/T 28449-2018 측정평가과정지침, 그리고 상위 준칙인 GB 17859-1999 「컴퓨터정보시스템 안전보호 등급구분 준칙」이 포함된다. GB/T 22239-2019 는 2025 년 5 월 30 일 전국정보안전표준화기술위원회의 재심사를 거쳐 ‘계속 유효’로 결론지어졌으며, 이는 동 표준이 중·단기적으로 안정성을 유지함을 의미한다.

업종 층위에서는, 「의료보건기관 네트워크안전 관리방법」 제 5 조, 제 6 조, 제 9 조, 제 10 조가 의료보건기관의 등급보호 업무를 업종에 맞게 세부화한다. 동 방법 제 6 조 제 4 호는 의료보건기관이 이미 등급이 결정되어 비안된 네트워크의

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

안전성을 검측·평가하도록 명확히 요구한다. 즉 제 3 급 또는 제 4 급의 네트워크는 등급보호 측정평가기관에 위탁하여 매년 1 회 이상 네트워크안전 등급측정평가를 실시하고, 제 2 급의 네트워크 중 10 만 명 이상의 개인정보가 관련되는 것은 3 년에 1 회 이상, 그 밖의 것은 5 년에 1 회 이상 실시하여야 한다.

2. 네트워크안전등급보호제도 2.0 표준의 내용

GB/T 22239-2019 는 ‘1+5’ 모델을 채택한다. 즉 1 개의 안전 통용요구에 클라우드컴퓨팅, 모바일인터넷, 사물인터넷, 산업제어, 빅데이터의 5 대 신기술·신응용 분야 안전 확장요구를 더한 것이다. 안전요구는 2 대 부류 10 대 항목으로 나뉜다. 기술요구에는 안전 물리환경, 안전 통신네트워크, 안전 구역경계, 안전 컴퓨팅환경, 안전 관리센터의 다섯 항목이, 관리요구에는 안전 관리제도, 안전 관리기구, 안전 관리인원, 안전 구축관리, 안전 운영유지관리의 다섯 항목이 포함된다.

등급보호의 대상은 침해 시 초래할 수 있는 영향의 정도에 따라 5 등급으로 나뉜다. 제 1 급 ‘자주보호급’은 일반 네트워크에 적용되고, 제 2 급 ‘지도보호급’은 침해 시 공민·법인의 적법한 권익을 해치는 네트워크에 적용되며, 제 3 급 ‘감독보호급’은 침해 시 사회질서·공공이익을 해치는 네트워크에 적용되어 매년 1 회 이상의 등급보호 측정평가가 요구되고, 제 4 급 ‘강제보호급’은 침해 시 사회질서·공공이익을 중대하게 해치거나 국가안전을 해치는 네트워크에 적용되어 반년에 1 회 이상의 측정평가가 요구되며, 제 5 급 ‘전문통제보호급’은 침해 시 국가안전을 중대하게 해치는 네트워크에 적용된다. 등급보호 2.0 은 2008 년의 등급보호 1.0 에 비하여 표준 명칭(‘정보시스템’에서 ‘네트워크’로), 분류의 조정, 신뢰성 검증의 강화 등에서 실질적 변화를 보였다.

3. 의료기관의 등급보호제도 시행과 본 사건 베이징우의병원의 등급보호 현황

의료기관의 통상적 등급 결정에 관한 업계 관행에 따르면, 2급 이상 종합병원, 3급 병원, 지역 보건의료 정보플랫폼, 의료보험 정보시스템, 전자진료기록 시스템 등은 통상 제 3급으로, 국가급 의학데이터센터, 국가급 인류유전자원 표본은행, 국가 건강의료빅데이터센터 등은 제 4급으로 결정되며, 일반 외래관리시스템, 기초 재무시스템 등 비핵심 시스템은 제 2급으로 결정될 수 있다.

본 사건의 실제 사실로는, 베이징시 보건위생위원회 공식 홈페이지가 “병원 정보센터가 네트워크안전·데이터안전을 다시 평가하여 병원의 네트워크안전 제도가 완비되고 실효성 있게 이행되며 안전방어 기술능력이 등급보호 등 표준규범에 부합함을 확인하였다”고 공개하였다. 이 표현은 베이징우의병원이 본 사건 신고 전에 네트워크안전등급보호 컴플라이언스 재평가를 완료하였음을 명확히 보여준다.

의료기관의 통상적 등급 결정에 따른 추론으로는(본 연구의 사실적 결론을 구성하지 않는다), 대형 3급 갑등 종합병원이자 국가소화기질환 임상의학연구센터 수행기관, 소화건강 전국중점실험실 수행기관인 베이징우의병원의 핵심 의료정보시스템은 제 3급 이상으로 결정되어야 할 것이다. 다만 베이징우의병원 각 정보시스템의 구체적 등급 결정 결과, 등급보호 측정평가기관의 신원, 측정평가 보고서의 내용, 부적합 사항의 시정 상황, 측정평가의 유효기간, 그리고 등급보호 컴플라이언스 재평가의 구체적 시점은 모두 공개자료에 밝혀져 있지 않다.

4. 등급보호제도 2.0 과 본 사건 데이터 국외이전 신고의 연계관계

본 사건의 실제 절차 순서는 등급보호 컴플라이언스가 사실상 데이터 국외이전 신고의 선행 조건을 구성함을 보여준다. 규명된 사실에 따르면 본 사건의 전체 절차 순서는 세 국면으로 정리할 수 있다. 제 1 국면은 병원 과학기술처가 프로젝트의 과학적 의의, 산출 가치, 인류유전자원 상황을 내부 평가한 것이고, 제 2 국면은 병원 정보센터가 네트워크안전·데이터안전을 다시 평가하여 등급보호 등 표준규범에 부합함을 확인한 것이며, 제 3 국면은 베이징시 인터넷정보판공실에 데이터 국외이전 신고를 제출하여 국가인터넷정보판공실의 평가를 통과한 것이다. 등급보호 컴플라이언스는 제 2 국면에 위치하며, 제 3 국면 안전평가 신고의 사실상의 선행 조건이다.

규범 차원에서 보면, 「데이터 국외이전 안전평가 방법」 제 8 조 제 5 호는 안전평가가 “본 방법이 규정한 절차 이행의 적법성, 중국의 법률·행정법규·부문규장 규정예의 부합 여부”를 평가하도록 규정한다. 등급보호 컴플라이언스는 「네트워크안전법」 제 21 조가 규정하는 법정 의무로서 데이터 처리자의 일반적 컴플라이언스 의무의 구성 부분이다. 따라서 안전평가에서 국내 측 안전수준에 대한 평가는 사실상 등급보호 컴플라이언스를 선행 조건으로 한다. 이러한 ‘등급보호 컴플라이언스 — 국외이전 안전평가’의 사실적 승계관계가 본 사건에서 온전히 드러난다.

5. 등급보호제도와 그 밖의 규범의 병행적용 관계

본 사건에서 등급보호제도 2.0 과 그 밖의 규범의 병행적용 관계는 분명한 분업을 보인다. 등급보호 2.0 은 병원 정보센터 평가의 점검 근거이자 안전평가의 사실상의 선행 조건이고, 데이터 분류등급(GB/T 39725-2020)은 병원 데이터 거버넌스의 분류 근거이며, 개인정보 영향평가(GB/T 39335-2020)는 PIPL

제 55 조의 기술지침이고, 인류유전자원 관리(인류유전자원관리조례)는 병원 과학기술처 평가의 판정 근거 중 하나이며, PIRL 제 38 조와 「데이터 국외이전 안전평가 방법」은 본 사건의 핵심 적용규범이다.

각 규범은 본 사건에서 병행하는 컴플라이언스 요구로서 각자의 범위에서 적용된다. 절차의 순서에서 보면, 등급보호 컴플라이언스는 데이터 국외이전 신고의 사전 기초이고, 분류등급은 병원 데이터 거버넌스의 기초 도구이며, 개인정보 영향평가는 이미 실시되었을 것이고, 인류유전자원 식별은 병원 과학기술처가 완료하였다. 규범들 사이에 주종관계나 선후관계는 존재하지 않으나, 등급보호 컴플라이언스는 네트워크안전의 기초적 의무로서 사실상 본 사건 컴플라이언스의 ‘기저’ 기초를 구성한다.

종합하면, 본 장이 제시한 사실은 다음을 보여준다. 등급보호제도 2.0 은 본 사건에서 독립한 컴플라이언스 의무인 동시에(「네트워크안전법」 제 21 조의 직접 요구), 데이터 국외이전 신고의 사실상의 선행 조건이기도 하다(「데이터 국외이전 안전평가 방법」 제 8 조 제 5 호의 간접 요구). 베이징우의병원이 본 사건 신고 전에 등급보호 컴플라이언스 재평가를 완료한 사실은 이러한 ‘이중적 위상’이 실무에서 구체적으로 작동하는 모습을 반영한다. 다만 본 사건에서 등급보호 컴플라이언스의 구체적 세부사항(등급 결정 결과, 측정평가기관, 측정평가 보고서 등)은 공개 경로에 밝혀져 있지 않으며, 본 연구의 미확인 사항 중 하나를 구성한다.

이로써 법원(法源), 데이터 분류등급(그 기술표준 체계 포함), 네트워크안전등급보호의 각 제도가 본 사건에 적용되는 모습이 각각 제시되었다. 다음 장에서는 위 규범들을 본 사건 데이터의 전생애주기에 집성하여 투영하고, ‘8 개 단계 적용규범 매트릭스’로써 규범과 사실의 총대조를 완성한다.

VI. 의료데이터 전생애주기 컴플라이언스의 매트릭스 집성

데이터 전생애주기 관리는 중국 데이터 거버넌스 체계의 핵심 작동 메커니즘으로서, 데이터의 수집부터 삭제까지의 전 단계를 포괄한다. 본 장에서는 먼저 본 사건의 국외이전 단계와 상류 각 단계 사이의 의존관계를 정리하고, 이어 ‘8 개 단계 적용규범 매트릭스’로 본 사건 데이터의 전생애주기 각 단계에서의 규범 배치를 체계적으로 제시한다. 이 매트릭스가 응답하는 것은 평가사항 중 ‘국외이전 중과 국외이전 후’ 전 과정 위험의 심사 차원이다. 그중 가공 단계(코드화·비식별화된 데이터도 여전히 개인정보에 속하므로 평가의 틀 안에 남아야 한다는 점)와 삭제 단계(개인의 삭제청구권과 임상연구 보존의무 사이의, 규범을 가로지르는 긴장)에서 추출되는 의료 특유의 규칙은, 의료 임상연구라는 상황이 일반 데이터 컴플라이언스 규칙을 수정·구체화하는 모습을 집약적으로 보여준다.

1. 전생애주기 관리의 규범적 기초

데이터 전생애주기 관리가 중국 규범체계에서 처음으로 체계적으로 표현된 것은 국가보건위생위원회가 2018 년 9 월 13 일 발표한 「국가 건강의료빅데이터 표준·안전·서비스 관리방법(시행)」 제 16 조이다. 동 조는 건강의료빅데이터 안전관리란 데이터의 채집·저장·발굴·응용·운영·전송 등 여러 단계에서의 안전과 관리를 말한다고 규정한다. 동 조에 열거된 여섯 단계가 의료데이터 전생애주기 관리의 기초 골격을 구성한다.

「개인정보보호법」 제 2 장 제 1 절 ‘개인정보 처리규칙’은 개인정보 처리의 전생애주기를 더욱 완결적으로 규범화한다. 수집 국면은 제 13 조(적법한 처리 근거), 제 14 조~제 17 조(고지의무, 최소필요 원칙) 및 제 29 조(민감개인정보 단독 동의)에, 저장 국면은 제 19 조(최단 보존기간)에, 사용·가공 국면은

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

제 21 조(위탁처리), 제 22 조(개인정보의 이전)와 제 73 조(익명화·비식별화의 정의)에, 제공·공개 국면(국외이전 포함)은 제 23 조(타인에의 제공), 제 25 조(공개 처리)와 제 38 조~제 43 조(국외이전 경로와 컴플라이언스 요건)에, 삭제 국면은 제 47 조(삭제권과 처리자의 능동적 삭제의무)에 대응한다.

「데이터안전법」 제 3 장 ‘데이터안전 제도’는 ‘데이터 처리활동’의 관점에서 전생애주기에 대한 보충 규정을 두며, 동 법상 ‘데이터 처리’는 데이터의 수집, 저장, 사용, 가공, 전송, 제공, 공개 등을 포함한다.

의료업종 차원에서는 「의료보건기관 네트워크안전 관리방법」 제 22 조가 의료보건기관 데이터의 전생애주기 관리를 업종에 맞게 세부화하여, 의료데이터의 채집·저장·사용·전송·제공·공개·삭제 등 각 단계에서 안전보호 책임을 이행하도록 요구한다.

임상연구 분야의 특별 규범은 두 규장으로 구성된다. 하나는 「약물 임상시험 품질관리규범」(GCP, 2020 년 7 월 1 일 시행)으로 국가약품감독관리국과 국가보건위생위원회가 공동으로 공포하였다. 동 규범의 직접 적용대상은 약물 임상시험이고 본 사건의 COLOR III·COLOR IV 는 외과 수술 연구이므로 GCP 가 직접 적용되지는 않으나, 충분한 설명에 근거한 동의, 데이터 무결성, 원본기록 보존, 모니터링과 점검에 관한 GCP 의 방법론은 국내 임상연구 실무에서 널리 참조·적용되므로 본 연구는 이를 참조적용 규범으로 분류한다. 다른 하나는 「인간 대상 생물의학연구 윤리심사방법」(위계위 11 호령, 2016)으로서 본 사건 심사 시 적용된 윤리심사 규범이며, 2023 년 2 월 18 일 발표·시행된 「인간 대상 생명과학 및 의학연구 윤리심사 방법」(国卫科教发[2023]4 号)과 병행하여 존재한다.

2. 본 사건에 적용되는 8 개 단계

위 규범들을 종합하면, 본 사건에 적용되는 의료데이터 전생애주기는 수집, 저장, 사용, 가공, 전송, 제공(국외이전 포함), 공개, 삭제의 8 개 단계로 정리할 수 있다. 이하에서 각 단계에서의 본 사건의 사실 상황과 규범 적용관계를 기술한다.

수집 단계. 베이징우의병원 일반외과센터는 COLOR III 연구에서 중국 환자데이터의 수집을 담당하였으며 본 사건 공시 시점까지 170 레를 등록하였고, COLOR IV 연구계획은 1,158 레(전 세계 다기관 합계 규모)의 등록을 계획한다. COLOR III 협약은 병리학적으로 확진된 I~III 기 직장암을 등록 기준으로 명문화하고, COLOR IV 협약은 18~80 세의 병리학적 또는 세포학적으로 확진된 우측 결장암 환자를 요구한다. 본 단계에는 PIPL 제 13 조, 제 14 조~제 17 조, 제 29 조 및 윤리심사 관련 규범과 약물 임상시험 품질관리규범이 적용된다. 본 사건에서 피험자 동의 취득의 구체적 방식(서면 동의서의 내용, 단독 동의의 범위, 데이터 국외이전 고지의 포괄 범위, 국외 수령자의 고지, 사망 피험자의 처리, 동의 철회 메커니즘 등)은 공개 경로에 밝혀져 있지 않으며, 제 II 장 제 8 절의 동의 문제 부분에서 상술하였다.

저장 단계. 베이징시 보건위생위원회의 공식 공개에 따르면, 병원 정보센터는 “네트워크안전·데이터안전을 다시 평가하여 병원의 네트워크안전 제도가 완비되고 실효성 있게 이행되며 안전방어 기술능력이 등급보호 등 표준규범에 부합함을 확인”하였다. 본 단계에는 PIPL 제 19 조(최단 보존기간), PIPL 제 40 조(CMO 와 100 만 명 이상 규모 처리자의 현지화), 「네트워크안전법」 제 37 조, 「데이터안전법」 제 27 조(데이터 안전관리제도의 수립), 등급보호 2.0 및 「의료보건기관 네트워크안전 관리방법」이 적용된다. 구체적인 저장 위치, 암호화 조치, 접근통제, 보존기간 등 기술적 세부사항은 공개 경로에 밝혀져 있지 않다.

사용 단계. 본 사건 데이터는 COLOR III 연구의 직장암 환주절제연(CRM)

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구
침범률과 5 년 생존율 평가, 그리고 COLOR IV 연구의 30 일 문합부 누출률과
3 년 무병생존율 평가에 사용된다. 본 단계에는 PIPL 제 6 조(처리목적의
명확·합리)와 제 14 조 제 2 항(목적·방식 변경 시 재동의)이 적용된다. 본 사건의
데이터 사용 목적은 위 두 연구의 임상 평가변수 평가로 명확히 한정되어
있으며, 수집 시 고지한 목적과 일치하여야 한다.

가공 단계. 본 사건의 가공에는 임상데이터의 통계분석, 데이터 클리닝,
중양화 재판독(COLOR III 협약이 명문으로 요구하는 중양화 MRI 재판독과
중양화 병리 재판독), 다기관 데이터의 병합, 그리고 비식별화 처리가 포함된다.
본 단계에는 PIPL 제 73 조의 ‘익명화’와 ‘비식별화’에 대한 법정 구분이
적용된다. PIPL 제 73 조에 따르면 비식별화된 데이터는 여전히 개인정보의
범주에 속하여 PIPL 의 모든 구속을 받으며, 진정한 ‘익명화’ 데이터(복원이
불가능한 것)만이 더 이상 PIPL 의 관할을 받지 않는다. 본 사건에 관하여
말하면, 국제 다기관 연구가 중양화 재판독과 학술 발표를 위하여 행하는
코드화·비식별화 처리는 이 구분에 따라 여전히 개인정보 처리에 해당하므로,
해당 데이터의 국외이전은 ‘이미 비식별화되었다’는 이유로 규제에서 벗어나는
것이 아니라 여전히 안전평가의 틀에 편입되어야 한다. 이것이 의료 임상연구
상황의 특유 규칙 중 하나이다. 본 사건에서 가공 후 데이터의 재연계 가능성
키의 보관 위치, 비식별화와 익명화의 구체적 경계는 공개 경로에 밝혀져 있지
않다.⁴²

전송 단계(국내). 본 사건은 병원 내부 각 정보시스템 사이, 병원과 연구협력
플랫폼 사이의 국내 데이터 전송을 수반한다. 본 단계에는 등급보호 2.0 의
전송 안전에 대한 기술요구(암호화, 무결성 검증, 신원인증)와 「의료보건기관
네트워크안전 관리방법」이 적용된다. 공식 공개에 따르면 병원의 안전방어
기술능력은 등급보호 등 표준규범에 부합하며, 이는 전송 단계가 등급보호

⁴²夏庆锋：《个人信息匿名化制度的反思与改进》，载《财经法学》2024 年第 5 期，第 41—58 页 참조.

2.0의 기술요구를 충족함을 의미한다.

제공 단계(국내+국외). 본 단계는 본 사건의 핵심 단계이다. 국내 제공자는 베이징우의병원이고, 국외 수령자는 COLOR III에서는 Amsterdam UMC이며, COLOR IV에서는 비교적 명확한 것이 Amsterdam UMC와 중앙화 데이터시스템 관리자이고, 그 밖의 국제 참여기관이 중국 측 피험자의 개인 수준 데이터에 접근할 수 있는지는 공개자료에 밝혀져 있지 않다. 국내 제공에는 PIPL 제 23조(타인에게 개인정보를 제공하는 경우 수령자를 고지하고 단독 동의를 취득)가 적용된다. 국외 제공에는 PIPL 제 38조~제 43조, 「데이터 국외이전 안전평가 방법」, 「네트워크안전법」 제 37조 및 「데이터안전법」 제 31조가 적용된다. 본 사건은 PIPL 제 38조 제 1호의 국외이전 안전평가 경로를 적용하여 베이징시 인터넷정보판공실이 접수하고 국가인터넷정보판공실이 평가하였으며, 최종적으로 공시번호 20220001 사건으로 승인되었다. 본 사건의 구체적인 촉발 사유(「데이터 국외이전 안전평가 방법」 제 4조의 몇 호가 적용되었는지)와 평가 유효기간 만료 후의 처리 상황(원 규칙에 따르면 2024년 9월 만료, 2024년 3월 22일 시행된 「데이터 국경 간 이동 촉진 및 규범화 규정」 제 9조의 신규칙에 따르면 2025년 9월 만료이며, 본 연구 작성 시점인 2026년 5월 기준 어느 쪽이든 이미 만료)은 공개자료에 밝혀져 있지 않다.

공개 단계. 연구 결과는 학술논문의 형식으로 공개된다. COLOR III의 단기 결과는 2026년 3월 The Lancet Gastroenterology & Hepatology에 정식 게재되었고(OncoDaily 등 학술 매체가 동시 보도), 전 세계 28개 센터에서 총 1,103명의 환자가 무작위 등록되었다.⁴³ COLOR IV의 연구 협약은 2025년 2월 Surgical Endoscopy지에 정식 게재되었다. 본 단계에는 PIPL 제 25조(처리자는

⁴³Tuynman JB, Yao H, Moolenaar LR, et al. Transanal total mesorectal excision versus laparoscopic total mesorectal excision for mid and low rectal cancer (COLOR III): short-term outcomes of an international, multicentre, phase 3, randomised, controlled, non-inferiority trial. Lancet Gastroenterol Hepatol. 2026 참조. 동 연구는 전 세계 28개 병원에서 수행되었다.

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

처리하는 개인정보를 공개하여서는 아니 되나, 개인의 단독 동의를 취득한 경우는 예외)가 적용된다. 학술 발표의 통상적 관행에 따라 본 사건 데이터는 집계 통계와 비식별화된 증례의 형식으로 제시되며 개인 신원정보를 직접 공개하지 않는다.

삭제 단계. 본 사건의 데이터 삭제 메커니즘은 공개자료에 밝혀져 있지 않다. 본 단계에는 PIPL 제 47 조(삭제 의무의 다섯 가지 사유)와 임상연구 분야의 특별 보존기간 규칙이 적용된다. 「약물 임상시험 품질관리규범」 제 80 조에 따르면 임상연구의 필수문서는 시험약물의 시판 승인 후 5 년 또는 임상시험 종료 후 5 년까지 보존하여야 하며, 다기관·복수 법역에 걸친 장기 연구에서는 서로 다른 법역의 요건을 중첩적으로 충족하여야 하므로 규제 점검과 과학적 재검증에 대비하여 실제 보존기간이 연구 종료 후 10 년 이상으로 연장되는 경우가 많다. 이로부터 의료 상황 특유의, 규범을 가로지르는 긴장이 형성된다. 즉 피험자가 PIPL 에 따라 가지는 동의 철회권·삭제청구권과 임상연구 규범의 장기 보존의무가 적용상 교차하는 것인데, 그 연계 경로는 PIPL 제 47 조 제2항에 있다. 법정 또는 규범상의 보존기간이 만료되지 않은 때에는 처리자는 즉시 삭제할 것이 아니라 저장과 필요한 안전보호 조치 이외의 처리를 중지하여야 한다.⁴⁴

3. 국외이전 단계와 상류 단계의 의존관계

⁴⁴ 「약물 임상시험 품질관리규범」(2020 년) 제 80 조는, 의약품 등록 신청에 사용되는 임상시험의 필수문서는 시험약물의 시판 승인 후 적어도 5 년까지, 등록 신청에 사용되지 아니한 임상시험의 필수문서는 시험 종료 후 적어도 5 년까지 보존하도록 규정한다. ICH-GCP E6(R2) §5.5.11 도 의뢰자에게 필수문서를 해당 지역에서 시험약물이 시판 승인된 후 적어도 2 년 또는 임상개발의 공식 종료 후 적어도 2 년까지 보존할 것을 요구한다. 다기관·복수 법역에 걸친 장기 임상연구는 서로 다른 법역의 최장 보존요건을 동시에 충족하여야 하므로, 실무상 보존기간이 연구 종료 후 10 년 이상으로 연장되는 경우가 많다.

본 사건의 국외이전 행위는 ‘제공 단계’의 특수한 형태에 속한다. 그러나 국외이전 단계의 컴플라이언스 의무 이행은 상류 단계의 컴플라이언스 품질에 의존한다. 수집 단계에서 유효한 동의를 취득하지 못하면 국외이전 단계에서 이를 보완할 수 없고, 저장 단계에서 역내 저장과 안전보호를 실현하지 못하면 국외이전 안전평가를 통과하기 어려우며, 가공 단계에서 진정한 익명화를 실현하지 못하면 국외이전 데이터는 여전히 PIPL 의 모든 구속을 받는다. 이러한 ‘상류 컴플라이언스가 하류 컴플라이언스를 결정하는’ 사슬형 의존관계는, 국외이전 안전평가가 사실상 국외이전 자체만이 아니라 처리자 전체의 컴플라이언스 수준을 간접적으로 평가하는 것임을 결정짓는다.⁴⁵

베이징시 보건위생위원회 공식 홈페이지가 공개한 병원의 신고 준비 업무(병원 과학기술처 평가, 병원 정보센터 평가, 병원 내부 「데이터 국외이전 안전관리방법」의 제정)는 실제로 전생애주기 상류 단계 컴플라이언스 품질에 대한 사전 보장이다. 이러한 ‘먼저 내부 심사, 다음에 외부 신고’의 절차 모델이 본 사건 컴플라이언스 설계의 핵심 특징을 구성한다.

4.8 개 단계의 적용규범 매트릭스

	수집	저장	사용	가공	전송	제공(국외이 전 포함)	공개	삭제
PIPL	☐	☐	☐	☐	☐	☐ (핵심)	☐	☐
「데이터안전법」	☐	☐	☐	☐	☐	☐ (핵심)	☐	☐
「네트워크안전법」/등급보 호제도	☐	☐	☐	☐	☐	☐	☐	☐

⁴⁵刘权：《论个人信息保护影响评估——以〈个人信息保护法〉第55、56条为中心》，载《上海交通大学学报（哲学社会科学版）》2022年第5期，第39—50页 참조.

	수집	저장	사용	가공	전송	제공(국외이전 포함)	공개	삭제
건강의료빅데이터 방법	□	□	□	□	□	□	□	□
의료보건기관	□	□	□	□	□	□	□	□
네트워크안전 관리방법								
데이터 국외이전						□(핵심)		
안전평가 방법								
윤리심사방법(11 호령/2023년 방법)	□	○	□	□	○	□	□	□
약물 임상시험	○	○	○	○	○	○	○	○
품질관리규범(참조적용)								
인류유전자원관리조례	□	□	□	□	□	□	○	○

주: □는 직접 적용, ○는 간접 적용을 표시한다.

본 표는 본 사건의 전생애주기 컴플라이언스가 적어도 아홉 층위 규범의 병행적용을 수반함을 보여준다. 규범 층수에서 보면 제공(국외이전 포함) 단계에 적용되는 규범이 가장 많아 법률 층위, 행정법규 층위, 부문규장 층위, 국가표준 층위, 업종규장 층위와 임상연구 특별규장을 아우른다. 핵심 단계에서 보면 제공(국외이전 포함) 단계가 본 사건 컴플라이언스의 핵심을 구성하나, 동시에 수집 단계가 피험자 동의 문제와 관련되어 컴플라이언스 품질의 원천이 된다.

VII. 본 사건 데이터 국외이전의 관할과 법적 책임

앞의 각 장에서는 본 사건 데이터가 어떻게 분류등급되고, 병원이 어떻게 내부 식별을 이행하며, 각 제도가 등급보호와 전생애주기의 차원에서 어떻게

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

전개되는지를 분석하였다. 그러나 제도의 실효성은 결국 하나의 물음에 달려 있다. 즉 데이터 국외이전 단계에서 위법이 발생하면 누가, 어떤 규범에 의하여, 어떤 책임을 부과하는가이다. 본 사건의 데이터는 베이징우의병원에서 암스테르담 UMC 로 이전되어 중국과 EU 의 두 법역을 가로지르므로, 규제관할은 단일 국가 내부의 문제가 아니라 중국과 EU 두 규제체계의 교차 문제가 된다. 본 장에서는 먼저 중국 측의 규제관할과 법적 책임을 정리하고, 다음으로 EU·네덜란드 측의 국외 수령자에 대한 관할을 분석하며, 마지막으로 두 관할체계의 교차와 충돌의 핵심 문제 — 특히 데이터 주권을 배경으로 한 국경 간 사법적 데이터 제출요구의 충돌 — 에 초점을 맞춘다. 평가의 구조에서 본 장은 평가사항 중 국외 수령자 소재 법역의 법률환경에 대한 심사 차원에 대응한다.

1. 중국 측의 규제관할과 법적 책임

중국 측의 규제관할은 국내 데이터 이전 주체(즉 베이징우의병원)를 대상으로 하며, ‘인터넷정보 부서의 총괄, 산업 주관부서의 분담’이라는 다원적 구조를 보이고, 위법행위의 성질에 따라 서로 다른 주관기관과 벌칙이 대응한다.

첫째, 데이터 국외이전 안전평가 의무 위반은 인터넷정보 부서가 관할한다. 본 사건의 데이터 국외이전은 베이징시 인터넷정보판공실에 안전평가를 신고하였으며, 지방 인터넷정보 부서가 제 1 선 규제기관이고 국가 인터넷정보 부서가 총괄·조정을 담당한다. 데이터 처리자가 평가 없이 국외이전하거나 평가의 범위를 넘어 국외이전하는 경우에는 「데이터안전법」, 「개인정보보호법」 및 「데이터 국외이전 안전평가 방법」에 따라 책임을 진다.

둘째, 데이터안전 보호의무·중요데이터 관리의무 위반은 관련 주관부서가 관할한다. 「데이터안전법」 제 45 조에 따르면, 데이터 처리활동을 수행하는 조직·개인이 동 법 제27조, 제29조, 제30조가 규정하는 데이터안전 보호의무를

이행하지 아니하는 경우 관련 주관부서가 시정을 명하고 경고하며 5 만 위안 이상 50 만 위안 이하의 벌금을 병과할 수 있고, 시정을 거부하거나 대량의 데이터 유출 등 중대한 결과를 초래한 경우에는 50 만 위안 이상 200 만 위안 이하의 벌금에 처하며, 관련 업무의 정지, 영업정지·정돈, 관련 업무허가증 또는 영업집조의 취소를 명할 수 있다.⁴⁶ 의료업종에 관하여는 보건위생 주관부서가 해당 업종 내에서 데이터안전 규제 직책을 담당하며, 이는 제4장·제5장에서 본 ‘산업 측’ 분류등급 절차와 연계된다. 즉 분류등급의 산업 주관부서가 동시에 상응하는 집행 주관부서이기도 하다.

셋째, 개인정보 보호의무 위반은 개인정보보호 직책을 이행하는 부서가 관할한다. 「개인정보보호법」 제 60 조에 따르면 국가 인터넷정보 부서가 개인정보보호 업무의 총괄·조정을 담당하고, 국무원 관련 부서가 각자의 직책 범위에서 감독관리를 담당하며, 현급 이상 지방인민정부의 관련 부서는 국가의 규정에 따라 직책을 확정하는데, 이 셋을 합하여 ‘개인정보보호 직책을 이행하는 부서’라 한다. 벌칙에 관하여는 동 법 제 66 조에 따라, 위법하게 개인정보를 처리하거나 보호의무를 이행하지 아니한 경우 개인정보보호 직책을 이행하는 부서가 시정 명령, 경고, 위법소득의 몰수를 하고 시정을 거부하면 100 만 위안 이하의 벌금을 병과하며, 정상이 중한 경우에는 성급 이상 부서가 시정을 명하고 위법소득을 몰수하며 5,000 만 위안 이하 또는 전년도 매출액 100 분의 5 이하의 벌금에 처하고, 관련 업무의 정지·영업정지 정돈·허가 또는 영업집조의 취소를 명할 수 있으며, 직접 책임이 있는 주관자에게는 10 만 위안 이상 100 만 위안 이하의 벌금에 처하고 일정 기간의 취업제한을 결정할 수 있다. 본 사건은 민감개인정보를 처리하고 국외에 제공하므로 제 66 조의 규율

⁴⁶ 「데이터안전법」 제 45 조 제 1 항. 국가핵심데이터 관리제도를 위반하여 국가의 주권·안전과 발전이익을 위해한 경우에는 동 조 제 2 항에 따라 200 만 위안 이상 1,000 만 위안 이하의 벌금에 처하고, 상황에 따라 영업정지·정돈, 관련 업무허가증 또는 영업집조의 취소를 명하며, 범죄를 구성하는 경우 법에 따라 형사책임을 추궁한다.

범위에 속한다.

넷째, 인류유전자원이 관련되는 경우에는 과학기술 주관부서가 관할한다. 「인류유전자원관리조례」에 따르면 인류유전자원의 채집·보존·이용·국외제공은 국가 과학기술 주관부서가 심사·규제한다. 다만 제 4 장에서 본 바와 같이 본 사건 데이터는 식별 결과 인류유전자원정보를 구성하지 않으므로 본 사건은 과학기술 주관부서의 인류유전자원 심사·처벌 궤도에 들어가지 않는다. 이러한 관할의 배제는 바로 제 4 장의 인류유전자원정보 배제 판단이 집행 차원으로 연장된 것이다.

종합하면, 중국 측의 규제관할은 ‘총괄 더하기 분담’의 구조적 특징을 보인다. 인터넷정보 부서가 데이터 국외이전과 개인정보보호를 총괄하고, 보건위생 주관부서가 업종별 분담에 따라 규제하며, 과학기술 주관부서가 인류유전자원을 전담한다. 이 구조는 본 사건 분류등급의 ‘산업 측/처리자 측’ 이중 절차와 서로 호응한다. 데이터 등급을 식별하는 주체가 흔히 상응하는 집행 주체이기도 한 것이다. 그 공통된 특징은, 중국 측 규제관할의 대상이 언제나 국내 이전 주체인 베이징우의병원이고, 규제 수단은 사전 안전평가, 국외이전 계약상 의무의 설정, 그리고 사후 이전 주체에 대한 책임 추궁이라는 점이다.

2. EU·네덜란드 측의 규제관할

데이터가 암스테르담 UMC 로 이전된 후에는 곧 EU 「일반개인정보보호규정」(GDPR)의 관할 범위에 들어간다. 본 사건의 국외 수령자인 UMC 는 네덜란드에 소재하며, 그 관할은 다음의 특징을 보인다.

관할기관의 측면에서, 네덜란드 데이터보호청(Autoriteit Persoonsgegevens, AP)이 네덜란드 역내의 주관 감독기관이다. 데이터 처리가 복수의 회원국에 관련되는 경우에는 주도 감독기관을 중심으로 하는 일관성

메커니즘(유럽데이터보호이사회 EDPB 가 조정)이 추가로 존재하여 GDPR 의 EU 역내 통일적 적용을 보장한다.

관할 근거의 측면에서, GDPR 제 3 조는 속지주의와 표적지향을 결합한 적용범위를 확립한다. EU 역내에 설립된 컨트롤러 또는 프로세서가 처리활동을 수행하는 한, 처리행위가 어디에서 이루어지는지를 불문하고 GDPR 이 적용된다.⁴⁷ 암스테르담 UMC 는 네덜란드에 설립된 기관으로서 본 사건 데이터에 대한 그 처리는 GDPR 의 관할을 직접 받는다.

벌칙의 측면에서, GDPR 제 83 조는 2 단계 행정 과징금 체계를 둔다. 비교적 가벼운 위반에는 최고 1,000 만 유로 또는 직전 회계연도 전 세계 매출액의 2%(둘 중 높은 금액)까지, 비교적 무거운 위반(처리의 기본원칙, 정보주체의 권리, 제 3 국 이전 규정의 위반 등)에는 최고 2,000 만 유로 또는 전 세계 매출액의 4%(둘 중 높은 금액)까지 부과할 수 있다.⁴⁸ 이에 따라 UMC 가 EU 역내에서 행하는 본 사건 데이터의 처리(처리의 적법성 근거, 정보주체 권리의 보장, 재이전 제한 등 포함)는 GDPR 의 요건을 독립적으로 충족하여야 하며, 그렇지 못하면 네덜란드 AP 의 제재에 직면한다.

강조할 점은, GDPR 의 UMC 에 대한 관할과 중국 측의 데이터 국외이전 안전평가는 서로 독립된 두 갈래의 컴플라이언스 심사라는 것이다. 중국 측은 데이터가 ‘국외로 나갈 수 있는지, 어떤 조건으로 나가는지’를 심사하고, EU 측은 데이터가 들어온 후 ‘수령자의 처리가 적법한지’를 심사한다. 동일한 데이터 이동이 이로써 이전지와 수령지의 두 규범체계에 동시에 구속되며, 양자는 기준이 다르고 서로 독립적이며 서로를 대체하지 않는다.

⁴⁷GDPR Article 3 (Territorial scope). EU 역내에 설립된 컨트롤러·프로세서의 처리활동에는 처리가 EU 역내에서 이루어지는지를 불문하고 동 규정이 적용된다.

⁴⁸GDPR Article 83(4)(5). 2 단계 과징금: 상한은 각각 1,000 만 유로 또는 전 세계 연간 매출액의 2%, 2,000 만 유로 또는 전 세계 연간 매출액의 4% 중 높은 금액이다.

3. 두 관할체계의 교착과 충돌

본 사건의 데이터 국외이전은 중국과 EU 의 두 법역을 가로지르며, 두 규제관할은 단순히 포개지는 것이 아니라 연결 지점에서 교착과 잠재적 충돌을 낳는다.

첫째, 이중 컴플라이언스와 상호 불승인. 앞서 본 바와 같이 중국 측의 데이터 국외이전 안전평가와 EU 측의 GDPR 컴플라이언스는 서로 독립된 두 심사이므로, 중국 측 평가의 통과가 EU 측 의무를 면제하지 않으며 그 역도 마찬가지이다. 베이징우의병원과 암스테르담 UMC 의 협력은 실제로 양쪽의 요건을 동시에 충족하여야 하며, 이는 국경 간 의료데이터 협력의 이중 컴플라이언스 부담을 구성한다.

둘째, 관할의 ‘중첩’이 아닌 ‘릴레이’. 중국 측의 규제관할은 데이터의 국외이전 시점까지 미치며 그 대상은 국내 이전 주체이고, EU 측의 관할은 데이터의 역내 유입 시점부터 시작되며 그 대상은 국외 수령자이다. 두 구간의 관할을 잇는 것은 데이터 국외이전 계약(개인정보 국외이전 표준계약 등)으로서, 데이터보호 의무를 이전 주체로부터 수령자에게 ‘릴레이’식으로 전달한다. 중국 규제기관은 네덜란드에 소재한 UMC 에 대하여 직접적인 집행 능력을 가지지 못하며, 계약상 약정된 의무와 국내 이전 주체에 대한 책임 추구를 통하여 국외 처리 단계에 대한 관할을 간접적으로 실현할 수 있을 뿐이다. 이것이 데이터 국경 간 규제의 구조적 한계이다.

셋째, 방향성의 구분 — GDPR 국경 간 이전 규칙의 본 사건에서의 적용 한계. GDPR 제 45 조의 적정성 결정과 제 46 조의 표준계약조항(SCC) 등 적절한 보호조치는 EU 에서 제 3 국으로의 데이터 이전을 규율한다. 본 사건의 ‘중국에서 EU 로’라는 기본 흐름에 관하여 보면, UMC 가 본 사건 데이터를 수령하여 EU 역내에서 처리하는 데 따른 의무는 주로 GDPR 의 일반 처리규칙과 특수 범주 데이터 처리에 관한 규정(적법한 처리 근거, 과학연구

마봉초- 중국 의료데이터 국외이전 규제에 관한 연구

예외, 정보주체의 권리와 안전 의무 등)에서 나오며, GDPR 제 5 장의 국경 간 이전 수단에서 나오는 것이 아니다. 다만 UMC 가 본 사건 데이터를 중국으로 회송하거나 다른 비 EU 법역으로 재이전하는 경우에는 GDPR 제 5 장의 국경 간 이전 규칙이 별도로 촉발되며, 그때에는 EU 와 중국 사이에 적정성 결정이 존재하지 않으므로 SCC 등 적절한 보호조치로 연계하여야 하고 컴플라이언스 비용과 불확실성이 그만큼 높아진다.⁴⁹

넷째, 국경 간 사법적 데이터 제출요구의 충돌 — 데이터 주권을 배경으로 한 두 관할의 정면 충돌. 이는 두 관할체계의 교차 중 가장 첨예한 문제로서 상세히 분석할 필요가 있다. 한편으로 「데이터안전법」 제 36 조는, 중화인민공화국의 주관기관은 관련 법률과 체결·가입한 국제조약·협정에 따라, 또는 평등호혜의 원칙에 따라 외국 사법기관 또는 집행기관의 데이터 제공 요청을 처리하며, 중화인민공화국 주관기관의 비준 없이 역내의 조직·개인은 외국 사법기관 또는 집행기관에 중화인민공화국 역내에 저장된 데이터를 제공하여서는 아니 된다고 규정한다. 「개인정보보호법」 제 41 조는 평행 규정을 두어 개인정보 분야의 대응 차단조항을 구성한다. 이 두 조항은 중국의 ‘차단조항(Blocking Provision)’이라 불리는데, 그 입법 의도는 일부 국가가 국제사법공조를 우회하여 국내법으로 자국 기관에 국외 데이터를 강제로 취득할 권한을 부여하는 것에 대응하여, 사전 비준을 설정함으로써 타국의 역외관할을 차단하는 데 있다.⁵⁰

⁴⁹본 연구 작성 시점까지 EU 집행위원회는 중국에 대하여 GDPR 제 45 조 의미의 적정성 결정을 내린 바 없다. 동 결정과 제 46 조의 적절한 보호조치는 EU 에서 제 3 국으로의 데이터 이전을 대상으로 한다. 따라서 EU 측에서 중국으로의 회송 또는 재이전이 발생하는 경우에만 표준계약조항(SCC) 등 제 46 조 소정의 적절한 보호조치에 의한 연계가 필요하며, 본 사건의 ‘중국에서 EU 로’라는 기본 흐름은 이를 국외이전의 근거로 하지 않는다.

⁵⁰ 中伦律师事务所: 《数据安全, 国之重器——〈数据安全法〉第三十六条的适用与合规应对》, 2022 年 참조. 「개인정보보호법」 제 41 조는 평행 규정을 두며, 양자를 합하여 ‘차단조항(Blocking Provision)’이라 부른다.

이 차단조항 위반의 법적 책임은 명확하다. 「데이터안전법」 제 48 조 제 2 항에 따르면, 제 36 조를 위반하여 주관기관의 비준 없이 외국 사법기관 또는 집행기관에 데이터를 제공한 경우 관련 주관부서가 경고하고 10 만 위안 이상 100 만 위안 이하의 벌금을 병과할 수 있으며, 중대한 결과를 초래한 경우에는 100 만 위안 이상 500 만 위안 이하의 벌금에 처하고 관련 업무의 정지, 영업정지·정돈, 관련 업무허가증 또는 영업집조의 취소를 명할 수 있다.

다른 한편으로 EU 측에는 거울상의 규정이 존재한다. GDPR 제 48 조는, 제 3 국의 법원 또는 행정기관이 컨트롤러 또는 프로세서에게 개인데이터의 이전 또는 공개를 요구하는 판결·결정은 그것이 요청국과 EU 또는 회원국 사이의 국제협정(사법공조조약 등)에 기초하는 경우에 한하여 승인되거나 집행될 수 있다고 규정한다. 바꾸어 말하면 EU 도 국제협정의 틀을 거치지 않은 외국(중국 포함)의 직접적인 제출요구를 승인하지 않는다. 이로써 중국과 EU 양측은 각각 ‘자기 측의 비준 또는 국제협정 없이는 상대방 사법·집행기관에 데이터를 제공할 수 없다’는 규칙을 두어 데이터 주권 차원의 쌍방향 차단을 형성한다.

이 충돌의 현실적 의의는 다음과 같다. 어느 한쪽의 사법기관 또는 집행기관이 본 사건 데이터의 제출을 요구하는데 그 데이터가 상대방 역내에 저장되어 있는 경우, 데이터 보유자는 ‘한쪽은 제공을 요구하고 다른 쪽은 제공을 금지하는’ 법적 곤경에 동시에 직면하게 된다. 본 사건의 베이징우의병원과 암스테르담 UMC 의 장기 임상연구 협력에서는 데이터가 중국과 EU 양쪽에 분산되어 있으므로, 어느 한쪽에서 소송, 규제 조사 또는 집행 절차가 발생하여 상대방 역내의 데이터 제출이 필요해지면 위 충돌이 촉발될 수 있다. 본 사건의 공개자료에는 그러한 상황이 발생하였다는 기록이 없으나, 국경 간 의료데이터 협력의 구조적 위험으로서 그것은 두 규제관할이 데이터 주권 차원에서 피할 수 없는 잠재적 충돌 지점을 구성한다.

4. 본 사건 규제관할의 전체상

위 분석을 종합하면, 본 사건 베이징우의병원과 암스테르담 UMC 의 데이터 국외이전은 ‘중국 측은 국외이전을 관할하고, EU 측은 유입을 관할하며, 계약이 릴레이하고, 사법적 제출요구의 충돌은 미해결로 유보된’ 관할 상태에 놓여 있다. 중국 측은 인터넷정보 부서의 총괄과 보건위생 주관부서의 분담이라는 구조로 국내 이전 주체인 베이징우의병원에 대하여 사전 평가와 사후 책임 추궁을 시행하고, EU 측은 네덜란드 AP 를 주관기관으로 하여 GDPR 에 따라 국외 수령자 UMC 의 유입 후 처리를 규제하며, 두 구간의 관할은 데이터 국외이전 계약으로 연결되나, 적정성 결정이 없고 쌍방향 차단조항이 존재하는 상황에서 그 연결 지점에는 이중 컴플라이언스 부담과 잠재적인 사법적 제출요구 충돌이 상존한다.

이 관할의 전체상은 본 연구가 거듭 드러내 온 특징을 확인하여 준다. 의료데이터 국경 간 이전이라는 신흥 영역에서 규범 공급은 날로 완비되어 가나, 법역을 가로지르는 관할 조정 메커니즘은 여전히 성숙하지 못하였다. 본 사건 데이터 국외이전의 컴플라이언스는 분류등급, 안전평가 등 실체 제도의 적용 문제일 뿐만 아니라, 통일된 조정 틀이 없는 가운데 두 독립된 규제관할이 병행하여 작동하는 문제이기도 하다. 이 구조적 특징이 본 연구가 결론 부분에서 더 논의할 기초를 구성한다.

VIII. 결론과 전망

1. 연구의 회고와 본 사건의 표본가치

본 연구는 베이징우의병원과 Amsterdam UMC 가 협력한 국제 다기관 임상연구(COLOR III, COLOR IV)를 분석대상으로 하여, 공시번호 20220001 사건을 둘러싸고 ‘사실을 먼저, 규범을 나중’이라는 체계적 정리를 수행하였다. 본 사건의 사실 층위는 2017 년 COLOR IV 중국 측 재원의 과제 선정부터

2030 년 COLOR IV 의 완료 예정까지 13 년의 시간 폭에 걸치며, 중국 데이터 거버넌스 체계가 무에서 유로 구축된 전 기간을 가로지른다. 본 사건의 규범 층위는 법률, 행정법규, 부문규장, 국가표준과 지방규범의 다섯 규범 층위에 걸치며, 각 시기에 적용되는 규범의 차이가 본 사건 컴플라이언스 판단의 핵심 난점을 구성한다.

본 사건은 「데이터 국외이전 안전평가 방법」 시행 이래 전국 최초로 데이터 국외이전 안전평가를 통과한 사례로서 규칙 구축기의 표본가치를 가진다. 본 사건의 ‘컴플라이언스 통과’는 이 제도가 의료 분야에서 처음으로 실무 운용된 것이자, 이후 동종 사건의 컴플라이언스 판단에 사실적 참조를 제공한다. 본 연구가 지금까지 수행한 작업은 본 사건의 사실과 규범을 온전히 정리하는 것으로서, 컴플라이언스 판단도 위법 판단도 정책 제언도 하지 않는다. 다만 사실 층위의 제시는 자연스럽게 몇 가지 이론적 문제를 도출하므로, 본 장에서는 사실의 기초 위에서 초보적 분석을 하고 다음 단계의 연구 방향을 밝힌다.

2. 본 사건의 사실 제시가 도출하는 핵심 발견

이하의 다섯 발견은 ‘사실 관찰(발견 1, 2) — 제도 문제(발견 3, 4) — 이론적 구분(발견 5)’의 층위로 점층하며, 서론에서 제시한 핵심 논지를 함께 뒷받침한다. 첫째, 본 사건은 ‘병원 내부 선행 심사, 규제 외부 최종 평가’라는 실무 컴플라이언스 모델을 보여준다(제 2 장과 제 4 장에서 상술). 본 연구 제 2 장에서 규명한 사실에 따르면, 베이징우의병원은 베이징시 인터넷정보판공실에 신고하기 전에 세 국면의 병원 내부 심사를 완료하였다. 즉 병원 과학기술처가 프로젝트의 과학적 의의와 인류유전자원 상황을 내부 평가하였고, 병원 정보센터가 네트워크안전·데이터안전을 다시 평가하여

등급보호 등 표준규범에 부합함을 확인하였으며, 병원이 내부 「데이터 국외이전 안전관리방법」을 제정하고 “중요데이터 국외이전의 심사 메커니즘, 평가 메커니즘, 감독 메커니즘”의 수립을 명확히 하였다. 이 ‘3 국면 내부 심사’는 사실 차원에서 데이터 국외이전 안전평가의 선행적 품질보장을 구성한다. 최초 사례로서 본 사건의 내부 심사 모델은 이후 동종 신고에 관찰 가능한 실무 참조를 제공한다. 그러나 이러한 ‘실무 선행형’ 컴플라이언스 모델은 구조적 의존성을 가진다. 규제의 최종 평가가 실질적으로 병원 내부 심사의 컴플라이언스 품질에 의존하는 것이다. 병원 내부 심사의 구체적 내용, 심사 결론, 부적합 사항의 시정 상황이 모두 공개 경로에 밝혀져 있지 않은 상황에서, 규제의 국내 측 안전수준 평가가 구체적으로 어떻게 작동하는지는 아직 충분히 관찰되지 못한 컴플라이언스 문제로 남는다.

둘째, 본 사건은 ‘개인정보 유형 × 국외이전 시나리오 × 조합적용 논리’의 실무 작동 양상을 구체적으로 보여준다(제4장과 제6장에서 상술). 정보 유형의 축에서, 본 사건 데이터는 일반개인정보(환자의 기본 신원정보), 민감개인정보(PIPL 제 28 조에 따른 의료건강류와 주민신분증번호), 그리고 데이터 차원에서 ‘중요데이터’ 해당 여부가 식별 대기 중인 상황을 포괄한다. 국경 간 시나리오의 축에서, 본 사건은 COLOR III 의 ‘국외 의뢰자 주도·중국 측 참여’와 COLOR IV 의 ‘중국 측 의뢰자 주도·국외 참여’라는 상반된 두 시나리오 구조를 보여주는데, 양자 모두 중국 데이터 국외이전 규제의 범위에 포섭된다. 이는 본 사건의 국경 간 시나리오 판단이 의뢰자의 신원이 아니라 ‘데이터가 실제로 국경을 넘어 전송되는가’를 기준으로 함을 보여준다. 조합적용의 논리에서, 본 사건은 개인정보 차원의 컴플라이언스 근거(PIPL 제 38 조·제 39 조, 윤리심사방법, 상호인정연맹 규칙)와 데이터 차원의 컴플라이언스 근거(DSL 제 21 조, 안전평가방법 제 4 조 제 2 호, 베이징 자유무역시험구 네거티브리스트)가 병행하는 두 판단 틀을 구성하고, 양자가

‘의료건강류 민감개인정보’라는 교집합 필드에서 중첩적용 관계를 넣음을 보여준다. 이러한 ‘두 축 병행·교집합 중첩’의 조합 판단 구조는 본 사건의 사실 층위가 객관적으로 드러내는 실무 양상이자, 의료데이터 국외이전 규제가 현행 규범체계에서 구체적으로 전개되는 형식이다.

셋째, 본 사건은 평가 유효기간 메커니즘과 장기 임상연구 사이의 구조적 긴장을 드러낸다. 「데이터 국외이전 안전평가 방법」 제 14 조에 따라 평가 유효기간은 본래 2 년이었고, 2024 년 3 월 22 일 시행된 「데이터 국경 간 이동 촉진 및 규범화 규정」 제 9 조에 따라 유효기간은 3 년으로 연장되었다. 본 사건의 COLOR IV 는 2030 년까지 지속될 예정이고 COLOR III 의 장기 생존율 추적관찰도 여러 해 계속된다. 그런데 본 사건의 심사는 2022 년 9 월부터 2023 년 초에 통과되었으므로, 원래의 2 년 규칙에 따르면 평가 유효기간은 2024 년 9 월에 이미 만료되었고(약 1 년 8 개월 경과), 새로운 3 년 규칙으로 추산하더라도 약 2025 년 9 월에 만료되었다(승인 시점 기준, 약 8 개월 경과). 2026 년 5 월 시점에 본 사건의 컴플라이언스 지속 상태는 공개 경로에 밝혀져 있지 않다. 임상연구의 실제 주기(ICH-GCP 의 통상 실무에 따르면 데이터 보존기간은 연구 종료 후 10~15 년)와 규제 평가의 유효기간(2~3 년) 사이에는 몇 배에서 수십 배에 이르는 시간적 차이가 존재한다. 이러한 구조적 긴장은, 장기 임상연구가 평가 유효기간 만료 후 필연적으로 재신고 또는 평가 연장의 컴플라이언스 의무에 직면하며, 그 시점에 적용되는 규범상태가 이미 실질적으로 변화하였을 수 있음(본 사건 심사 시에는 존재하지 않았던 2024 년 베이징 자유무역시험구 의약산업 중요데이터 네거티브리스트, GB/T 43697-2024 데이터 분류등급 규칙 등)을 의미한다. 본 사건의 컴플라이언스 지속 문제는 이로써 평가제도 자체가 장기 임상연구라는 상황에서 응답하여야 할 실무적·이론적 문제가 된다.

넷째, 본 사건은 다중 규범의 병행적용 속 연계 공백을 보여준다. 본 사건은

적어도 아홉 층위 규범의 병행적용을 수반한다(제 6 장의 8 개 단계 적용규범 매트릭스에서 상술). 인간 대상 연구의 윤리심사 차원에서는 11 호령(심사 시 적용)과 国卫科教发[2023]4 号 방법(컴플라이언스 지속 단계 적용)이 병존하고, 병원 네트워크안전 차원에서는 등급보호 2.0(GB/T 22239-2019)과 「의료보건기관 네트워크안전 관리방법」이 병존하며, 데이터 국외이전 차원에서는 안전평가방법(첫 번째 경로)과 「데이터 국경 간 이동 촉진 및 규범화 규정」, 베이징 자유무역시험구 네거티브리스트가 병존한다. 각 규범은 각자의 범위에서 전개되나, 규범들 사이의 연계 관계 — 윤리심사의 ‘상호인정’ 메커니즘과 국경 간 데이터 국외이전의 ‘독립 심사’를 어떻게 구분할 것인지, 병원 등급보호 컴플라이언스와 데이터 국외이전 안전평가의 사실적 승계, 병원 내부 방법과 규제 외부 평가의 효력 관계 — 는 아직 규범 차원에서 명확히 처리되지 않았다. 본 사건의 실무 운용은 사실상 병원과 규제기관의 구체적 상호작용을 통하여 이러한 연계 공백을 메운 것이나, 그 메움의 구체적 경로는 공개되지 않았다.

다섯째, 본 사건은 ‘컴플라이언스 통과’와 ‘지속적 컴플라이언스’의 경계, ‘미공개’와 ‘위법’의 경계라는 두 핵심 이론 문제를 도출한다. 본 사건이 국가인터넷정보판공실의 평가를 통과한 것은 확정된 사실이다. 그러나 평가 통과는 평가 시점의 컴플라이언스 수준에만 미치며, 평가 유효기간 내 컴플라이언스의 지속적 품질에는 미치지 않고, 평가 유효기간 만료 후의 컴플라이언스 상태에는 더더욱 미치지 않는다. 본 연구가 지적한 여러 ‘공개 경로에 밝혀지지 않은’ 사항 — 동의서의 구체적 내용, 병원 내부 방법의 전문, 등급보호 등급 결정 결과, 개인정보보호 영향평가 문서, 심사 통과의 정확한 시점, 컴플라이언스 지속 상태 등 — 은 본 연구 사실기반의 미지(未知) 부분을 구성하나, 미지 자체는 위법의 인정도 컴플라이언스의 인정도 구성하지 않는다. 본 사건은 이러한 이론적 구분에 구체적인 사실 소재를 제공한다. 평가

통과라는 ‘컴플라이언스 통과’를 미공개 사항이라는 ‘사실의 미지’와 어떻게 구분할 것인지, 평가 유효기간 만료 후의 ‘재평가 대기’ 상태를 ‘위법 운영’ 상태와 어떻게 구분할 것인지 — 이러한 구분은 평가 메커니즘 자체의 효력 범위에 대한 정밀한 이론 분석에 의존하며, 본 연구 다음 단계의 핵심 이론 문제이다. 허가의 시간적 효력에서 관찰하면, 평가 통과는 유효기간이 붙은 컴플라이언스 판정이다. 그 효력의 종기는 행정관리의 주기가 결정하는 반면 임상연구의 데이터 처리활동은 지속성을 가지므로, 양자의 시간 구조는 본래부터 어긋나 있다. 장기 국제 임상연구에 관하여 이는, 컴플라이언스 설계가 처음부터 ‘연장 — 재신고’를 연구 전 주기의 계획에 편입하여야 하며 평가 통과를 일회성 통관으로 보아서는 안 됨을 의미한다.

3. 향후 연구방향

본 연구가 취한 ‘사실을 먼저, 규범을 나중에’의 제시 방식은 방법론적 의의를 가진다. 중국의 데이터 국외이전 제도는 2021 년부터 2026 년 5 월까지 5 년 사이에 규칙의 구축에서 규칙의 세부화로 이어지는 밀도 높은 변동을 겪었으며, 그 과정에서 구체적 사건에 대한 사실의 제시를 규범에 대한 이론적 평가보다 앞세우는 것은 이론이 선입견의 틀로 사실 판단을 왜곡하는 것을 피하기 위한 필수적 경로이다. 본 연구가 지금까지 수행한 작업은 주로 사실의 제시에 속하며, 이론적 평가는 사실이 충분히 완전해진 기초 위에서 자연스럽게 떠올라야 한다. 최초 사례로서 본 사건의 표본가치는 바로 그 사실 제시가 이후 동종 사건의 이론 구축에 경험적 기초를 제공할 수 있다는 데 있다. 인정하여야 할 것은, 본 연구의 사실 층위에는 여전히 공개 경로에 밝혀지지 않은 몇 가지 핵심 사항이 남아 있다는 점이다. 이러한 미확인 사항이 본 연구의 객관적 한계를 구성한다.

본 사건의 사실 제시와 초보적 발견에 기초하여, 본 연구는 다음의 방향을 다음 단계의 연구 내용으로 확정한다.

첫째는 본 사건 핵심 사실의 확인 방향이다. 구체적으로는 베이징우의병원 자체 윤리위원회의 COLOR III·COLOR IV 심사에서의 실제 동의서 내용, 본 사건 심사 통과와 구체적 일자와 촉발 사유, 평가 유효기간 만료 후의 처리 상태, 병원 내부 「데이터 국외이전 안전관리방법」의 전문과 작동 메커니즘이 포함된다.

둘째는 국경 간 시나리오 유형화의 이론 구축 방향이다. 본 사건은 ‘두 축 병행·교집합 중첩’의 조합 판단 구조를 보여주었으나, 중국 데이터 국외이전 규제의 현행 규범체계는 아직 명확한 ‘정보 유형 × 국외이전 시나리오’의 2 차원 판단 매트릭스를 형성하지 못하였다. 다음 단계에서는 본 사건과 동종 사건의 사실 기초 위에서 의료데이터 국경 간 이전의 컴플라이언스 규칙을 추출하여 유형화 분석을 하여야 한다. 이는 의료데이터 국외이전 연구가 이론 구축의 차원에서 전개될 방향이다.

셋째는 한중 비교법의 전개 방향이다. 다음 단계에서는 중국법의 사실 기초가 충분히 완전해진 뒤에 한국 「개인정보 보호법」(PIPA)상의 의료데이터 국경 간 이전 규칙을 도입하여, ‘민감개인정보의 식별’, ‘국외이전 평가 메커니즘’, ‘윤리심사와 데이터 컴플라이언스의 연계’ 등 구체적 차원에서 양국을 체계적으로 비교하여야 한다. 한중 비교법의 전개가 본 연구 다음 단계의 핵심 방향이다.

참고문헌

외국어문헌

[중국어]

〈논문〉

丁晓东：《数据跨境流动的法理反思与制度重构——兼评〈数据出境安全评估办法〉》，载《行政法学研究》2023 年第 1 期。

洪延青：《国家安全视野中的数据分类分级保护》，载《中国法律评论》2021 年第 5 期。

刘权：《论个人信息保护影响评估——以〈个人信息保护法〉第 55、56 条为中心》，载《上海交通大学学报（哲学社会科学版）》2022 年第 5 期。

王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解
释为背景》，载《当代法学》2022 年第 1 期。

夏庆锋：《个人信息匿名化制度的反思与改进》，载《财经法学》2024 年第 5 期。

【영어】

〈논문〉

DEIJEN, C.L., et al., “COLOR III: a multicentre randomised clinical trial comparing transanal TME versus laparoscopic TME for mid and low rectal cancer,” 30 *Surgical Endoscopy*, 2016.

TUYNMAN, J.B., et al., “Transanal total mesorectal excision versus laparoscopic total mesorectal excision for mid and low rectal cancer (COLOR III): short-term outcomes of an international, multicentre, phase 3, randomised, controlled, non-inferiority trial,” *Lancet Gastroenterology & Hepatology*, 2026.

WU, S., et al., “COLOR IV: a multicenter randomized clinical trial comparing intracorporeal and extracorporeal ileocolic anastomosis after laparoscopic right colectomy for colon cancer,” 39 *Surgical Endoscopy*, 2025.

초 록

본 연구는 「데이터 국외이전 안전평가 방법」(2022 년 9 월 1 일 시행) 시행 이래 전국 최초로 데이터 국외이전 안전평가를 통과한 사건인 공시번호 20220001 사건을 분석대상으로 한다. 본 사건은 수도의과대학 부속 베이징우의병원과 네덜란드 암스테르담대학교 의학센터(Amsterdam UMC)의 국제 다기관 임상연구(COLOR III·COLOR IV)를 내용으로 한다. 본 연구는 “사실을 먼저, 규범을 나중에”라는 분석순서에 따라, 2017 년부터 2030 년에 이르는 본 사건의 객관적 사실관계를 먼저 정리한 후, 각 단계에 적용되는 중국법 규범을 법률·행정법규·부문규장·국가표준·지방성 규범의 5 개 위계에 따라 체계적으로 정리한다. 본 연구는 다음을 확인한다. 첫째, 본 사건은 “병원 내부 선행 심사, 규제 외부 최종 평가”라는 실무적 컴플라이언스 모델을 보여준다. 둘째, 평가 유효기간 메커니즘과 장기 임상연구 사이의 구조적 긴장, 다중 규범 병행적용에서의 연계 공백, 그리고 “컴플라이언스 통과와 지속적 컴플라이언스” 및 “미공개와 위법”의 경계라는 이론적 문제가 도출된다. 본 연구는 위법 판단이나 정책 제언을 내리지 않고 사실과 규범의 완전한 정리에 집중함으로써, 후속 동종 사례 및 한중 비교법 연구의 사실적 기반을 마련한다.

<주제어> 데이터 국외이전, 의료데이터, 개인정보 보호, 데이터 분류·등급, 데이터 국외이전 안전평가

摘 要

本文以公示编号 20220001 案件为分析对象。该案系首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心(Amsterdam UMC)合作开展的国际多中心临床研究(COLOR III、COLOR IV)，是《数据出境安全评估办法》(2022 年 9 月 1 日施行)实施以来全国首例通过数据出境安全评估的案件。本文采用“事实先行、规范在后”的分析顺序，先梳理本案自 2017 年至 2030 年的客观事实，再依法律、行政法规、部门规章、国家标准与地方性规范五个位阶，系统整理各阶段适用的中国法规范。研究发现：其一，本案呈现“医院内部前置审查、监管外部最终评估”的实务合规模式；其二，本案揭示了评估有效期机制与长期临床研究之间的结构性张力、多重规范并行适用中的衔接空白，以及“通过评估与持续合规”“未披露与违法”之边界等理论问题。本文不作违法判断，亦不提政策建议，而着力于事实与规范的完整梳理，为后续同类案件及中韩比较法研究奠定事实基础。

关键词：数据出境，医疗数据，个人信息保护，数据分类分级，数据出境安全评估