环球律师事务所
GLOBAL LAW OFFICE

环球生命科学及医疗法律专递

GLO Law & Policy News Letter in Life Science and Healthcare

环球生命科学及医疗团队

GLO Life Science & Healthcare Practice Group

2019 年 第三期 （总第二十九期）

Issue 3 of 2019 (Volume 29)

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987

中国生命科学及医疗领域法规最新发展

目录

2019 年第三期

Cybersecurity and data protection in Chinese healthcare industry

中国医疗行业网络安全与数据保护

by Alan Zhou | Charlene Huang

An overview of the regulatory environment for cybersecurity and data protection in the Chinese healthcare industry. The note introduces the evolving Chinese cybersecurity regime and its implications on the healthcare industry. It focuses on cybersecurity protection, data localisation, data export and other issues that pharmaceutical companies and medical institutions operating in China (or their overseas investors) need to be aware of.

Scope of this note

This note provides an overview of the legal framework for cybersecurity and data protection in the Chinese healthcare industry, looking at the national legal regime and sector-specific legislation affecting the healthcare industry.

The note analyses the types of healthcare data and maps them with specific types of data regulated under national and industry legislation. It addresses issues that might be encountered by pharmaceutical companies and medical institutions, in particular regarding the utilisation, local storage and cross-border transfer of patient data (including personal information and aggregate data). The note also lists the civil, administrative and criminal liabilities for various breaches and discusses information governance best practices for healthcare market players.

Booming value of big data versus cybersecurity and data protection

With the rapid development of cloud computing and the internet of things (IoT) technology, the e-health industry has been increasingly promoted. Well-known products of the e-health market include:

- Large-scale applications of electronic medical records (EMR) by medical institutions.
- Booming co-operations among pharmaceutical companies, technology giants and medical service providers in mobile health and online hospitals.

Chinese authorities, local and multinational market players realise the tremendous economic value of aggregate data (such as the patient behaviour pattern, medical or health statistics and so on).

Against this backdrop, legislation needs to balance the interests of various groups, including:

- State interest.
- Data sovereign.
- Privacy protection.
- Sustainable incentives to the e-health market.

Legislative background and rationale

Before 2013, Chinese legislation regarding cybersecurity and data protection mainly focused on the telecommunications industry, by requiring internet service providers to take security protection measures on their computer systems and networks. The regime was enforced by the *Ministry of Public Security* (MPS) to protect users' personal information under the governance of the *Ministry of Industry and Information Technology* (MIIT).

Subsequently, with the rising threat of cyber-attacks and the uncovered PRISM incident (that is, the US surveillance programme), many countries (such as the US, EU, Japan, and Australia) tightened the

legislation of cybersecurity from the perspective of data protection and safeguarding sovereignty. In such an environment *China* is on the alert for potential security risks.

In February 2014, the Office of the Central Leading Group for Cyberspace Affairs (OCLGCA) was established specifically for the development of overall strategies and policies on cybersecurity in China, with President Xi Jinping being the head officer. In March 2018, the leading group was elevated into a more powerful commission, namely, the Central Cyberspace Affairs Commission (CCAC) (中央网络安全和信息化委员会),as part of the 2018 government institutional reform (see *Practice note, Understanding the 2018 government institutional reform: China: Elevated party leadership and control*).

Since April 2014, the former OCLGCA (and the CCAC) office has been directly supervising the operation of the *Cyberspace Administration of China* (CAC), which in turn is responsible for cyberspace security and internet content regulation.

The legislative rationale behind the central government to strengthen the Chinese legal system of cybersecurity comes from the following motivations:

- **Emphasising cyber and data sovereignty.** Establishing a safety supervision system on cross-border data transfers to ensure the safety of national basic data or sensitive information, was identified as one of the key national tasks (*Notice of State Council on the 13th Five-Year National Information Plan 2016* (国务院关于印发“十三五”国家信息化规划的通知)).
- **Protecting personal information.** Since 2012, the central government has emphasised the legislative planning to improve the protection of personal information and privacy from misappropriation (*Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection 2012*).

On June 1, 2017, the *Cybersecurity Law of the People's Republic of China 2016* (2016 Cybersecurity Law) took effect, which constitutes one of the legal foundations for cybersecurity and data protection in China. The law provides that the state enhances network management to safeguard sovereignty, security and development interests of cyberspace in the state.

Notably in the five-year legislative plan of the 13th *National People's Congress (NPC) Standing Committee* released in September 2018, Personal Information Protection Law and Data Security Law appear as category I legislative items. This means the Standing Committee considers them as relatively mature bills, which are in a position of being submitted for deliberation within the five-year tenure of the 13th NPC. (See *Legal update, 13th NPC Standing Committee releases five-year legislative plan*.)

Legal framework: overview

The current legislation structures the framework respectively from civil, administrative and criminal perspectives, to secure cybersecurity and data sovereignty and to protect personal information.

Specifically for the healthcare industry, the former National Health and Family Planning Commission (NHFPC) issued several departmental rules to protect aggregate data and personal information generated

in this industry.

As part of the 2018 government institutional reform, the State Council established three new regulators, namely, the *National Health Commission* (NHC) (国家卫生健康委员会),State Medical Insurance Administration (SMIA) (国家医疗保障局)and State Medical Insurance Administration (SMIA) (国家医疗保障局)by integrating the function of several others. The NHC, replacing the NHFPC for the administration of health-related policies and medical and healthcare reforms, assumes the responsibility of guiding, administrating and supervising the utilisation of health data.

For detailed coverage of the healthcare institutional reform, see *Practice note, Understanding the 2018 government institutional reform: China: Healthcare*.

As a result, business operators in the healthcare industry not only need to follow the rules under the general cybersecurity and data protection regime, but also must comply with the sector rules formulated by the NHC.

National and industry legislation on cybersecurity and data protection: summary

Civil

- *General Provisions on the Civil Code of the People's Republic of China 2017* (2017 Civil Code Provisions). (For a general discussion on the implications of this development, see *Legal update, China enacts general provisions of civil code*.)
- *Tort Liability Law of the People's Republic of China 2009*. (For a general discussion on tort law implications on data privacy issues, see *Practice note, Data privacy in China: 2009 Tort Law*.)

Cybersecurity

- *2016 Cybersecurity Law*. (For an overview of this cybersecurity regime, see *Legal update, China passes Cybersecurity Law*.)
- *Measures for Security Review of Network Products and Services (For Trial Implementation) 2017*. (For more information on this development, see *Legal update, CAC issues trial measures on security review of network products and services*.)
- *Emergency Response Plan for Cybersecurity Incidents 2017* (国家网络安全事件应急预案).(For detailed discussions on this plan, see *Article, Petya attack calls for emergency plan: what should Chinese companies do?: Structure and key provisions of the plan: table*.)

Criminal

- *Amendment (IX) to the Criminal Law of the People's Republic of China 2015* (2015 Criminal Law Amendment (IX)). (For a general discussion on data privacy criminal offences, see *Practice note, Data privacy in China: 1997 Criminal Law*.)

Interpretation on Several Issues on the Application of Law to the Adjudication of Criminal Cases involving the Infringement of Citizens' Personal Information 2017 (2017 Judicial Interpretation on Privacy Criminal Offences) (关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释).(For more information on this development, see *Legal update, SPC and SPP release interpretation on criminal infringement of personal information*.)

Healthcare departmental rules

- *Administrative Measures for Population Health Information (for Trial Implementation) 2014* (2014 Population Health Information Measures).
- *Regulations for Medical Institutions on Medical Records Management 2013* (医疗机构病历管理规定).
- *EMR Administrative Measures (for Trial Implementation) 2017* (电子病历应用管理规范（试行）).
- *Measures on the Administration of National Health and Medical Big Data Standards, Security and Services (Trial) 2018* (国家健康医疗大数据标准、安全和服务管理办法（试行）)(2018 Health and Medical Big Data Measures). (For more coverage on this development, see *Legal update, NHC issues guidelines on health and medical big data standards, security and services*.)

National standards

- *Information Security Technology – Personal Information Security Specifications (GB/ T 35273-2017)* (信息安全技术个人信息安全规范)(2017 Personal Information Security Specifications). Its revised draft was released on 1 February 2019 for public consultation. (For more coverage, see *Legal updates, TC 260 issues national standard on personal information security* and *TC 260 circulates draft amendments to personal information security standard*.)
- The draft version of *Information Security Technology - Guide for Health Information Security* (信息安全技术健康医疗信息安全指南)(Draft Guide for Health Information Security), which was released on 26 December 2018 for public consultation.

Healthcare data

In the healthcare industry, the following information is normally of interest to market players:

- Basic information of both physicians and patients (including any such person's name, gender, age,

identity number, birthday, contact information and address, behaviour pattern and so on) (collectively mentioned as **Individual Basic Information**).

- Information in relation to medical records, including for example, personal and family medical history, and outpatient, inpatient and discharge records (collectively mentioned as **Medical Records**).
- Medical prescription or consumption records (collectively mentioned as **Medical Prescription Records**).
- Other operation information of medical institutions (collectively mentioned as **Other MI Operation Information**).

Mapping the existing legal framework, healthcare information may fall into one or more types of data.

Personal information and sensitive personal information

Since there is no single overarching law, there is also no uniform definition of "personal information" in

China. Article 76(5) of the *2016 Cybersecurity Law* defines personal information as various types of:

> "information that can be used separately or in combination with other information to identify a natural person, including the person's name, birthday, identity number, personal biological identification information, address and telephone number."

The non-binding 2017 Personal Information Security Specifications and its revised draft define personal information as:

> "information recorded by electronic or other means that can be used alone or in combination with other information to identify a natural person's identity or reflect the activities of a natural person, such as name, date of birth, identity document number, account password, property status, and location."

Specifically, "sensitive personal information" is defined as information that, if disclosed or modified, could have an adverse effect on the data subject. Examples include the data subject's identity document number, individual biometric information, bank account number, correspondence records and contents, property information, credit information, whereabouts, lodging information, health and physiological information and transaction information and personal information of children under 14 years old.

The Draft Guide for Health Information Security introduces the concept of "personal health information" as:

> "information that can be used alone or in combination with other information to identify a specific natural person's mentor or physical health information, involving the individual's previous, current or future mentor or physical health conditions, medial services accepted and corresponding payment records."

Based on above definitions, personal health information is one type of sensitive personal information, and its utilisation should not only follow the general rules and requirements regarding personal information, but also comply with any special rules regarding sensitive personal information.

From this perspective,

- Individual Basic Information is deemed as personal information.
- Medical Records and Medical Prescription Records, if sufficiently specific and detailed, might constitute personal health information and sensitive personal information as well.

(For detail on what constitutes personal information under national and industry legislation, see *Practice note, Data privacy in China: What constitutes personal information?*.)

CII data

CII refers to the critical information infrastructure in important industries and sectors, the damage, disable, disclosure of data of which may severely threaten the national security, national economy, social and public interests (*Article 31, 2016 Cybersecurity Law*). The scope of CII and the ways to identify CII are yet to be promulgated. It is proposed that the healthcare industry can fall into the ambit of CII (*Article 18, Rules on the Protection of Critical Information Infrastructure Security (Draft for Comments) 2017* (关键信息基础设施安全保护条例（征求意见稿）). If medial institutions are viewed as CII operators (which is likely given the various CII security protection drafts circulated in the last couple of years), personal information and important data collected and generated during their operation might be deemed as CII data. Specifically, this could cover all the following information:

- Individual Basic Information.
- Medical Records.
- Medical Prescription Records.
- Other MI Operation Information.

Health and medical big data

Big data is aggregate data characterised by its volume, velocity, variety and value, the utilisation of which is aimed to discover, develop and improve new knowledge, technology and value (*Action Plan to Improve Big Data Development 2015* (促进大数据发展行动纲要)).

For health and medical big data, it could be traced back to the concept of "population health data", meaning basic demographic information, medical and healthcare services information and other health information generated during the operation of all types of medical institutions in China (*Article 3*, *2014 Population Health Information Measures*). This can include e-health files, e-medical records and health statistics information (*NHFPC's Interpretation of the 2014 Population Health Information Measures* (人口健康信息管理办法（试行）解读)).Although the 2014 measures do not specifically use the term "health and medical big data", the rationale behind the measures is centralisation of big data generated by various medical institutions during their medical activities, and management of the data through a unified platform.

On 24 January 2017, the former NHFPC promulgated its *13th Five-Year National Information Plan on Population Health Information* ("十三五"全国人口健康信息化发展规划),under which the major task is to establish a unified platform for population health information, centralising the health and medical big data, and adopting classification management and sharing methodology.

On 25 April, 2018, the State Council issued its *Opinions on Promoting the Development of Internet plus Healthcare* (关于促进“互联网+医疗健康”发展的意见), which emphasised that local governments should co-ordinate to facilitate the establishment of the unified national health information platform which will gradually be connected with the national data sharing platform.

Within this background, from 2017, several provinces and cities (such as Qinghai, Guizhou, Guangdong, Fuzhou city of Fujian) issued local administrative rules on utilisation and management of health and medical big data.

On 12 July, 2018, NHC, from national level, promulgated the 2018 Health and Medical Big Data Measures, which define health and medical big data as "health and medical aggregate information generated in the course of disease control and prevention, as well as health management", and request that "all kinds of medical institutions at all levels should connect with the corresponding regional platforms of national health information, transmit and backup the data generated during healthcare services, and provide the monitoring ports to the health administrative departments" (*Articles 4 and 38, 2018 Health and Medical Big Data Measures*).

With a broad interpretation, the following types of information concerning patients and their aggregate data generated by medical institutions may fall into the concept of health and medical big data or population health data:

- Medical Records.
- Medical Prescription Records.
- Other MI Operation Information.

For different types of data, Chinese law imposes different implications on network operators for collection, storage and utilisation.

Cybersecurity obligations

The *2016 Cybersecurity Law* requires the establishment of a comprehensive graded protection regime for cybersecurity, including various general obligations and requirements applicable to network operators, and an additional set of obligations specifically on CII operators.

A network operator refers to the owner, manager or internet service provider of a network (*Article 76(3)*, *2016 Cybersecurity Law*). For example:

- A medical institution is the network operator of its system (such as the EMR or hospital information system).
- A pharmaceutical company is the network operator of its owned or managed internal system, software and website.

Security protection

Under the *2016 Cybersecurity Law*, all the network operators are obligated to ensure the security of their networks, including:

- Forming a protective system dependant on the corresponding grade.
- Taking necessary technical measures (such as data classification, and backup and encryption of important data).
- Developing emergency plan for cybersecurity events.
- Providing technical support and assistance for authorities' investigations.

(*Articles 21, 25 and 28*.)

For detailed discussion, see *Legal update, China passes Cybersecurity Law: Cybersecurity obligations*.

Data localisation for CII operators

As the operation safety of CII concerns the national and society safeguard, CII operators must take up stricter and more complicated measures to secure their networks.

The *2016 Cybersecurity Law* requires CII operators to store within China, personal information and important data that was collected or generated in China during their onshore operation; however, these

may be transmitted abroad on the successful completion of a security assessment (*Article 37*). See also *Data export implications*.

The concrete list of CII has not been promulgated. During CAC's 2016 and 2017 CII status surveys, urgent care centres and medical institutions' operation systems were among the targets. It is likely that information generated by medical institutions may be subject to data localisation in the future.

For an overview of the general data localisation requirement under the 2016 Cybersecurity Law, see *Practice note, Cross-border data transfers: China : Data localisation under the 2016 Cybersecurity Law*.

Utilisation and localisation for health and medical big data

Medical institutions are obligated to transmit and backup the data generated during their operations to the corresponding central-managed platform, and provide access to local counterparts of NHC for their monitoring (see *Health and medical big data*). Future legislative trends might require data sharing and disclosure by medical institutions to third parties be subject to strict monitoring and restrictions, coupled with classification and cataloguing of different types of health and medical data.

In addition, considering the sensitiveness of health and medical big data, data localisation is always a fundamental principal. Under the *2014 Population Health Information Measures*, all medical, health care, and family planning service entities are required to store population health information in onshore servers and the information cannot be stored in an overseas server or through a hosted or rented overseas server (*Article 10*). Article 30 of the 2018 Health and Medical Big Data Measures, adopting same principal, requires all health and medical big data be stored in safe and trustworthy servers within China and that the export of such data should only be permitted on an as needed basis after satisfying a security assessment.

Data privacy obligations

The *2016 Cybersecurity Law* requires network operators to keep the user information they collect strictly confidential, and to establish and improve their user information protection systems.

More specifically:

- The collection and using of personal information must follow the principle of "lawful, justifiable and necessary".
- A network operator must expressly notify the data subject the purpose, method and scope of the collection and use, and obtain corresponding consent from the data subject.
- In case there is any leakage or damage of the personal information stored, the operator must immediately take remedy actions, inform the data subject and file a report to competent authorities.

(*Articles 41-43*.)

From the national standard perspective, 2017 Personal Information Security Specifications provide detailed guidance on the protection of personal information and sensitive personal information, including requirements and protective measures during the collection, storage, transfer and sharing and retention of personal information.

The Draft Guide for Health Information Security, on the other hand, is aimed to provide guidance of cybersecurity and data protection on the following typical scenarios involving health and medical big data:

- Sharing among medical institutions.
- Utilisation during online medical treatment.
- Management by the centralised platform.
- Application of health and medical sensing devices.
- Application of software or apps.
- Clinical trials.
- Insurance.
- Repair and maintenance of medical devices.

Under each scenario, the draft guide intends to provide detailed rules for involved parties, covering data transmit, storage, access control, de-identification, safety measures, audit management, and so on. The guide, upon adopted, could play an important role in healthcare industry regulation.

For more information, see:

- *Legal update, China passes Cybersecurity Law: Data privacy obligations*.
- *Practice note, Data privacy in China*.
- *Practice note, Data breach notification in China*.

Data export implications

Provision of personal information and important data generated within China to overseas entities (including storing in overseas servers or granting access to overseas entities) is deemed as data export, which would only be allowed after the completion of corresponding data export security assessment.

The final legislation regarding data export security assessment has not been promulgated. However,

- On 11 April 2017, the CAC circulated for public comments the *Measures on Security Assessments for the Export of Personal Information and Important Data (Draft for Comments)* (个人信息和重要数据出境安全 评估办法（征求意见稿）)(see *Legal update, CAC circulates draft rules on exporting personal information and important data*).
- On May 19, 2017, the CAC called an internal meeting with the US-China Business Council and its several member companies to discuss a revised draft version of the above rule (*2017 CAC Revised Draft Measures on Data Export*), and the full text of the same is not publically circulated.
- On 30 August 2017, the National Information Security Standardisation Technical Committee (TC 260) circulated for public comments its revised draft of the *Guidelines for the Security Assessment of Data Export (Draft for Comments)* (2017 Data Export Security Assessment Draft Guidelines) (数据出境安全评估指南（征求意见稿）)(see *Legal update, TC 260 circulates revised draft guidelines on data export security assessments*). TC 260's guidelines are non-binding national standards, but like all its other standards, should play an important role in filling the legislation gap and predicting the authority's enforcement stance on specific issues.

According to the 2017 CAC Revised Draft Measures on Data Export, for any export of personal information and important data, a network operator (which does not necessarily have to be a CII operator) must:

- **Have informed consent from the data subject.** The network operator should notify the data subject of the transferring details (including the purpose, scope, type and the county or region where the recipient locates), and should obtain the consent from the data subject. The consent can be inferred where the data subject initiates the export (such as making international phone calls, sending emails or instant messages to the overseas recipient, and making cross-border e-commerce transactions).
- **Complete necessary security assessment.** Specifically, where the number of data subjects is below 500,000 individuals, the assessment can be performed by the network operator itself. However, where the number of data subjects accumulatively reaches 500,000 individuals, the security assessment needs to be formed by the CAC, or its authorised industrial authority.

The 2017 CAC Revised Draft Measures on Data Export further provide that data may not be exported if any of the following circumstances is identified during a security assessment:

- Where there is no consent from the data subject.
- Where the export may damage public and national interests.
- Where the export may endanger the security of national politics, territory, military, economy, technology, culture, society, information, ecological environment, resources, nuclear facilities and so on.
- Where there are other prohibited circumstances that the CAC or other authorities may determine.

Violation liabilities

The laws and regulations governing cybersecurity and data privacy in China provide for a wide range of civil, administrative and criminal sanctions and penalties for violations.

Civil liabilities

Under the *2017 Civil Code Provisions*, the methods of assuming civil liabilities include, among others:

- Stopping the infringement.
- Compensating for the actual and direct loss.
- Paying liquidated damages.
- Eliminating the impact.
- Apologies.

(*Article 160*.)

As there is no support of punitive damages under Chinese civil law, the number of civil claims raised by individuals(normally, patients) is limited.

Administrative liabilities

The *2016 Cybersecurity Law* stipulates different liabilities for network operators' violations.

Violations	Penalties
Failure to establish a protection system or timely perform an emergency plan.	• The network operator must correct as per the requirement of the competent local MPS or the CAC. • In the case of any refusal of correction, or a damage to network security, authorities may impose a fine of RMB10,000-100,000 on the operator, and RMB5,000-50,000 on the person directly in charge. • Where the violator is a CII operator, the penalties will be significantly increased to a fine of RMB100,000-1,000,000 on the operator and RMB10,000-100,000 on the person directly in charge. (*Article 59*.)

• Failure to comply with the principle of being lawful, justifiable and necessary for collecting and using personal information. • Failure to delete or correct relevant information as per the request of a data subject.	• Relevant authorities may require rectification, issue warnings, confiscate illegal gains, or impose a fine of one to ten times of the illegal gains. • Where there is no illegal gain, authorities may impose a fine up to RMB1million on the operator, and RMB10,000-100,000 on the person directly in charge.
	• Where the circumstances are serious, authorities may suspend the operator's business, close down the website, or revoke relevant business permits or the business licence. (*Article 64*.)
Unlawfully obtaining, selling or providing personal information to others.	• The competent local MPS may confiscate the illegal gains, and impose a fine of one to ten times of the illegal gains. • Where there is no illegal gain, authorities may impose a fine up to RMB1million on the operator.
Unlawfully storing network data or providing network data overseas by CII operators	• Authorities may require rectification, issue warnings, confiscate illegal gains, and impose a fine of RMB50,000-500,000 on the operator and RMB10,000-100,000 on the person directly in charge. • Authorities may also order the operator to suspend relevant business, close down the website, or revoke relevant business permits or the business licence. (*Article 66*.)

Criminal liabilities

The NPC passed the *2015 Criminal Law Amendment (IX)* on 29 August 2015. The amendment, which took effect on 1 November 2015, creates new offences and increases penalties for data privacy and cybersecurity violations (among other things). The principal changes are:

- Increased scope and penalties for offences of the sale or disclosure of personal information.
- New offences of violating cybersecurity laws, which apply to internet service or content providers and their responsible persons.
- New offences of using and facilitating the use of information networks for an illicit purpose.

(For detailed discussions, see *Legal update, Criminal Law amendment: new individual and corporate offences for data privacy and cybersecurity violations*.)

Subsequently, the 2017 Judicial Interpretation on Privacy Criminal Offences clarifies sentencing standards for "serious" and "particularly serious" criminal offences. (For more information, see *Legal update, SPC and SPP release interpretation on criminal infringement of personal information*.)

For example, where a network operator unlawfully obtains, sells or provides others with over 500 pieces of personal information concerning health, the criminal offence is likely triggered. The criminal liabilities are three to seven years of imprisonment for the responsible person, with concurrently a fine of one to five times of the illegal gains on the operator. (*Articles 5 and 12, 2017 Judicial Interpretation on Privacy Criminal Offences* and *Article17, 2015 Criminal Law Amendment (IX).*)

Information governance: best practices for healthcare industry

Strong information governance is a key for many healthcare data compliance issues, including ensuring compliance with the relevant cross-border transfer and local storage rules.

For medical institutions and their co-operators or investors

Medical institutions and practicing physicians are normally the collectors of patient data. In practice, co-operators or investors of medical institutions may intend to obtain the data generated by medical institutions, especially labs or institutions with overseas background.

Where a medical institution shares data with its co-operator or investor, the following rules need to be followed:

- The medical institution should obtain informed consent from patients on the collection, use and transfer of their personal information.
- With respect to patients' medical records (including EMR), the medical institution should be

responsible for the storage and management of medical records. Any storage and process of medical records by other entities should require an express authorisation from the medical institution, and any disclosure of patients' medical records for non-medical, non-teaching or non-research purposes is forbidden.

- The health and medical big data or population health data generated by the medical institution needs to be stored and processed within China.

Besides, as it is possible that a medical institution may constitute a CII operator, any cross-border transfer of data generated in its core system may face restriction, depending on the further development of CAC's regulations.

For pharmaceutical companies

Normally, for pharmaceutical companies (especially multinational companies), data will be centralised, stored and processed in a specific system. During operation of the system, the following key questions need to be analysed.

- **Who is the network operator?** Sometimes the concerning system is owned by an overseas headquarter, and operated by local subsidiaries with the authorisation from the headquarter. Under this circumstance, Chinese authorities may view the overseas headquarter as the network operator. To identify the network operator is actually to identify who is the responsible person to assume relevant obligations under the *2016 Cybersecurity Law*.
- **What kind of data is involved?** In practice, the data involved in the operation of pharmaceutical companies may contain personal information (patients, potential consumers, physicians and so on) and medical and health aggregate data. The data sources of pharmaceutical companies may come from different channels, including self-collection by employees, collection from medical institutions or third party agents. Different types of data may face different protection requirements:
  - for personal information, informed consent of the data subject is necessary and in case the consent may not be obtained, de-identification could be an effective risk mitigation method; and
  - for medical records and health and medical big data/population health data obtained from medical institutions, local storage and utilisation is recommended and this needs an express authorisation from medical institutions.

  (For more information, see *Healthcare data*.)

- **Is there any cross-border transfer?** The system, in certain circumstances, may directly be based on an overseas server or open access to overseas affiliates without limitation. In such cases there could happen cross-border data transfers.

Though the 2017 CAC Revised Draft Measures on Data Export is only at a drafting stage (see *Data export implications*), it is possible that pharmaceutical companies may need to establish a security assessment mechanism on cross-border data transfers once the final version is promulgated.

Taking reference from the 2017 Data Export Security Assessment Draft Guidelines, key assessment elements may include:

- Justified and necessary needs (that is, necessary for the business' operation, contractual obligations and so on).
- A plan of risk control.
- Protective capacity of the sender and recipient.
- The legislative or political environment of the recipient's country.

It is common for pharmaceutical companies to have a centralised system to receive data from subsidiaries and affiliates in various jurisdictions. In such cases, legislation of more than one jurisdiction might be applied to the same single system. In those circumstances, companies are recommended to have a gap analysis over the system. Such analysis will assess the current status and practices of the company, compare the requirements of various jurisdictions and conclude a risk-based standard most suitable to the company.

Alan Zhou is a partner, based in our Shanghai Office. He is the leading partner of its Life Science and Healthcare practice group. He has represented many multinational corporations, Chinese state-owned and private corporations, and private equity/venture capital funds and has a particularly strong background in life science and healthcare.
Email：alanzhou@glo.com.cn

Charlene Huang is an Of Counsel based in our Shanghai office. Her main practice areas encompass foreign direct investment (“FDI”), mergers and acquisitions (“M&A”), compliance and general corporate. She is experienced in the healthcare service sector, data security compliance and other fields of healthcare.
Email：xuchunhuang@glo.com.cn

外商投资医疗行业 —— 外资限制与 VIE 模式探讨

作者：周磊 I 孙胤翔 I 王之衍 I 董秋艳

2016 年 12 月 27 日，国务院印发通知《“十三五”深化医药卫生体制改革规划》，鼓励社会力量兴办健康服务业，目标进一步优化政策环境，督促各地落实在市场准入等方面对所有医疗机构同等对待的政策措施，被视为社会办医外资准入再次放开的政策信号。但是，尽管近年来深化医改和鼓励社会办医的宏观政策接连推出，与之相对应的是，2015 年新修订《外商投资产业指导目录》后，对于外商投资医疗机构却由原来的允许类重新被列入限制类行业，并仅限于以合资、合作形式设立。此后的 2017 年最新修订《外商投资产业指导目录》及后续相关外资准入目录和负面清单中，外商投资医疗机构在总体上仍然归为限制类行业并延续至今。

近年来医院投资和交易活跃，医疗机构数量呈现总体增长趋势。在弘和仁爱、凤凰医疗、新世纪医疗等医院集团相继通过红筹模式在香港上市，而国内 A 股市场仅有个别成功获批，近期康宁医院上市被否的背景下，是否设计搭建境外结构寻求海外上市路径，对境内医疗机构而言是一个无法规避的命题。本文试图梳理中国近年来对于外商投资医疗机构的政策演变，并结合当前外资设立医疗机构受到一定程度限制的现实状况，探讨采取合约安排形式投资医疗服务产业的相关案例。

一、 外商投资医疗机构（除港澳台）的政策演变及现状

中国政府对于外商投资医疗机构的限制并非一直存在，而是经历了全面限制、政策试点放宽、再恢复限制的政策变迁。大致可以分为 2010 年之前（国家普遍限制设立外商独资医疗机构）、2010—2015 年（外商投资医疗机构政策放宽试点）及 2015 年之后（重新对外商投资医疗机构进行限制）这三个阶段，具体如下：

(一) 总体限制阶段：2010 年之前

1997 年，国家发展和改革委员会（“**发改委**”）、对外贸易与经济合作部发布的《外商投资产业指导目录》（1997 修订）明确将医疗机构纳入限制外商

投资的目录，限制要求中方必须控股或占主导地位。此后，卫生部、对外贸易与经济合作部于 2000 年发布的《中外合资、合作医疗机构管理暂行办法》（“**《合资暂行办法》**”）放宽外资比例限制，规定中方在中外合资、合作医疗机构中所占的股权比例或权益不得低于 30%（即外资比例不得超过 70%）。基于此，2002 年再次修订的《外商投资产业指导目录》虽仍然保留医疗机构为外商投资限制类，但为了与卫生部的规定相衔接，将限制条件修改为限于合资、合作，不再要求中方控股或主导。此后 2004 年、2007 年两次对于《外商投资产业指导目录》的修订均沿用上述限制条件。

(二) 试点放宽阶段：2010 年至 2015 年

2010 年国务院办公厅转发发改委及卫生部等部门《关于进一步鼓励和引导社会资本举办医疗机构的意见》，提出进一步扩大医疗机构对外开放，将境外资本举办医疗机构调整为允许类外商投资项目，逐步取消对境外资本的股权比例限制，对具备条件的境外资本在我国境内设立独资医疗机构进行试点、逐步放开。随后在 2011 年修订的《外商投资产业指导目录》中，医疗机构不再被列为外商投资限制类，转为允许类行业。2013 年 9 月 28 日，国务院进一步发布《关于促进健康服务业发展的若干意见》，其所列主要任务之一即包含进一步放宽中外合资、合作办医条件，逐步扩大具备条件的境外资本设立独资医疗机构试点。

2013 年 12 月 30 日，国家卫生和计划生育委员会（“**卫计委**”）、国家中医药管理局发布《关于加快发展社会办医的若干意见》，明确具备条件的境外资本可在中国（上海）自由贸易试验区等特定区域设立独资医疗机构。2013 年，上海市制订《中国（上海）自由贸易试验区外商独资医疗机构管理暂行办法》（“**《上海自贸区暂行办法》**”），该暂行办法允许外国投资者在中国（上海）自由贸易试验区以独资形式设立营利性医疗机构。符合条件的外国投资者应当 (1) 具有直接从事医疗机构投资与管理 5 年以上的经验；(2) 能够提供国际先进的医疗机构管理经验、管理模式和服务模式，或能够提供具有国际领先水平的医学技术和设备，或可以补充或改善所在地医疗服务能力、医疗质量、技术、资金和医疗设施方面的不足。

2014 年，卫计委、商务部发布《关于开展设立外资独资医院试点工作的通知》（“**244 号文**”），允许境外投资者通过新设或并购的方式在试点省市设立外资独资医院。根据该通知，境外投资者设立外商独资医院的试点地区扩大到北京市、天津市、上海市、江苏省、福建省、广东省和海南省。对于外国投资者的要求与《上海自贸区暂行办法》基本一致。

(三) 再限制阶段：2015 年至今

2015 年修订的《外商投资产业指导目录》，医疗机构重新被列入外商投资限制类行业，仅限于合资、合作。并且，在同年国务院办公厅印发的《自由贸易区外商投资准入特别管理措施（负面清单）》（“**自贸区负面清单**”）中，也将医疗机构明确规定为限制类且仅限于合资、合作。此后历次修订的《外商投资产业指导目录》及自贸区负面清单均将医疗机构保留在外资限制目录中。因此，尽管《上海自贸区暂行办法》和 244 号文等文件并未被正式废止，但是实践中各卫生行政部门原则上均不再接受外商设立独资医疗机构的审批申请。而对于合资、合作的外商投资医疗机构而言，又由于自贸区负面清单以及《外商投资产业指导目录》均未明确相应的外资持股的比例要求，因此实践中，大部分地区的卫生部门普遍按照 2000 年发布的《合资暂行办法》，要求中方持股不得低于 30%。

尽管大部分地区的卫生部门仍然依据《合资暂行办法》的要求确定外资受限比例，根据 2011 年《卫生部关于调整中外合资合作医疗机构审批权限的通知》，中外合资合作医疗机构的审批权限已经下放至省级，部分地区已经出台了专项规定设置和明确当地医疗机构的外资投资比例。以四川省为例，四川省卫生厅、商务厅于 2012 年发布《关于印发四川省中外合资合作医疗机构管理办法的通知》，规定中方在合资、合作医疗机构中所占的股权比例或权益不得低于 10%，较《合资暂行办法》有较大突破。此外，对于以诊所形式设立的医疗机构，根据 2017 年 8 月 8 日发布的《国家卫生计生委关于深化“放管服”改革激发医疗领域投资活力的通知》，外国医疗机构、公司、企业和其他经济组织以合资或者合作形式设立的诊所，放宽外方投资股权比

例不超过 70%的限制，属于对于诊疗服务规模较小的特定类型医疗机构的特别放宽措施。

二、 港澳台投资医疗机构的相关政策

承上文所述，尽管有部分地区的外商投资医疗机构的股权比例已经突破了 70%，但是在包括北京、上海、广东等经济发达省份、城市以及其他大部分区域，外商投资医疗机构目前仍然受限于 70%的外资比例限制，这对于希望能够全资控股境内医疗机构的投资者（包括通过海外市场融资和上市的投资者）而言无疑仍然是一大障碍。

与前文第一部分所述的外商投资医疗机构不同的是，基于《内地与香港关于建立更紧密经贸关系的安排》、《内地与澳门关于建立更紧密经贸关系的安排》及其补充协议（以下合称“**CEPA**”）、《海峡两岸经济合作协议》及其补充协议（以下简称“**ECFA**”），医疗服务产业对于港澳台投资设立独资医院的政策更加宽松，具体而言：(1)卫生部及商务部基于 CEPA 于 2010 年发布了《香港和澳门服务提供者在内地设立独资医院管理暂行办法》（“**109 号文**”），放开了香港和澳门服务提供者在试点地区（上海市、福建省、广东省、海南省和重庆市）设立独资医院、疗养院提供医疗服务，并于 2012 年先后发布《关于扩大香港和澳门服务提供者在内地设立独资医院地域范围的通知》及《关于香港和澳门服务提供者在内地设立医疗机构有关问题的通知》，于 2012 年 4 月 1 日将香港和澳门服务提供者在内地设立独资医院的地域范围扩大到所有直辖市及省会城市后、又于 2013 年 1 月 1 日起取消了对于香港和澳门服务提供者在内地设立独资医院的地域限制；(2)卫生部及商务部基于 ECFA 于 2010 年发布了《台湾服务提供者在大陆设立独资医院管理暂行办法》（“**110 号文**”）的通知，允许台湾服务提供者在大陆试点省市（上海市、江苏省、福建省、广东省和海南省）设立独资医院。综上所述，若能够适用 CEPA 或 ECFA 而以台港澳投资的方式实现对境内医疗机构的投资，则可以很大程度上解锁《外商投资产业指导目录》及自贸区负面清单对于外商独资投资医疗机构的限制。实践中，已经有一些港澳台资独资医院成功设立，例如深圳希玛林顺潮眼科医院由香港希玛国际眼科医疗集团（中国）有限公司全资于 2013 年设立、费森尤斯医药香港有限公司也在昆明、福州和泉州分别以新设或收购的方式设立了港资

全资的血液透析中心等。

需注意的是，通过 CEPA 或 ECFA 设立港澳台独资投资医疗机构，其对于港澳台股东的资质审查要求可能更严格于《合资暂行办法》中对于合资设立的外商投资医疗机构的外方股东的资质要求。以《内地与香港关于建立更紧密经贸关系的安排》为例，其对于符合条件的"服务提供者"的要求包括：(i)香港服务提供者符合内地法律法规和行政规章对外商投资主体的业务性质和范围的限制性规定（即能够提供先进的医院管理经验、管理模式和服务模式、或能够提供具有国际领先水平的医学技术）、(ii)香港服务提供者应已在香港注册或登记设立并从事实质性商业经营 3 年以上（含 3 年）、(iii) 香港服务提供者在香港从事实质性商业经营期间依法缴纳利得税、(iv)香港服务提供者应在香港拥有或租用业务场所从事实质性商业经营，其业务场所应与其业务范围和规模相符合。

此外，虽然 109 号文和 110 号文及其后续通知明确香港、澳门和台湾服务提供者可以设立独资医院、独资疗养院，且除独资医院、独资疗养院外其他独资医疗机构的设置的标准和要求按照内地单位或个人设置医疗机构进行办理，但在实践中，我们注意到不同地区的主管部门对此有不同的理解。对于有意通过 CEPA 或 ECFA 设立诊所、门诊部、卫生院等其它形式的港澳台独资投资医疗机构的投资者，应提早做好相应规划并确认所在地主管部门的监管意见。

三、 外资限制环境下外方参与医疗机构的模式——合约安排

在以上外资准入的整体政策框架下，尽管《合资暂行办法》、CEPA 及 ECFA 等规定为外资进入大陆医疗机构投资领域进行了一定程度的放开，但是鉴于仍然存在的外资比例限制，针对于具体案例，在无法通过 CEPA 或 ECFA 设立港澳台独资投资医疗机构、或通过《合资暂行办法》可以取得的医疗机构中的外资股比无法满足商业需求的情形下，是否采取 VIE 合约安排作为解决方案是可以相应探讨和作为商业考量的。

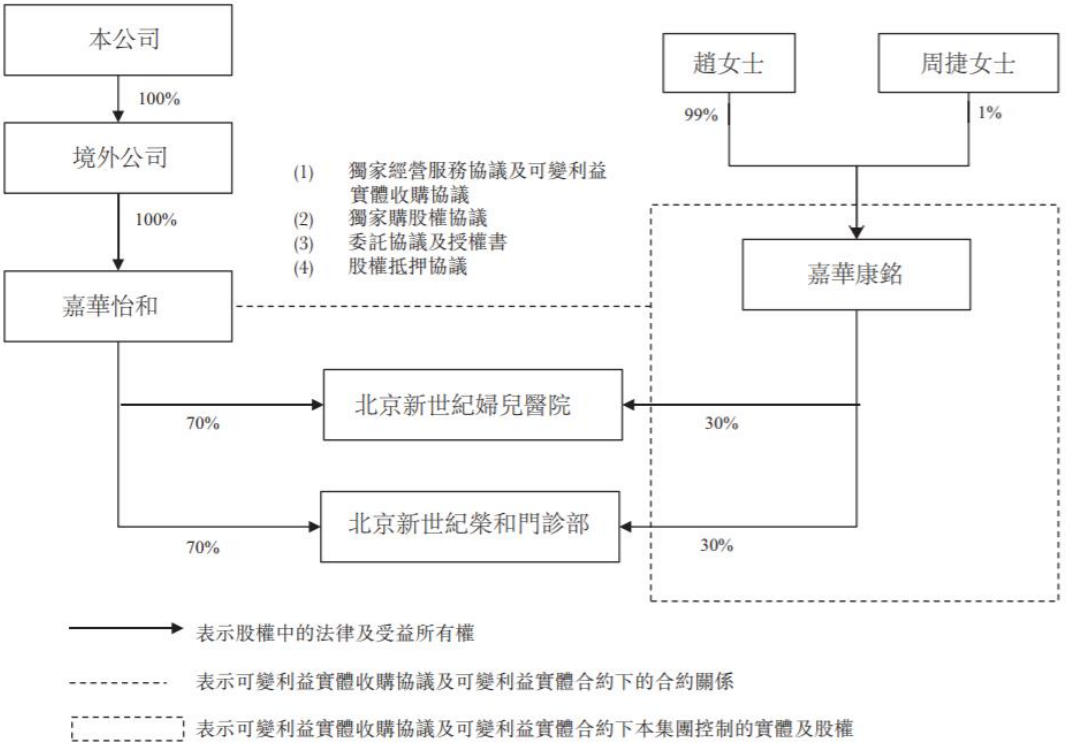
以香港联交所为例，根据香港交易所刊发的上市决策，上市申请人应当严格限制使用合约安排，其只可于必要的情况下以合约安排解决外资持股的限制，否则上

市申请人必须直接持有运营公司的最大许可权益。因此，香港联交所可接受的合约安排限于政策明确限制的行业或主管监管机关明确没有可遵循的审批程序或指引的情况。我们理解，由于医疗服务产业仍被列于外资限制目录，通过合约安排实现将外资受限的权益纳入整体境外上市体系存在可行性和可操作性。在医疗机构 VIE 架构设计和安排上，不同于其他外资完全限制行业，投资者应首先按照所在地区的外商准入政策，明确外资股比的实际限制比例，并在此基础上针对限制外资比例的部分进行 VIE 结构建立，其余权益仍应通过直接持股方式予以保留在股权控制结构下。其次，对于多机构或医疗集团类型企业，应当充分考虑是否按照各地机构实际限制比例进行“归总”过程，亦即探讨是否在各机构层面实现多个平行 VIE 结构，或在可行的情况下通过持有/控制多个医疗机构的上层持股平台进行 VIE 搭建。

虽然按照当前有关政策，医疗行业采用 VIE 结构在法律制度上似乎并无特殊限制，我们提醒读者注意，目前外资医疗机构采取 VIE 架构的实际案例相对有限，在具体实例中应当审慎评估使用。我们通过如下两个公开上市公司案例进行分析以对外资投资医疗机构的 VIE 合约安排进行进一步探讨：

(一) 新世纪医疗

新世纪医疗控股有限公司（“**新世纪医疗**”，01518.HK）于 2017 年 1 月于香港交易所主板上市。根据新世纪医疗公告信息显示，其主要从事其在北京的三间医疗机构提供儿科及妇产科专科服务。由于上文所述的外资投资医疗机构限制的原因，新世纪医疗通过北京嘉华怡和管理咨询有限公司（“**嘉华怡和**”）分别持有北京新世纪妇儿医院有限公司及北京新世纪荣和门诊部有限公司各 70%的股权，而剩余 30%的股权则由北京嘉华康铭医疗投资管理有限公司（“**嘉华康铭**”，由新世纪医疗实际控制人配偶赵女士及妹妹周捷女士分别持有 99%及 1%的股权）持有。于新世纪医疗上市后不久后的 2017 年 9 月，新世纪医疗即公告披露，嘉华怡和以人民币 3000 万元的对价与赵女士、周女士以及嘉华康铭签署 VIE 合约安排的方式以实际享有嘉华康铭所以经济利益，进而实现享有对北京新世纪妇儿医院有限公司及北京新世纪荣和门诊部有限公司的 100%的经济利益。上述交易的相关主体结构如下所示：



新世纪医疗的上述案例特殊之处在于，该等 VIE 合约的安排在新世纪医疗上市后同年进行，其在联交所上市申请时并未采取 VIE 架构形式并就此进行审查。通过查阅新世纪医疗的上市文件可以进一步发现，对于赵女士及周女士持有的嘉华康铭 100%的股权，已经协议安排由新世纪医疗上市前的各股东（或其关联方）实益享有相关权益、并由新世纪医疗享有独家购买权购买嘉华康铭持有的北京新世纪妇儿医院有限公司及北京新世纪荣和门诊部有限公司的 30%的股权。新世纪医疗的上述 VIE 合约安排，实际是变相实现了新世纪医疗于上市前对于嘉华康铭的上述两家医疗机构 30%股权的购买权。

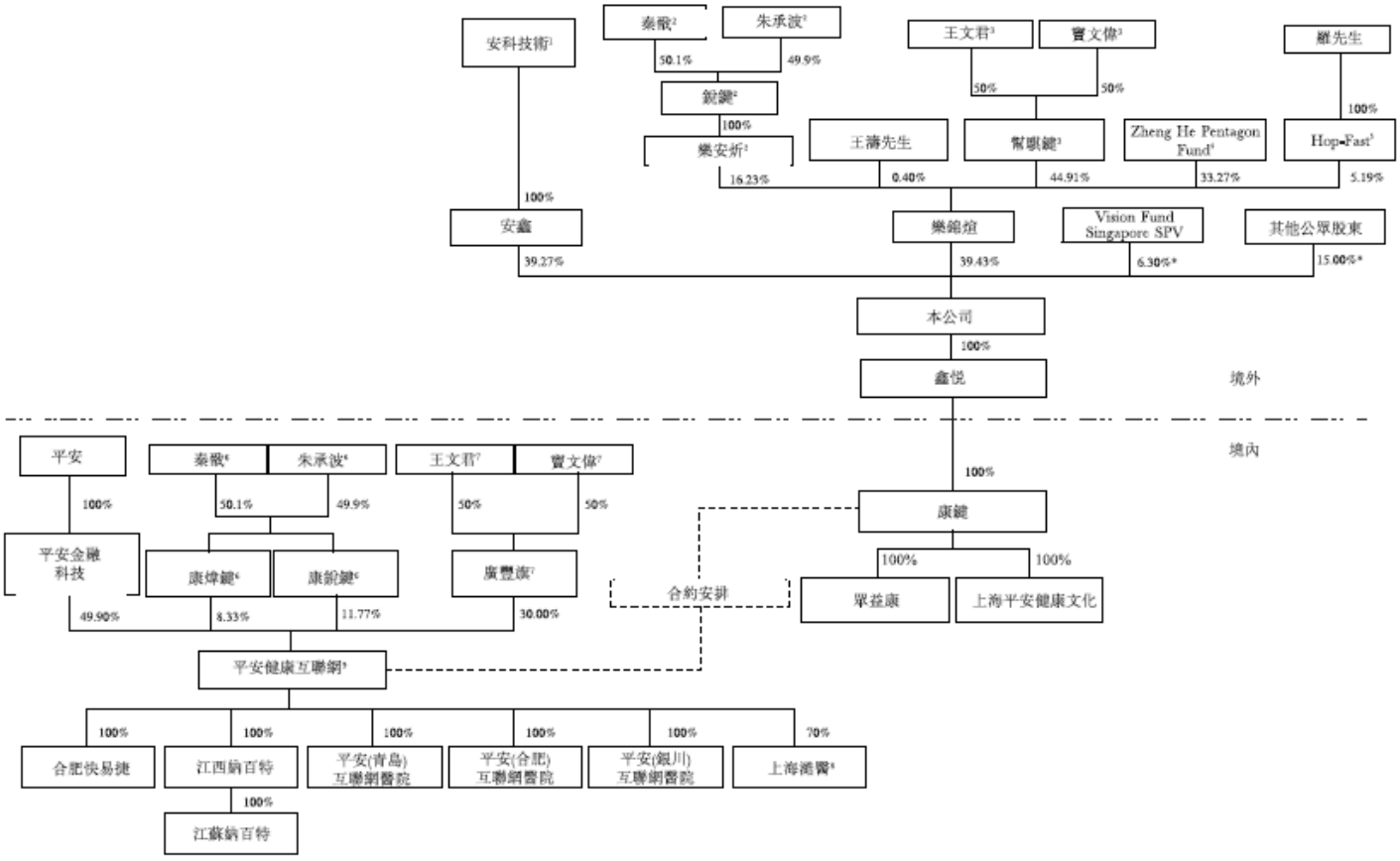
新世纪医疗的上述操作一定程度上加重市场的担忧，认为联交所对于医疗机构 VIE 合约安排是否存在谨慎甚至变相否认态度、亦或是新世纪医疗的上市中介机构出于谨慎考虑而进行的特殊安排。但是不可否认的是，由于新世纪医疗相关合约安排的两家医疗机构都位于北京，其以外资身份仅能持有两家医疗机构各 70%的股权的情况，与此前华润医疗（01515.HK）2013 年上市时以外资身份 100%持有北京市健宫医院有限公司的情况[1]不一致，不排除

[1] 华润医疗对于北京市健宫医院有限公司的相关结构建立过程，正处于国家对于外商投资医疗机构的放开阶段，且其具有一定个案的特殊性，我们理解，在目前阶段不具有普适性的直接参考价值。

因此导致新世纪医疗在与香港交易所沟通解释的过程中存在一定困难。

(二) 平安好医生

2018 年 5 月 4 日，平安健康医疗科技有限公司（“**平安好医生**”，01833.HK）于香港交易所主板上市。平安好医生致力于移动医疗领域，从产品上线到正式上市不足 3 年时间。于重组完成上市前，平安好医生的股权结构如下：



其中，平安（合肥）互联网医院及平安（青岛）互联网医院经营线上医疗服务，分别持有合肥市蜀山区卫生和计划生育局及青岛市崂山区卫生和计划生育局颁发的医疗机构执业许可证。平安好医生解释，根据《外商投资产业指导目录》及《合资暂行办法》，经营医疗机构属于限制类范畴，且外国投资者不得持有医疗机构 70%以上股权。因此该两家公司最终采用合约安排的方式合并进入上市公司体系。

这一案例同时存在互联网医疗的特殊性，并使其采取的上市前最终结构未适用外资可准入股比直接持股。如上图所示，平安（合肥）互联网医院及平安（青岛）互联网医院 100%的股权都通过合约安排的模式进入上市体系，这一点似乎不符合上市决策中要求的“上市申请人必须直接持有运营公司的最大许可权益”。对此，招股书披露，鉴于该两家公司系“线上”医疗机构，安徽省卫生和计划委员会及青岛市卫生和计划委员会均口头确认不存在涉及外商投资限制的与线上医疗机构有关的适用法规，且其不会受理及批准外商投资企业在其各自辖区内成立线上医疗机构的任何申请。基于上述，平安好医生的法律顾问认为，实际上，外国投资者不得持有该两家互联网医院的任何股权。因此，该两家公司的 100%股权全部通过合约安排的方式进入上市公司体系。

通过上述两个案例，我们理解在医疗行业中采取合约安排形式仍应采取谨慎态度。典型的合约安排针对一般行业而言，可以较为有效的实现对企业的全面控制与决策管理，而对于医疗机构而言，相较一般企业，其同时受到卫生主管部门的监督管理，执行合约安排需要符合卫生主管部门对于医疗机构的设置与运营要求，包括由具有资质的专业人士进行管理运营。因此，如何设计该等合约安排，以及该等合约安排是否可能受到卫生主管部门的挑战，仍有待实践中的进一步观察与探讨。尽管如此，从现阶段医疗行业对接境外资本的角度来看，上述两家上市公司的案例也提供了一定的借鉴意义。平安好医生的案例提供了一个较为新颖的思路，即在医疗行业受限的基础上，结合其他行业的外资禁入要求，合理阐释其采用合约安排的合理性。新世纪医疗的案例相对特别，其在上市之前搭建一个非典型合约安排的结构，并于上市后执行相关约定以实现最终的典型合约安排形式。从结果来说，该两家公司都实现了最终境外上市的需求。而对于其它医疗机构投资者而言，如何根据行业监管要求与自身经营特点，设计与搭建出合理的结构以实现对医疗机构的控制及与境外资本的对接，仍需要专业人士就个案提供不同的分析与建议。

周磊为环球律师事务所上海办公室合伙人，主要执业领域为医药和健康、收购兼并、私募股权/风险投资、合规风控和公司法。

邮箱：alanzhou@glo.com.cn

孙胤翔为环球律师事务所上海办公室合伙人，其职业领域为医药和健康、风险投资与私募股权、公司与并购业务。

邮箱：robertsun@glo.com.cn

王之衍为环球律师事务所上海办公室的顾问，其职业领域为并购、私募股权投资以及企业治理和日常运营。

邮箱：lawrencewang@glo.com.cn

董秋艳为环球律师事务所上海办公室的律师，其职业领域为医药和健康、并购和股权投资。

邮箱： sylviadong@glo.com.cn

创新医疗器械特别审查程序简评

作者：曹思思 | 王冠洁

一、 前言

为鼓励医疗器械研发创新，促进医疗器械新技术的推广和应用，推动医疗器械产业高质量发展，原国家食品药品监督管理局于 2014 年 2 月 7 日颁布了《创新医疗器械特别审批程序（试行）》（“**《特别审查程序（试行）》**”）。经历了近 5 年的试行实践，随着《医疗器械注册管理办法》（2014 年 7 月 3 日颁布）、《国家创新驱动发展战略纲要》（2016 年 5 月 19 日印发）、以及《医疗器械监督管理条例》（2017 年 5 月 4 日修订）的相继施行，国家药品监督管理局（“**国家药监局**”）于 2018 年 11 月 5 日发布了《关于发布创新医疗器械特别审查程序的公告》（2018 年第 83 号），公告国家药监局组织修订的《创新医疗器械特别审查程序》（“**《特别审查程序》**”）自 2018 年 12 月 1 日起施行，《特别审查程序（试行）》同时废止。本文将从《特别审查程序》发布的行业背景入手，介绍特别审查程序对于医疗器械注册申请者而言的主要优势，特别审查程序的适用范围以及特别审查程序的具体流程，并分析特别审查程序的行业影响。

二、 行业背景

2015 年 8 月，国务院出台《关于改革药品医疗器械审评审批制度的意见》，药品医疗器械审评审批改革正式启动，其中明确，将改革医疗器械审批方式，鼓励医疗器械研发创新，将拥有产品核心技术发明专利、具有重大临床价值的创新医疗器械注册申请,列入特殊审评审批范围，予以优先办理，与之相关是一系列配套政策的发布或更新。

2017 年国务院办公厅发布的《关于深化审评审批制度改革鼓励药品医疗器械创新的意见》进一步明确，应当加快医疗器械注册审评审批流程，包括对于临床急需、罕见病治疗医疗器械以及创新医疗器械等类型的医疗器械，给予优先审评审批的优惠条件。优先审评审批，可以根据适用条件，通过优先审批程序、特别审查程

序以及医疗器械应急审批程序等多种途径实现。不同途径的适用范围具体如下表：

	优先审批程序	特别审查程序	医疗器械应急审批程序
设立依据	2016年10月25日发布《医疗器械优先审批程序》	2014年2月7日发布《创新医疗器械特别审批程序（试行）》 2018年11月2日发布《创新医疗器械特别审批程序》	2009年8月28日发布《医疗器械应急审批程序》
适用范围	罕见病；常见肿瘤；老年人特有和多发疾病；儿童和临床急需产品、列入国家科技重大专项或者国家重点研发计划的医疗器械	技术创新类型医疗器械	突发公共卫生事件应急所需，且在我国境内尚无同类产品上市，或虽在我国境内已有同类产品上市，但产品供应不能满足突发公共卫生事件应急处理需要

特别审查程序作为优先审评审批的重要路径之一，其主要目的在于鼓励技术开发和技术创新，加强对于自主开发企业的保护，以提高国家整体的医疗器械技术开发能力。

三、 特别审查程序的优势

创新医疗器械特别审查程序，是指针对符合一定标准的创新型医疗器械，允许其在标准不降低、程序不减少的前提下，可以在提交医疗器械注册申请之前，首先进行创新医疗器械申请，通过审评人员早期介入、专人管理和科学审查，对通过审查被认定为创新医疗器械的产品予以优先办理，并加强与申请人的沟通交流。

下文将对特别审查程序的优势进行详细说明：

(一) 优先办理

根据《特别审查程序》，国家药监局行政事项受理服务和投诉举报中心（“**受理中心**”）在受理创新医疗器械注册申请后，会将注册申请的项目标记为“创新医疗器械”，并及时进行资料流转。对已受理注册申报的创新医疗器械，将从技术审评到行政审批均享有优先办理的权利[1]。

按照创新医疗器械特别审查程序获准注册的医疗器械产品申请许可事项变更的，国家药监局同样将予以优先办理[2]。

优先办理是申请创新医疗器械最重要的优势之一，据统计，2018 年共有 21 项创新医疗器械上市，创新医疗器械的审评时间较其他首次注册的三类医疗器械平均缩短了 83 天[3]。而在北京地区，据北京药品监督管理部门统计，其职责范围内的二类创新医疗器械审批的全流程时限平均由 170 天缩短至 22 天。

目前新技术层出不穷，产品更新迅速，尽早上市对于研发者来说不仅能够尽快获得销售收入，对于创新产品而言更是可以通过缩短上市所用时间这一优势抢占市场占有率。

(二) 与各级药品监督管理部门的沟通交流

根据《特别审查程序》，对于同意按照特别审查程序审查的创新医疗器械，申请人所在地省级药品监督管理部门应当指定专人进行沟通指导。

[1] 《特别审查程序》第二十、二十一条
[2] 《特别审查程序》第二十四条
[3] 《二十一个创新医疗器械一年内获批上市》，中国医药报, 胡芳，http://m.people.cn/n4/2019/0111/c34-12175727.html

对于创新医疗器械，在产品注册受理前以及技术审评过程中，国家药监局医疗器械技术审评中心（“**审评中心**”）将指定专人，应申请人要求进行沟通和指导，讨论技术相关问题[4]。

每一创新医疗器械进行申请注册时面临最主要问题之一在于就该医疗器械的技术审查无先例或少有先例可循，如何判定创新医疗器械的安全性和有效性，需要申请者与审评中心密切沟通产品的功能性能、技术参数等。通过提供有效的沟通渠道，可以帮助申请者向审评中心进行阐述解释，并且加快申请者的准备和审评进度。

(三) 分类界定

如上文所述，创新医疗器械由于缺少先例，往往出现申请人无法对产品进行正确分类界定。由于医疗器械产品的分类界定将直接影响国家对产品的注册、生产和经营的监管，因此就创新医疗器械而言，《特别审查程序》特别明确创新医疗器械审查办公室在出具审查意见时，应当一并对医疗器械管理类别进行界定。避免管理类别模糊，申请人无从申请的困境[5]的同时，也避免申请人另行申请分类界定导致延长总的申请注册时间。

四、 适用范围

《特别审查程序》明确了适用于创新医疗器械特别审查程序的情形[6]，即：

（1） 申请人通过其主导的技术创新活动，在中国依法拥有产品核心技术发明专利权，或者依法通过受让取得在中国发明专利权或其使用权，创新医疗器械特别审查申请时间距专利授权公告日不超过 5 年；或者核心技术发明专利的申请已由国务院专利行政部门公开，并由国家知识产权局专利检索咨询中心出具检索报告，报告载明产品核心技术方案具备新颖性和创造性。

（2） 申请人已完成产品的前期研究并具有基本定型产品，研究过程真实和受控，

[4] 《特别审查程序》第十三条、第十七至第十九条
[5] 《特别审查程序》第十二条
[6] 《特别审查程序》第二条

研究数据完整和可溯源。

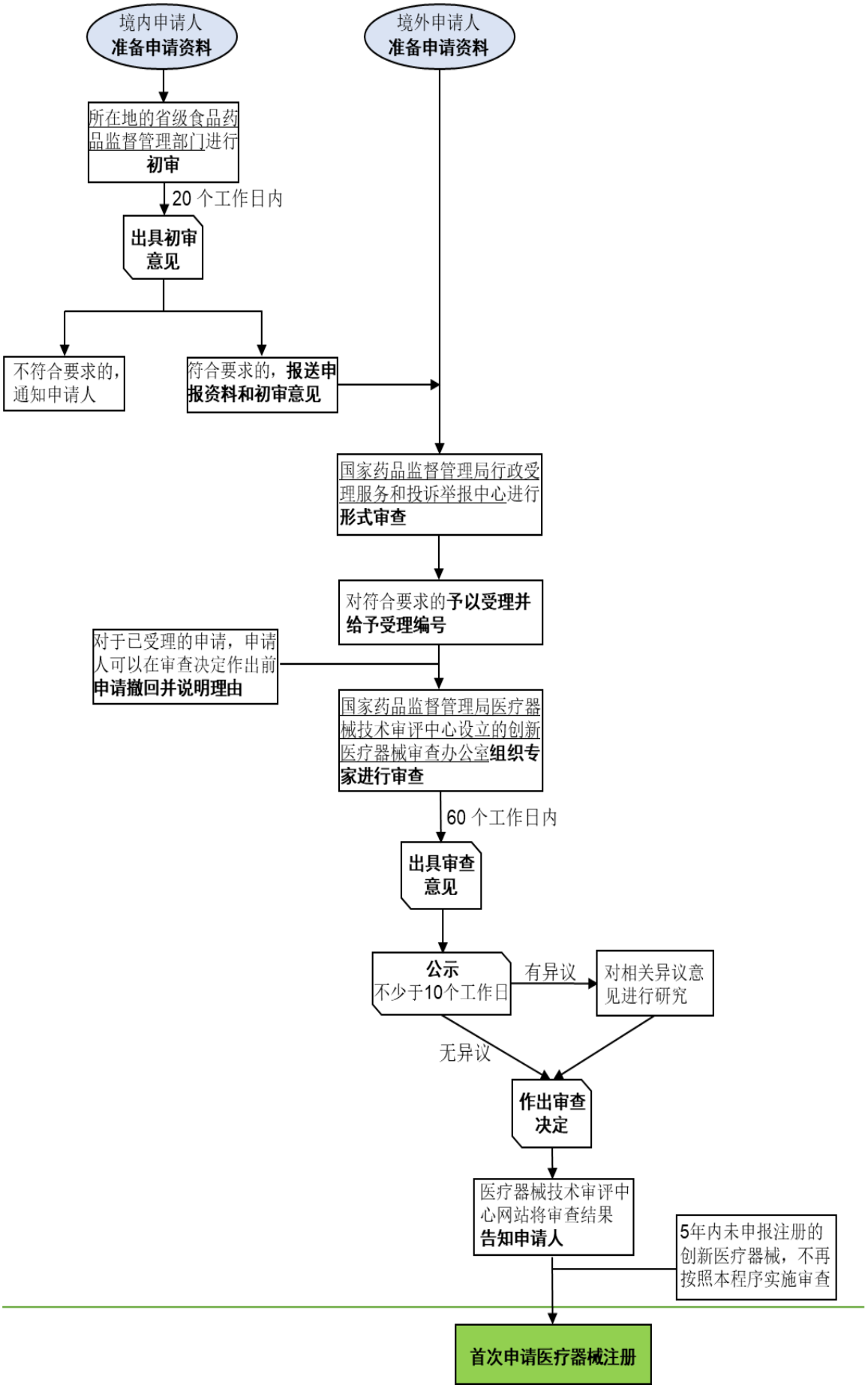
（3） 产品主要工作原理或者作用机理为国内首创，产品性能或者安全性与同类产品比较有根本性改进，技术上处于国际领先水平，且具有显著的临床应用价值。

尽管相较于《特别审查程序（试行）》，《特别审查程序》删去了“同时符合”三项适用情形的措辞，但从适用情形的实质而言，申请人仍应当做到同时符合。三项适用情形的核心仍然是产品具有创新性，不仅需要是国内首创并且较同类产品具有根本性改进，所有权或使用权，或者具有获得专利可能性的证明。同时，产品应当已经完成前期研究并基本定型。避免产品最终的安全性和有效性发生显著偏移。

此外，创新医疗器械特别审查程序仅针对二类和三类进口以及国产医疗器械的首次注册，对于一类医疗器械备案以及所有类别医疗器械的延续注册或许可事项变更不适用。

五、 适用程序

依据《特别审查程序》的相关规定，创新医疗器械的特别审查程序主要包括对境内申请人的申请项目进行初审、对境内申请人和境外申请人的申请申报资料进行形式审查以判断是否受理、对受理的申请项目进行审查并出具审查意见、经公示与异议处理后作出审查决定。以下流程图反映了《特别审查程序》中的申报和审查流程。


境内申请人
准备申请资料
境外申请人
准备申请资料
所在地的省级食品药品监督管理部门进行
初审
20 个工作日内
出具初审意见
不符合要求的，通知申请人
符合要求的，**报送申报资料和初审意见**
国家药品监督管理局行政受理服务和投诉举报中心进行
形式审查
对符合要求的**予以受理并给予受理编号**
对于已受理的申请，申请人可以在审查决定作出前**申请撤回并说明理由**
国家药品监督管理局医疗器械技术审评中心设立的创新医疗器械审查办公室**组织专家进行审查**
60 个工作日内
出具审查意见
公示
不少于10个工作日
有异议
对相关异议意见进行研究
无异议
作出审查决定
医疗器械技术审评中心网站将审查结果**告知申请人**
5年内未申报注册的创新医疗器械，不再按照本程序实施审查
首次申请医疗器械注册

六、 影响

据统计，自 2014 年至 2018 年期间，共计 197 项产品被国家药监局纳入创新医疗器械的特别审查程序，除 2018 年数量略有下降外，自 2014 年以来，获准进入特别审查程序的产品逐年上升。更重要的是，通过特别审查程序完成医疗器械注册产品的数量也在逐年增长，2018 年达到了最高值，共 21 项创新医疗器械产品获批。

不难看出，创新医疗器械的特别审查程序，对于具有核心专利和自有研发能力的医疗器械开发企业而言，可以加速其产品上市时间，减轻注册周期长带来的成本压力。对于市场上的创新型企业，特别是着眼于开发国内首创、国际领先技术的创新企业，例如医疗人工智能企业、基因测序产品开发企业，实现提前布局占领市场，获得先发优势，有着重要意义。

曹思思为环球律师事务所上海办公室的律师，其主要执业领域为争议解决、合规、劳动、破产重整等。

邮箱： kellycao@glo.com.cn

王冠洁为环球律师事务所上海办公室的律师，其主要执业领域为医药健康法、并购、风险投资、合规及公司法。

邮箱： feliciawang@glo.com.cn

生物新技术临床研究新规范及与临床试验质量管理规则的比较

作者： 赵烨韵 I 尤鹏飞

2 月 26 日，国家卫生健康委发布了由其起草的《生物医学新技术临床应用管理条例（征求意见稿）》（以下简称“**意见稿**”），对于生物医学新技术临床研究及应用进行了规范。

近年来，随着关键技术突破，医学技术发展迅速，各种生物医学技术不断问世，例如克隆技术、辅助生育、靶向治疗等。相比传统的医疗技术，一方面生物医学技术为预防、治疗病情，增进人类健康提供了新的手段，另一方面，如果在临床研究和应用中行为不当，也会产生对个人权利、公共安全的侵害以及社会伦理问题。但是，相对于药物、医疗器械临床试验已经出台了较为完善的管理规范，非药物、非医疗器械的新型医学技术的临床研究和应用的管理还十分缺乏。

目前，我国针对临床试验系统性规定主要有《药物临床试验质量管理规范》及《医疗器械临床试验质量管理规范》（统称“GCP”），而针对生物医学技术临床试验的规定更为碎片化，有针对伦理审查的《涉及人的生物医学研究伦理审查办法》，针对医疗机构项目管理的《医疗卫生机构开展临床研究项目管理办法》，有针对具体某类生物医学技术的《干细胞临床研究管理办法（试行）》、《人类辅助生殖技术规范》等。各法规之间有重合，但适用范围有限。缺少类似 GCP 的系统化规范。

就在贺建奎宣布中国诞生首例基因编辑婴儿后三个月，卫健委发布了意在整合并规范生物医学技术临床研究及应用的意见稿，可以被视作是对基因编辑婴儿事件暴露的监管漏洞的迅速回应，也是旨在加强对所有生物医学新技术临床应用风险的预防。

本文旨在介绍该意见稿如何完善生物医疗新技术临床研究监管模式，并通过与现行临床研究质量管理规范进行比较分析意见稿尚需完善之处。

一、 法规介绍

此次意见稿针对的是拟作用于细胞、分子水平的，以对疾病作出判断或预防疾病、消除疾病、缓解病情、减轻痛苦、改善功能、延长生命、帮助恢复健康等为目的的医学专业手段和措施。

该意见稿填补生物医学技术临床研究及应用的法规空白，从增加外部审查、提高内部监管水平、以及加强处罚力度三个方面加强了对于此类临床研究的监管。

(一) 首次引入外部分级审批制度

目前，根据《涉及人的生物医学研究伦理审查办法》针对生物医学研究的外部监管仅限于伦理委员会的设立及研究的备案，缺乏有效的外部审查导致生物医学研究的监管不利，根据各个机构的伦理委员会审查标准不同，各机构开展的生物医学研究的严谨性、安全性也良莠不齐。

意见稿建立了生物医学新技术临床研究和转化应用[1]行政审批制度，规定医疗机构开展生物医学新技术临床研究和转化应用必须经过行政部门批准。其中，临床研究是指在临床应用前在人体进行试验， 而转化应用是指经临床研究验证安全有效且符合伦理的生物医学新技术，经一定程序批准后在一定范围内或广泛应用的过程。[2]开展生物医学新技术临床研究和转化，需要首先通过医院内审，然后向医疗机构所在的省级卫生主管部门提出申请。省级

[1] 《生物医学新技术临床应用管理条例(征求意见稿)》第五条：生物医学新技术转化应用（以下简称转化应用）是指经临床研究验证安全有效且符合伦理的生物医学新技术，经一定程序批准后在一定范围内或广泛应用的过程。

[2] 《生物医学新技术临床应用管理条例(征求意见稿)》第六条

卫生机构依法自行审批或初审之后提交国务院卫生主管部门审批。未经审批不得开展临床研究[3]。此意见稿进一步根据临床研究风险等级进行分类管理，对于中低风险研究项目由省级卫生主管部门审批，高风险研究项目由省级卫生主管部门审核后国务院卫生主管部门审批。根据意见稿，高风险生物医学新技术包括但不限于以下情形：[4]

1. 涉及遗传物质改变或调控遗传物质表达的，如基因转移技术、基因编辑技术、基因调控技术、干细胞技术、体细胞技术、线粒体置换技术等；
2. 涉及异种细胞、组织、器官的，包括使用异种生物材料的，或通过克隆技术在异种进行培养的；
3. 产生新的生物或生物制品应用于人体的，包括人工合成生物、基因工程修饰的菌群移植技术等；
4. 涉及辅助生殖技术的；
5. 技术风险高、难度大，可能造成重大影响的其他研究项目。

可以看到，之前备受诟病的基因编辑研究被明确列为高风险研究项目，需要获得省级及国家卫生主管部门的双重审批。

但是，此规定除却明示列举的高风险项目之外，对于风险评级的规定仍过于宽泛。仅依照意见稿文本，对于何种研究项目属于“技术风险高、难度大、可能造成重大影响”的项目还难以判断。从法理角度究其原因，意见稿并未对“高风险”的标准进行概括规定，而直接进行了列举。作为列举的兜底条款，“技术风险高、难度大、可能造成重大影响”的概念在实际操作中并未比“高风险”的概念更细化。模糊的标准可能导致各地审批严格程度不同，或研究机构无法确定应该获得哪个层级的审批。另外，生物医学新技术风险目录是否真的可以有效地涵盖所有高风险的研究还有待商榷。通过目录来控制高风险研究固然可以使各地的审批标准统一，但是目录具有滞后性，是否能够适应

[3]《生物医学新技术临床应用管理条例(征求意见稿)》第十七条、第十八条、第二十五条
[4]《生物医学新技术临床应用管理条例(征求意见稿)》第七条

不断更新、发展的医学研究，对于新兴的医学研究是否能够前瞻性地判断其风险，还是有待进一步观察。

对医疗机构和研究人员资质提出更高要求

该意见稿另一个重要突破，是规定了开展生物医学新技术临床研究医疗机构和项目主要负责人的条件，提高了现行法律法规中对生物医学临床试验的资格要求。

此前在《涉及人的生物医学研究伦理审查办法》中，所有医疗机构都可以设立伦理委员会。而药物、医疗器械的临床试验均要求在经过审批的有资质的机构中展开。与药物、医疗器械临床试验相比，开展医学技术临床研究的资质要求过低，导致许多缺乏研究、试验能力的医疗机构滥设伦理委员会，开展一些不符合要求的研究。

而该意见稿规定只有三级甲等医院或三级甲等妇幼保健院可以开展生物新技术临床研究。这个要求与第三类医疗器械临床试验的机构要求一致，虽然药物临床试验没有要求三甲医院，但是大部分经过资质认定的都是三甲医院。

意见稿对于符合资质的医疗机构未作出审批或备案的要求。自 2018 年起，医疗器械临床试验机构的资质认定也从审批制改为备案制。根据《关于深化审评审批制度改革鼓励药品医疗器械创新的意见》及《药物临床试验机构管理规定（征求意见稿）》，药品临床试验机构也计划改为备案制。而此意见稿不设置备案或审批要求的“一刀切”的规定进一步简化了程序，有利于分担临床试验的压力，但也可能产生不利影响。首先，不论试验风险高低，一律只允许三级甲等医院进行临床试验，导致部分具有研究能力的非三甲医院无法参与研究，例如，上海市徐汇区中心医院为二级医院，但经过认定，具有进行呼吸内科、肿瘤科、内分泌、医学影像（诊断）、康复医学（心脑血

管）、神经内科药品临床试验的资质。其次，经过备案或审批，卫生主管部门可以重点监管经备案或审批的医疗机构实施临床试验的情况。而如果不设置备案或审批程序，则卫生主管部门需要对所有三甲医院都加以监管，提高了监管的难度和范围。

针对研究人员，该意见稿要求临床研究项目申请由项目负责人向所在医疗机构指定部门提出，研究项目负责人应当同时具备执业医师资格和高级职称，具有良好的科研信誉。这一规定有效地避免了贺建奎事件中，不具有医师执业资质的研究人员申请并负责研究项目的情况。

依照该要求，生物医学新技术的临床研究项目负责人在执业资格、职称要求以及任职场所有了新的要求。不仅诸如生物学者等未取得执业医师资格证的科研人员不能再担任临床研究的项目负责人，开展研究的医疗机构之外的执业医师也不能在其他医疗机构担任项目负责人。除了项目负责人外，在人体进行的操作及涉及的具体诊疗操作，应当由医务人员完成。[5] 这一规定具有其合理性。首先，作为涉及人体的医学研究，生物医学新技术的目的对疾病作出判断或预防疾病、消除疾病、缓解病情、减轻痛苦、改善功能、延长生命、帮助恢复健康。这个定义对于与《医疗机构管理条例实施细则》中对于诊疗行为的定义，即“通过各种检查，使用药物、器械及手术等方法，对疾病作出判断和消除疾病、缓解病情、减轻痛苦、改善功能、延长生命、帮助患者恢复健康的活动。”[6]如出一辙。在此定义下，研究行为本身就包含了诊疗行为，而实施诊疗的主体应当具备医师执业资格，否则可能构成非法行医。[7]另一方面，从执法层面上来说，医疗机构对于其聘任的医生有一定监管能力，而对于外部的研究人员缺乏有效的监管。另外，对于违反本条例规定开展临床研究和转化应用的情形，卫生主管部门对于执业医师也可以做出吊销执照、禁止执业等处罚。因此，明确研究人员必须具备执业资质，既是

[5] 《生物医学新技术临床应用管理条例(征求意见稿)》第九条，第二十九条
[6] 《医疗机构管理条例实施细则》第八十八条
[7] 《中华人民共和国刑法》第三百三十六条；《最高人民法院关于审理非法行医刑事案件具体应用法律若干问题的解释》

实施研究的需要，也是加强监管的需要。

(二) 加大处罚力度并明确个人责任

针对现有规定处罚力度弱，无法形成威慑的问题，该意见稿加大了违规行为的处罚范围及处罚力度。

首先，目前已出台的《涉及人的生物医学研究伦理审查办法》及《医疗卫生机构开展临床研究项目管理办法》中的罚则针对的都是医疗机构，涉及个人违法进行此类研究的都参照其他法律进行处罚，在法律的适用和责任的认定和划分上往往存在着困难。而此意见稿加入了对于个人的处罚，包括对医疗机构主要负责人和其他直接责任人员依法给予处分、对于所有医务人员进行警告、罚款、吊销执业证书，终生不得从事生物医学新技术临床研究。对于个人擅自开展临床研究，可以责令停止活动、取缔研究场所、没收设备、罚款。

其次，此意见稿也加强了处罚的力度和方式。在《涉及人的生物医学研究伦理审查办法》中，当医疗机构及其伦理委员会违法审查时，由县级以上地方卫生计生行政部门责令限期整改，并可根据情节轻重给予通报批评、警告；对机构主要负责人和其他责任人员，依法给予处分。[8]此次对于医疗机构的处罚增加了罚款、取消相关诊疗科目且5年内不得申请该诊疗科目、暂停执业、吊销执业证书、终生不得从事生物医学新技术临床研究的罚则。[9]

其中，取消诊疗科目及终生不得从事生物医学新技术临床研究都是较为少见的处罚方式，但是对于机构的威慑力可能更高于罚款，也能够有效避免医疗机构再三违法实施临床研究。

[8] 《涉及人的生物医学研究伦理审查办法》第四十六条
[9] 《生物医学新技术临床应用管理条例(征求意见稿)》第五十条,第五十三条

值得注意的是，此次还明确提出提供虚假资料或采用其他欺骗手段的，5 年内不受理相关责任人及单位提出的相关申请。可以看出，对于贺建奎事件中涉及的临床研究备案中造假问题，这次意见稿也明确做出了反应，可以看出卫健委在打击贺建奎之类的违规临床研究的态度和决心。

二、 与药物、医疗器械临床试验管理规定的比较

如前文所述，《药物临床试验质量管理规范》及《医疗器械临床试验质量管理规范》对于药物及医疗器械临床试验作出了较为系统的规定。质量管理规范与《药品管理法》、《医疗器械监督管理条例》、《医疗器械临床试验机构条件和备案管理办法》等法律法规共同构成了相对比较成熟的临床试验规范体系。因此，通过与药物、医疗器械临床试验的规则进行比较，可以看到该意见稿的亮点与不足，具体见下表：

	药物	医疗器械	生物医学新技术
研究机构	符合资质要求、通过资质认定的医疗机构[10]	符合资质要求、经过备案的医疗器械的医疗机构。[11]	有条件的三级甲等医院或三级甲等妇幼保健院。[12]
负责人资质要求	在该医疗机构中具有相应专业技术职务任职和行医资格	在该医疗机构中具有副主任医师、副教授、副研究员等副高级以上相关专业技术职称和资质[13]	具备执业医师资格和高级职称，具有良好的科研信誉。主要研究人员应当具备承担该项研究所需的专业知识背

[10] 《药物临床试验质量管理规范》第二十二条,《药物临床试验机构资格认定办法（试行）》第六条
[11] 《医疗器械临床试验机构条件和备案管理办法》 第四条
[12] 《生物医学新技术临床应用管理条例(征求意见稿)》第十二条
[13] 《医疗器械临床试验质量管理规范》第六十一条

			景、资格和能力。[14]
其他研究人员	无特殊要求	熟悉试验用医疗器械的原理、适用范围、产品性能、操作方法、安装要求以及技术指标，了解该试验用医疗器械的临床前研究资料和安全性资料，掌握临床试验可能产生风险的防范以及紧急处理方法。[15]	涉及的具体诊疗操作，必须由具备相应资质的卫生专业技术人员执行；在人体进行的操作应当由医务人员完成。[16]
对受试者的赔偿	申办者应对参加临床试验的受试者提供保险，对于发生与试验相关的损害或死亡的受试者承担治疗的费用及相应的经济补偿。[17]	申办者应当为发生与临床试验相关的伤害或者死亡的受试者承担治疗的费用以及相应的经济补偿，但在诊疗活动中由医疗机构及其医务人员过错造成的损害除外。[18]	无特殊规定（按照国家有关规定予以赔偿）
试验/研究的实施细则	试验方案内容、记录与报告的管理、监查员制度、数据管理与统计分析、多中	试验方案内容、监查员制度、数据管理与统计分析、多中心临床试验、医疗器械管理、文件管理等。	及时记录，保留材料[19]

[14] 《生物医学新技术临床应用管理条例(征求意见稿)》第十四条
[15] 《医疗器械临床试验质量管理规范》第六十四条
[16] 《生物医学新技术临床应用管理条例(征求意见稿)》第九条，第二十九条
[17] 《药物临床试验质量管理规范》第四十三条
[18] 《医疗器械临床试验质量管理规范》第四十八条
[19] 《生物医学新技术临床应用管理条例(征求意见稿)》第三十条

	心临床试验、药品管理等。		
受试者的权益保障	不良事件报告、情况说明、知情同意书等。	不良事件报告、情况说明、知情同意书	尊重受试者知情同意权、随访监测。关于不良事件，仅笼统地规定了出现严重不良反应或事件、差错或事故等，要立即报告省级人民政府卫生主管部门。
内部审查	获得该医疗机构伦理委员会的同意。	获得该医疗机构伦理委员会的同意。	获得该医疗机构的学术审查委员会和伦理审查委员会同意。[20]
外部审批/备案要求	经国务院药品监督管理部门批准后，方可进行临床试验[21]	并向临床试验提出者所在地省、自治区、直辖市人民政府食品药品监督管理部门备案。[22] 第三类医疗器械进行临床试验对人体具有较高风险的，应当经国务院食品药品监督管理部门批准。	对于申请开展高风险生物医学新技术临床研究的，省级人民政府卫生主管部门进行初步审查，并出具初审意见后，提交国务院卫生主管部门。[23]

[20] 《生物医学新技术临床应用管理条例(征求意见稿)》第八条，第十六条
[21] 《药品管理法》第二十九条
[22] 《医疗器械临床试验质量管理规范》第十八条
[23] 《生物医学新技术临床应用管理条例(征求意见稿)》第七条

罚则	药品生产、经营企业、医疗机构：警告，责令限期改正；逾期不改正的，责令停产、停业整顿，并处5千元-2万元的罚款；情节严重的，吊销《药品生产许可证》、《药品经营许可证》和药物临床试验机构的资格。[24]	医疗机构：责令改正或者立即停止临床试验，处5万元-10万元罚款；造成严重后果的，该机构5-10年内不得开展相关专业医疗器械临床试验。 个人：依法对直接负责的主管人员和其他直接责任人员给予降级、撤职或者开除的处分	医疗机构：责令限期整改；逾期不改正的，予以警告，暂停执业、3万元以上5万元以下罚款，有违法违规收入的，没收违法违规所得，并处违法违规所得10倍以上20倍以下罚款；造成严重后果的，取消相关诊疗科目，5年内不得申请该诊疗科目。[25] 个人：警告，暂停执业，吊销执业证书，5年至终身不得从事生物医学新技术临床研究；有违法违规收入的，没收违法违规所得，并处违法违规所得10倍以上20倍以下罚款。[26]

[24] 《药品管理法》第七十八条
[25] 《生物医学新技术临床应用管理条例(征求意见稿)》第五十条,第五十一条,第五十二条,第五十五条
[26] 《生物医学新技术临床应用管理条例(征求意见稿)》第五十五条,第五十三条

通过和药物、医疗器械临床研究管理规范进行比较，可以发现意见稿在大框架上对于临床研究的审批流程及监管基本都作了规定，且在诸如研究人员资质、针对个人的处罚等条款上更为严格。但是其内容还有待进一步细化，缺乏对于受试者的权利保护的规定（如强制购买保险）、试验过程管理等有指导性的细则等。例如，在药物、医疗器械临床研究管理规范中，对于发生不良反应或事件的情况，要求研究者采取治疗，记录在案，在总结时对不良事件进行描述和评价，并在发生严重不良事件时报告监督管理部门，而在意见稿中仅笼统地规定了"临床研究或转化应用过程中出现严重不良反应或事件、差错或事故等，要立即报告省级人民政府卫生主管部门"，[27]并未对受试者的治疗、不良反应的记录等给出详细的规定，缺乏一定的指导性和可操作性。

虽然生物医学技术的临床研究与药品、医疗器械不同，主要由研究者、研究机构主导，而非药品、医疗器械生产企业主导，将负责医疗机构限定在三甲医院一定程度上可以控制风险，如果出现需要赔偿的情况，三甲医院通常也有一定的偿付能力。但是，考虑到生物新技术医学研究的高风险，亟需国家出台进一步的管理细则，对临床研究的细节进行规定，实现对试验全流程的有效监管和风险防范。

三、 小结

兼备宽松的管制与先进的生物科技水平，中国曾被认为是生物医学技术的一片"自由热土"。

在贺建奎事件发生之前，有学者梳理了主要法域对基因编辑技术的法律限制[28]，认为中国现行限制规定的强制性较弱，且相关文件的法律位阶较低[29]。中国现行法缺少对包括了生物医学技术研究与应用的成体系监管，其原因一方面是法律规范的天然滞后性，另一方面是中国法此前未曾受到事件刺激。西方国家有着更多的对

[27] 《生物医学新技术临床应用管理条例(征求意见稿)》第四十五条
[28] Araki, M. and Ishii, T., 2014. International regulatory landscape and integration of corrective genome editing into in vitro fertilization. Reproductive biology and endocrinology, 12(1), p.108.
[29] 2003 年科学技术部和原卫生部颁布《人胚胎干细胞研究伦理指导原则》（以下简称《指导原则》），规定进行人胚胎干细胞研究，利用体外受精、体细胞核移植、单性复制技术或遗传修饰获得的囊胚，其体外培养期限自受精或核移植开始不得超过 14 天。但《指导原则》没有规定此类研究的主体责任归属，这意味着，违反该《指导原则》也无从惩罚。

涉及人的研究的限制，包括更严格的伦理审查要求[30]。这些法律限制主要并非源于西方立法机构的远见，而是二战之后西方社会对草率的人体实验及其严重后果的应激反应与反思。[31]中国的法律人深知运动式立法并不可取，但也理解法律漏洞急需填补。贺建奎事件后的短短几个月内，卫健委就协同各部门及专家起草了这份意见稿，为规范生物医学新技术的临床研究和应用草拟了框架，在一定程度上弥补此类临床研究监管的不足。意见稿对于研究者、研究机构来说明确了研究中需要承担的义务，对其提出了更高的合规要求，对于违规的处罚也更为严格，这些要求一定程度上可以降低研究的风险。但是，与现有的两部药品和医疗器械临床试验管理规范相比，该意见稿缺少可供研究者、研究机构参考的指导性细则，部分条款有待进一步确认和细化。

赵烨韵为环球律师事务所上海办公室的律师助理，其执业领域主要涵盖医药和健康、日常公司事务。

邮箱：verazhao@glo.com.cn

尤鹏飞为环球律师事务所上海办公室的律师助理，其执业领域主要涵盖医药和健康、广告法与竞争法。

邮箱：pengfeiyou@glo.com.cn

[30] 详见 2019 年第一期环球生命科学及医疗法律专递，基因编辑胎儿研究看我国的审查制度及胚胎实验的法律后果，伦理委员会相关章节。

[31] 如，二战结束后因纽伦堡审判而产生的一部人类试验科研伦理准则《纽伦堡规范》；又如，1972 年媒体曝光以 400 名非洲裔黑人男子为试验品秘密研究梅毒的实验（“塔斯基吉梅毒实验”）后发布的《贝尔蒙报告》。

“互联网＋护理服务”试点工作方案之解读

作者：董秋艳 I 李艺辉

一、 引言

护理资源紧缺的问题在我国由来已久。虽然我国护理人员的绝对数量较大，但相比极其庞大的人口基数而言，护理人员数量占总人口数的比例较低，无法充分满足现实的护理需求。而随着中国社会老龄化程度的加深，需要居家护理服务的高龄、失能、半失能老年人群不断扩大，使得护理资源紧缺的情况变得更加明显。除了扩大我国护理人才的培养规模、增加护理人员的绝对数量以外，更加充分、高效地利用现有的护理资源也是解决短缺问题的一个重要手段。“互联网+”风潮的发展让人们看到了互联网技术对行业产生颠覆性影响的可能性，虽然受限于目前互联网技术的发展程度，以及一些行业自身的特性，与互联网结合的行业并非都像餐饮、出租汽车一样因互联网技术而发生重大变革，但仍然受到了或多或少的影响，一些行业也仍处在探索与互联网更深、更好结合的过程中，“互联网+护理服务”正是其中之一。

推动“互联网+护理服务”的发展存在迫切的现实需求。也正因此，在国家尚未出台相关法规之时，实践中的尝试就已经先行一步了。近几年，“网约护士”、“共享护士”的概念时常出现在媒体中，并且出现了一批知名度相对较高的“网约护士”平台，如“医护到家”、“金牌护士”、“滴滴护士”等。但总体而言，“互联网+护理服务”的先期实践由于缺乏政策指导和统一性、强制性的制度安排而显示出诸多乱象。前期实践中常见的操作方式是，护理人员自行向平台注册并通过平台接单，然后到患者家中上门服务。一些平台除了吸纳医院在职的护理人员接单、服务以外，还允许已经离岗、退休的护理人员提供上门护理服务。这种操作方式不仅具有很大的安全风险，在实践中引发了一些对患者产生伤害的案例[1]，而且根据现行法规，护理服务作为一种诊疗活动只能由取得许可的医疗机构来实施，护士自行在院外提供护理服务的行为已经超出了相关法规所允许的在注册执业地点执业的范畴。

[1] 据相关新闻报道，某患者通过互联网平台预约护士上门注射针剂，护士未按照说明对针剂进行稀释，导致患者出现不良反应。

正是基于迫切的现实需求和混乱的实践，2019 年 1 月 22 日，国家卫生健康委办公厅（以下简称“国家卫健委”）出台了《关于开展“互联网+护理服务”试点工作的通知》（以下简称“《试点方案》”），就“互联网+护理服务”的试点工作做出了初步的制度安排。本文将对《试点方案》进行介绍和解读。

二、 《试点方案》的规定

(一) 试点安排

根据《试点方案》的规定，“互联网+护理服务”的试点将主要在六个省市开展，包括北京市、天津市、上海市、江苏省、浙江省、广东省，其他省份可以结合实际情况选取试点城市或地区开展试点工作。试点的时间期限为 2019 年 2 月至 12 月。

除了国家卫健委制定的《试点方案》之外，各个试点省市还需要结合地方实际情况出台更为详细的、当地化的试点安排。《试点方案》规定，各试点省份应于 2019 年 2 月 25 日前报送试点实施方案，但截至成文时为止，通过公开渠道能查询到的仅有浙江省卫健委出台的《关于征求<浙江省“互联网+护理服务”试点工作实施方案>的通知》（以下简称“浙江省《试点方案征求意见稿》”），其他省市的地方试点方案则有待后续的公开发布。

(二) “互联网+护理服务”的含义

《试点方案》中明确，“互联网＋护理服务”主要是指医疗机构利用在本机构注册的护士，依托互联网等信息技术，以“线上申请、线下服务”的模式为主，为出院患者或罹患疾病且行动不便的特殊人群提供的护理服务。根据该定义可知，“互联网+护理服务”延续了前期实践中的 O2O 模式，通过互联网信息技术平台将传统护理服务的提供方和需求方进行连接、匹配，并且改变了护理服务发生的地点，即从医疗机构内变为患者家中。护理服务的核心提供方仍为医疗机构，医疗机构既可以自建互联网信息技术平台，也可以

与第三方平台合作，实现护理服务需求的线上对接。

(三) 所涉服务主体的资质要求

在《试点方案》出台之前，前期实践中的所谓“互联网+护理服务”普遍由护理人员自行通过信息技术平台接单并提供服务，即，护理人员以其自身作为服务提供方，医疗机构则并不参与任何服务环节。在此情况下，对于执业护士来说，由于其系以个人名义接受患者订单，其所执业的医疗机构并不直接介入服务过程，只能依据内部管理制度对护士兼职进行管理，甚至很可能对机构内护士提供上门护理服务的情况并不知悉，也难以进行有效管控；而对于离岗、退休的护理人员来说，其行为已经完全脱离了卫生主管部门及医疗机构的管理，无法受到有效的监督。为了保障上门护理服务的质量并与现行护士执业制度接轨，《试点方案》明确将医疗机构纳入“互联网+护理服务”的重要一环，“互联网+护理服务”所涉及的服务提供主体因此从两方变为三方：

(1) 医疗机构

在我国现行法律框架下，护士并没有作为独立个体执业的空间，能够合法提供护理服务的只有医疗机构，护士只能作为受到医疗机构管理、指派的人员为患者提供护理服务。《试点方案》引入了整个医疗机构，将实践中护理人员自行为患者提供上门护理服务的模式，转变为医疗机构为患者提供护理服务，并派驻执业护士上门进行具体服务的模式，使得“互联网+护理服务”合法合规化。

根据《试点方案》的规定，提供“互联网+护理服务”的实体医疗机构应当合法持有医疗机构执业许可证，并且其执业许可中应当包括家庭病床、巡诊等服务方式。据此，可以初步确认提供服务的医疗机构除了需要具备相应的执业许可外，还应为实体医疗机构，仅以互联网医院作为第二名称的实体医疗机构显然应当符合前述要求，但对于依托实体医疗机构而独立设置的互联网医院是否满足开展“互联网+护理服务”

的资质条件则仍存有疑问。笔者认为，从谨慎开展试点工作的角度出发，本次试点阶段将依托实体医疗机构独立设置的互联网医院排除在外具有一定的合理性，但在试点后的正式实施阶段，是否将依托实体医疗机构而独立设置的互联网医院也纳入其中或许有待依据互联网医院的整体发展情况来确定。《互联网医院管理办法（试行）》于 2018 年 7 月 17 日方开始施行，迄今为止的实践经验比较有限，有赖于通过更长期的实践来考察依托实体医疗机构而独立设置的互联网医院能否保证护理服务质量、是否适于提供“互联网+护理服务”。

特别地，浙江省《试点方案征求意见稿》中则进一步要求，提供护理服务的医疗机构应取得互联网诊疗许可或者设置互联网医院，也就是说，在浙江省，未具有互联网诊疗相关条件的单纯的实体医疗机构并不能提供“互联网+护理服务”。笔者认为，这一安排将进一步缩小可提供“互联网+护理服务”的医疗机构的范围，与激活现有护理资源、满足日益扩大的护理需求的初衷似乎不完全一致，将有待试点阶段的进一步观察判断。

(2) 护士

对于网约汽车这类差异性较小、同质化程度很高的服务来说，服务需求方通常不需要对服务提供方做过于复杂的筛选，便可以获得质量比较稳定的服务。但对于护理服务而言，护士的学历、职称、技术水平、临床经验等因素的区别往往都意味着护理服务质量的较大差异。加之，上门护理服务对患者的生命健康存在相对较高的风险，所以，对提供上门护理服务的护士设置更高的门槛是必要的。根据《试点方案》，可以提供上门护理服务的护士除了需满足持有护士执业证书这一基本要求以外，还应当具备五年以上的临床护理工作经验和护师以上技术职称，如发生违法违规行为或者不良执业行为记录的，还应依据退出机制实施淘汰。为“互联网+护理服务”人员设置相对更高的资质要求，对于保证护理服务的质量是非常有益的。

(3) 互联网信息技术平台

“互联网+护理服务”中的互联网信息技术平台作为护患双方联系的纽带，可以由医疗机构自行建设，也可以由与医疗机构开展合作的、具备资质的第三方平台来建设。从《试点方案》的规定来看，目前对互联网信息技术平台并不设置专门的资质许可，只是列明了平台应当满足的技术性、功能性要求，包括应当具备相应的设备设施、技术、人员，确保能够实现身份识别、信息采集和保护、服务人员定位追踪、服务行为追溯、信息和隐私保护等基本功能。所以，试点阶段的互联网信息技术平台主要关注的应是在技术、功能层面能否符合要求。

此外，考虑到护理服务的特殊性，互联网信息技术平台可能还会涉及到患者隐私保护及病历数据保护的相关问题，因此应当特别关注互联网信息技术平台在网络安全及个人数据保护合规性方面的实践与管理，本文不就此展开。

(四) 服务内容

“互联网+护理服务”意在为患者接受护理服务提供更多便利，但基于护理服务天然的风险性，并非所有护理服务都能够或适合于脱离医疗机构的环境而在患者家中进行。对于哪些服务允许或不允许以“互联网+护理服务”的方式进行，《试点方案》中并未作详细规定。但是，《试点方案》中明确，“互联网+护理服务”的重点服务对象是高龄或失能老年人、康复期患者和终末期患者等行动不便的人群。事实上，开展“互联网+护理服务”试点的重要背景正是老年疾病人群的扩大，所以，“互联网+护理服务”试点从一开始便是与解决我国的老龄化问题相联系的。

临床护理活动包括多个类别和具体项目，[2]但对于“互联网+护理服务”所允许

[2] 《临床护理实践指南（2011 版）》中列举了十七个类别的临床护理项目，包括清洁与舒适管理、营养与排泄护理、身体活动管理、常见症状护理、皮肤、伤口、造口护理、气道护理、引流护理、围手术期护理、常用监测技术与身体评估、急救技术、常用标本采集、给药治疗与护理、化学治疗、生物治疗及放射治疗的护理、孕产期护理、新生儿及婴幼儿护理、血液净化专科护理、心理护理。

的服务项目，《试点方案》要求仅限于需求量大、医疗风险低、易操作实施的类型，而在具体项目上，则要求各试点省份应在遵循前述原则的前提下，根据其实际需求来确定，并建议采用“正面清单”+“负面清单”的方式来规定。

妥善确定允许的上门护理服务项目对于保障医疗质量和安全是至关重要的。浙江省《试点方案征求意见稿》中罗列了允许的 30 个服务项目，包括健康促进、常用临床护理、专科护理三大类别，具体项目分别涵盖生活自理能力训练、肌肉注射、普通造口护理等等。对于一些特殊类型的服务项目，护士还需要满足特殊的资质要求，例如提供母婴护理、普通造口护理的护士应当取得专科护士培训合格证，或具有副主任护士及以上技术职称并在相关专科工作三年以上。

另外可供参考的是，北京市卫健委及相关部门曾于 2018 年 12 月 25 日出台了《关于发展和规范互联网居家护理服务的通知》，该通知列明了北京市互联网居家护理服务项目的目录，同样包括健康促进、常用临床护理、专科护理三大类别，涵盖了生活自理能力训练、肌肉注射、造口护理等 25 个服务项目。在护士资质上，除了专科护理项目要求应为专科护士以外，其他项目均要求为执业护士。该通知中的部分规定与《试点方案》并不完全一致，[3]且其颁布的时间在《试点方案》出台之前，鉴于《试点方案》已经发布生效，该通知是否将继续适用存在较大疑问，而且《试点方案》要求各试点省市制定试点实施方案，所以北京市应当重新制定“互联网+护理服务”的相关规定。因此，笔者认为，虽然该通知具有一定的参考意义，但未来的落地实施还需要依据北京市制定的“互联网+护理服务”试点实施方案来操作。

(五) 上门护理前的首诊

[3] 《试点方案》要求提供“互联网+护理服务”的护士应具有五年以上临床护理工作经验，而北京市《关于发展和规范互联网居家护理服务的通知》仅要求三年以上临床护理工作经验；《试点方案》要求医疗机构在提供“互联网+护理服务”前应当对患者进行首诊，而北京市《关于发展和规范互联网居家护理服务的通知》要求医疗机构需在服务前对患者进行综合评估，并与患者签订知情同意书。

为了控制护理服务中的风险，避免上门护理可能对患者造成的人身损害，《试点方案》要求医疗机构在提供“互联网＋护理服务”前需要对接受服务的患者进行首诊，对其疾病状况、健康需求等情况进行评估，只有经评估认为可以提供“互联网＋护理服务”的，方可派出护士上门提供服务。针对此处所称的“首诊”，笔者认为医师除了需对疾病本身做出诊断结论以外，还需要就患者是否适合接受上门护理服务给出结论，也就是说，“首诊”是将疾病状况和患者是否适合接受上门护理两项内容结合所做的诊断。

(六) “互联网+护理服务”的定价与支付

关于“互联网+护理服务”的定价，《试点方案》仅作了原则性规定，即要求发挥市场议价机制，参照当地医疗服务价格收费标准，综合考虑交通成本、信息技术成本、护士劳务技术价值和劳动报酬等因素。在费用支付的问题上，《试点方案》则未作明确规定。

目前，“互联网+护理服务”的市场定价整体较高。以较为知名的某护理服务APP为例，笔者从其官方网站上查询到其收费标准，包括打针159元每次、输液189元每次、普通换药159元每次、吸痰189元每次、导尿219元每次等等。以上海市卫健委公开的上海市医疗机构医疗服务项目价格作为对照，肌肉注射3元每次、输液12元每次、换药14-50元每次（视创口大小而定）、吸痰 6 元每次、导尿 20 元每次。可见，即使扣除护士的交通费用、互联网信息技术平台的运维费用等成本，该APP的定价相对公立医疗机构仍然是比较“高昂”的。

考虑到《试点方案》允许的“互联网+护理服务”模式下，护理服务提供方仍然是医疗机构，只是对提供护理服务的地点进行了延伸，这似乎不能作为上门护理服务价格远高于医疗机构内护理服务价格的合理支撑。所以，笔者认为“互联网+护理服务”的价格仍应以医疗机构内的服务价格为基础，同时加上交通费、平台运维费等相关成本，包括考虑因为护士上门服务产生的额外的劳务成本，综合确定上门护理服务的定价机制与标准，并且应当公开其定价机制与标准接受监督，这样的定价方式似乎更为妥当。

同时，上门护理服务仍然属于医疗机构所提供的医疗服务，其性质并不因服务地点的改变而发生变化，从理论上来说，如果相关医疗服务原本属于医保可覆盖项目的，即使转变为上门服务，也应当能够使用医保支付。

(七) 事故责任

在“互联网＋护理服务”的新模式下，医疗机构、互联网信息技术平台和护士三方均为服务提供方，参与了护理服务的不同环节，如发生护理服务导致患者人身损害的，需要确定各方应当承担何种责任。

（1）民事责任

如前文所述，“互联网＋护理服务”是由医疗机构派遣护士到患者家中提供护理服务，与传统的院内护理服务模式并无本质区别，只是对服务的场所进行了延伸，所以当护理服务导致患者人身损害时，仍然应当按照医疗事故的相关处理规定来解决。根据《医疗事故处理条例》，发生医疗事故时，医疗机构而非护士个人需要作为责任主体向患者承担民事责任。但同时，如果第三方互联网信息技术平台对于损害后果的产生也存在过错的，该平台也应当承担相应的民事责任，但相关的民事责任在医疗机构和平台之间具体如何划分、承担则有赖于依据双方的事先约定来确定。正因此，为了减少争议，《试点方案》要求医疗机构在与第三方互联网信息技术平台合作时，应当在合作协议中明确各自在护患安全、纠纷处理等方面的责任。

（2）行政责任

在“互联网+护理服务”过程中如发生医疗事故的，根据《医疗事故处理条例》第五十五条的规定，医疗机构将视情节被处以警告、责令限期停业整顿或吊销执业许可证的处罚；护士如对医疗事故负有责任的，也将被依法给予行政处分或纪律处分，还可能被责令暂停 6

个月以上 1 年以下执业活动，甚至被吊销执业证书。

（3）刑事责任

在“互联网+护理服务”过程中，如果护士发生严重不负责任的行为，并因此造成患者死亡或者严重损害患者身体健康的，依据《刑法》第三百三十五条，该护士可被处以三年以下有期徒刑或者拘役。

(八) 服务质量的监督与管控

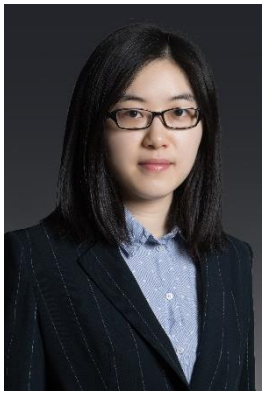
为了确保“互联网+护理服务”的质量，也为了保证服务过程中护士的人身安全，《试点方案》要求医疗机构或互联网信息技术平台应当采用相关的技术手段，如身份识别、手机 APP 定位追踪系统、护理工作记录仪等等，以实现对服务过程的监督和服务质量的管控。

三、 结论

上文就《试点方案》中的“互联网+护理服务”试点安排进行了分析和解读。现有的制度中仍然存在一些需要进一步明确的地方，但除了需要探索制度上的进步和完善以外，“互联网+护理服务”也面临着诸多现实性的困难。例如，在当前医患关系较为紧张的社会背景下，护士在患者家中提供护理服务的，其人身安全是否可能面临更大的威胁；目前已经存在护理人员整体数量不足的情形，护士们是否确有余力再提供上门护理服务；而且，护理服务始终具有一定的风险性，如在服务过程中发生突发状况的，如何确保患者的生命安全等等。这些现实性的困难决定了“互联网+护理服务”究竟能否在现实中取得长足的发展，帮助解决我国护理资源短缺的问题，而这些困难的解决也有赖于政府、医疗机构、互联网信息技术平台等各方的积极探索与合作。

董秋艳为环球律师事务所上海办公室的律师，其职业领域为医药和健康、并购和股权投资。

邮箱： sylviadong@glo.com.cn



李艺辉为环球律师事务所上海办公室的律师助理，其执业领域为医疗健康和公司法。

邮箱：amyli@glo.com.cn

环球生命科学及医疗领域近期代表性项目

环球为天境生物 2.2 亿美元 C 轮融资提供法律服务

2018 年 6 月 29 日，聚焦于肿瘤免疫和自身免疫疾病治疗领域的创新药物研发企业——天境生物（I-Mab）宣布完成 2.2 亿美金 C 轮融资，本次融资是目前为止中国创新药领域最大的融资之一，备受业界瞩目。本次融资由弘毅投资领投，高瓴资本、厚朴投资、鼎晖投资、汇桥资本以及以新加坡为基地的 EDBI 等参与，现有投资方康桥资本及天士力资本继续跟投。

作为一家立足于中国、面向全球研发创新抗体药物的研发公司，天境生物凭借在靶点生物学、抗体分子工程研发及转化医学研究上的优势，正快速推进具有国际竞争力的项目管线。

本轮融资将主要用于推进数个 Best-in-Class 及 First-in-Class 创新生物药的临床前及临床阶段的研究及开发。此次成功融资是天境生物继 2017 年 3 月获得 1.5 亿美元 B 轮融资后，再一次获得顶尖专业投资者青睐，彰显了其在全球创新性抗体药物研发领域的综合实力及发展前景。

环球团队代表投资方为本项目提供了全程法律服务，环球的项目团队由合伙人律师于淼、周磊、李占科和孙胤翔牵头，团队成员还包括罗岚、王冠洁、马瑞娜、贺静文、张艳冰和张静。

环球协助完成西门子医疗上市的中国业务重组工作

德国当地时间 3 月 16 日，医疗创新解决方案全球领先的提供者，西门子旗下医疗业务板块 Siemens Healthineers AG （下称“西门子医疗”），在法兰克福证券交易所首次成功上市。上市首日第一笔交易所报价为每股 29.10 欧元，远高于最终配售价格 28.00 欧元。共有 1.5 亿现存的已注册普通股（包括超额认购）在首次公开募股中发售，占流通股的 15%。西门子医疗是全球医疗领域最大的供应商之一,在影像诊断、临床治疗、实验室诊断、医疗 IT 等领域屹立在技术创新的前沿,可向客户提供全方位诊疗产品和解决方案。据报告，该 IPO 不仅是德国过去 20 年间最大的上市，也是今年欧洲市场最大的 IPO。

环球律师事务所生命科学及生命科学及医疗团队作为西门子的中国法律顾问，全程参与了西门子医疗上市项目下中国生命科学及医疗业务的重组，包括重组行动计划、重组文件、政府审批、完成交割以及中国法律问题建议等。环球的项目团队由合伙人周磊、王忠诚和范可牵头，团队成员还包括王冠洁、何墨秋和张蕊等。

环球协助完成中国首例上市许可制度下的生物制药商业化生产交易

1 月 9 日，百济神州与勃林格殷格翰生物药业（中国）有限公司宣布双方就百济神州的在研 PD-1 抗体 tislelizumab 签署了一项商业供应协议。作为百济神州和勃林格殷格翰探索实践“药品上市许可持有人制度”的一部分，tislelizumab 将在位于上海的世界一流的勃林格殷格翰生物制药生产基地进行生产。

基于供应协议条款，勃林格殷格翰将在数年内拥有 tislelizumab 的独家生产权（期限有可能延长）。除此之外，百济神州也获得了未来勃林格殷格翰在中国为其扩大产能的数项优先权。

此次签约，标志着百济神州与勃林格殷格翰建立了长期、稳固的战略合作伙伴关系，双方将一如既往地凭借自身在行业内的专业影响力推动中国健康领域的持续发展，为中国的健康事业，献出一份积极的力量。

环球律师事务所生命科学及医疗团队作为勃林格殷格翰的法律顾问，为商业化生产交易提供法律咨询意见，并协助起草了法律文件。该项目由合伙人周磊律师与合伙人范可律师牵头，团队成员还包括彭锦律师。

环球代表勃林格殷格翰公司与上海国际医学中心(SIMC) 达成康复中心战略合作

2017 年 11 月 23 日，勃林格殷格翰公司与上海国际医学中心(SIMC)举行战略合作签约仪式，宣布勃林格殷格翰旗下霁达康复团队与 SIMC 将携手共建一流的康复中心，以卒中康复为优势项目，同时提供其它神经、心脏病和骨科等领域的康复治疗方案。

目前中国的康复领域正处于发展期，现有康复行业的机构规模、专业人员及设施设备与发达国家相比仍有较大差距。作为卒中疾病领域的领跑者，勃林格殷格翰在脑卒中的预防及治疗方面拥有国际先进的专业知识和经验；而 SIMC 是一家根据国际联合委员会（JCI）标准建造的，拥有国际化医疗视野并提供现代化服务的综合性平台医院。通过战略合作，勃林格殷格翰与 SIMC 强强联手。勃林格殷格翰作为能提供卒中预防、急性期治疗和康复全程解决方案的公司，引进国际一流的康复技术与理念，携手 SIMC 打造国际化、专业化、特色的康复中心。

环球律师事务所生命科学及医疗团队作为勃林格殷格翰的法律顾问，为其完成交易提供了全面的法律服务。环球的项目团队由生命科学及医疗团队合伙人周磊和于淼律师牵头，团队成员还包括顾问律师黄旭春和律师助理何墨秋。

环球新闻——环球代表百济神州完成中国生物医药领域重大交易

环球协助百济神州（BeiGene，纳斯达克代码：BGNE）于 2017 年 8 月 31 日完成与新基公司（Celgene，纳斯达克代码：CELG）的肿瘤领域全球战略性合作相关交易，涉及金额近 14 亿美元。据相关媒体报道，该交易是迄今为止中国生物医药企业国际合作最大的交易。

这项合作最早于 2017 年 7 月 5 日宣布，根据双方约定，百济神州接手了新基在中国的商业团队，并且承担起新基在华获批产品 ABRAXANE®注射用紫杉醇（白蛋白结合型）、瑞复美®（来那度胺）和 VIDAZA®（注射用阿扎胞苷），以及在研产品 CC-122 的商业化责任。新基取得了在美国、欧洲、日本和亚洲以外的多个国家和地区针对 BGB-A317 实体瘤适应症开发和商业化的独家授权。百济神州保留针对 BGB-A317 在除日本以外亚洲地区的实体瘤权利，以及在血液瘤和内部药物组合领域的全球权利。百济神州将从新基获得总和 4.13 亿美元的授权许可预付款和股权投资，并有资格获得额外的 9.8 亿美元基于开发、药政和销售的里程碑付款，以及 BGB-A317 的未来销售许可费。环球律师事务所作为百济神州本次交易的中国法律顾问，全程参与了该战略性合作项目涉及中国业务交易的尽职调查、商业谈判、交易文件签署和交割，为相关合作提供全面法律支持。环球的项目团队由生命科学及医疗业务团队合伙人周磊、孙胤翔牵头，团队成员还包括王冠洁、董秋艳和沈鸿翔等。

环球助力美年大健康收购慈铭体检通过商务部反垄断审查

2017 年 5 月 9 日，美年大健康产业控股股份有限公司发布公告称：其子公司美年大健康产业（集团）有限公司（简称"美年大健康"）已收到商务部关于美年大健康及其关联企业收购慈铭体检公司股权涉嫌未依法申报经营者集中的最终处理决定，商务部认定该项经营者集中不具有排除、限制竞争的效果；公司已于日前向中国证监会申请恢复对公司发行股份购买慈铭体检 72.22%股权并募集配套资金暨关联交易的审查，待中国证监会核准后将尽快推进本次重大资产重组事项。

环球律师事务所就本案为美年大健康提供了全程法律服务，涵盖是否属于未依法申报经营者集中的初步调查阶段、评估竞争影响的进一步调查阶段以及行政处罚阶段。环球的项目团队由北京办公室合伙人任清律师牵头，团队成员还包括上海办公室合伙人周磊律师、北京办公室律师助理潘静怡等。

环球为弘和仁爱医疗集团（3869.HK）在香港联交所主板挂牌上市提供法律服务

2017 年 3 月 16 日，弘和仁爱医疗集团有限公司（下称“弘和仁爱”，股份代号：3869.HK）在香港联合交易所主板正式挂牌上市。

弘和仁爱目前以医院运营管理为主营业务，未来将会建立一个全国性医疗服务中心。弘和仁爱已经在上海布局两家医院：上海杨思医院及福华医院，其中上海杨思医院成立于 2007 年，是上海最大

的民营非营利性医院。弘和仁爱对旗下医院实施标准化及流程化的管理体系，并综合考虑各个医院的背景和具体情况，通过多种关键措施（包括激励及决策机制、战略规划及实施、财务管控及雇员培训）提升旗下医院的整体管理、接待能力及运营效率。上市后，弘和仁爱的目标锁定二级或三级医院或拥有二级或三级医院同等规模，并座落于人口规模较大及经济条件较发达的地区医院，以上海为战略起点布局区域医疗服务中心，通过战略性并购建立全国性的医疗服务网络。弘和仁爱作为弘毅投资的医院运营及管理业务的核心平台，致力于打造中国第一流的医疗管理集团。

环球律师事务所作为弘和仁爱的中国律师，协助完成本次上市项目。环球的项目团队由北京办公室合伙人于淼律师牵头，团队成员包括罗岚、张心怡和肖雄。

环球为永胜医疗（1612.HK）在香港联交所主板挂牌上市提供法律服务

永胜医疗控股有限公司（下称“永胜医疗”，股份代号：1612.HK）于 2016 年 7 月 13 日在香港联交所有限公司主板正式挂牌买卖。

永胜医疗控股有限公司创立于 1997 年，总部位于香港的医疗器械集团。集团开发、生产及销售多种医疗器械，尤其专注向中国及海外市场的客户提供符合国际认可质量保证标准的呼吸产品、一次性造影 CMPI 用品及骨科支护具康复器具。集团自成立以来已建立 OEM 业务，在 2003 年以自有品牌“英仕医疗”开展 OBM 业务。根据灼识企业管理咨询报告，按出口价值计，永胜医疗是 2015 年中国第二大呼吸与麻醉一次性产品出口商。

本项目由上银国际有限公司担任独家保荐人和独家全球协调人。环球律师事务所作为独家保荐人的中国律师，协助永胜医疗完成该项目。环球的项目团队由李琤律师和孙海珊律师两位合伙人牵头，团队成员还包括文丹微和易格格等。

环球协助华盖医疗投资诺康达医药

2017 年农历新年伊始，华盖医疗完成对诺康达医药的 B 轮投资。此次诺康达医药的融资规模达到 1.6 亿元人民币，华盖资本为领投方，参与投资的其他机构还包括险峰旗云基金等。

诺康达医药是一家专业从事医药研发服务外包（CRO）、一致性评价、创新制剂和器械耗材等相关领域研发的高科技公司，研发外包服务团队及业务在本土研发企业中位居前茅。诺康达拥有国内医药行业前 20 强的固定合作客户，并已与国内外多家知名医药上市公司达成了战略合作。
华盖医疗为华盖资本旗下专注生命科学及医疗产业的股权投资平台，此次投资诺康达医药的华盖生命科学及医疗产业二期基金总规模约 20 亿元人民币，拥有超过 20 家上市公司（包括 A 股与港股主板上市公司大股东或其投资平台）为 LP，其中绝大多数为生命科学及医疗行业的知名上市企业

集团。

环球律师事务所为华盖资本投资诺康达医药提供全程法律咨询服务，包括进行尽职调查，起草尽职调查报告、投资协议、交割文件等，与公司、前轮投资人谈判，协助交割等。环球的项目团队由合伙人赵博嘉律师牵头。

环球协助金浦健服收购创泰集团控股权

重庆创泰医院投资管理有限公司于 2013 年 2 月注册成立，是一家专门从事医院项目投资，接受医院委托从事医院管理的专业化营运机构，其作为一家医疗管理公司全资持有或控股重庆创泰黄杨新城医院有限公司、重庆二郎医院有限公司、重庆达尔康医院有限责任公司、重庆创泰其济医院有限责任公司、重庆创太达尔康医院有限责任公司。创泰集团发展目标明确、市场定位及规划清晰，致力于重庆市基层医疗服务的发展，主要投资、拓展一级医疗机构。创泰集团探索发展具有特色的连锁品牌，在药品、耗材采购、人事制度、财务制度等方面均由医院管理公司进行统一指导管理，深入社区，为社区人群特别是中老年人提供慢病管理服务，赢得当地好评。创泰集团拟未来通过并购或者新设的方式逐步增加基层医疗机构的数量，扩大其在重庆市的影响力。

金浦健服是一家致力于生命科学及医疗服务产业投资、并购与整合的专业管理公司，管理团队由来自国内外的在医疗、金融、投资、法律等领域具有丰富经验的专业人士组成，强调行业研究与价值导向，致力于成为国内生命科学及医疗服务产业最专注最有影响力的专业投资机构。

环球律师事务所为金浦健服收购创泰集团提供法律服务，协助金浦健服通过受让部分旧股及增资的形式完成对创泰集团的收购。环球的项目团队由合伙人赵博嘉律师牵头。

环球协助阳光医疗收购四会万隆医院

2017 年初，阳光医疗完成对广东四会万隆医院股权的收购。

广东四会万隆医院，成立于 2002 年，经过近 15 年的发展，已建设成为集医疗、预防、保健、科研、康复于一体的现代化综合医院。万隆医院自开办以来，依靠自身的品牌、专家与技术，建立了规范的医疗管理制度、赢得了良好的社会口碑，其微创外科、急诊科、妇产科在当地形成一定影响力，并于 2010 年被评定为二级甲等综合医院，且是当地唯一一家非营利民营综合二级甲等医院。万隆医院在当地另设有眼科门诊部，最大程度满足周边居民基本医疗需求。医院目前除承担周边居民基本医疗需求外，同时负责当地绝大部分企事业单位职工体检及诊疗服务，是当地居民首选就医地点。此外，万隆医院已经做到医保全覆盖，其中包括肇庆市城镇居民、新农合及职工医保。

阳光医疗是阳光控股旗下专门从事医疗健康和养生养老投资与运营管理的产业集团。阳光控股是以地产、医疗、教育、金融等行业投资为主营业务的大新投资控股集团。目前，阳光医疗的业务已涉足医疗服务、健康管理、医药器械、科研教学、养生养老、互联网医疗等多个领域，已与国内外众多著名医疗机构、医学院校建立了业务联系，如今正在大力拓展医疗健康与养生养老产业。

此次交易是阳光医疗拓展医疗养老产业的重要部署。环球律师事务所为此次交易提供全程法律咨询服务，协助阳光医疗完成对万隆医院的重组并收购万隆医院的控股权，助力阳光医疗踏出医疗健康与养生养老领域的坚实一步。

环球的项目团队由合伙人赵博嘉律师牵头，团队成员还包括史晓雯、李悄然、刘珊珊等。

环球为平安好医生 A 轮五亿美元融资提供法律服务

近日，平安集团旗下“平安好医生”向媒体宣布，已获 5 亿美元 A 轮投资，参与本轮投资的机构包括海外知名股权投资基金、世界五百强大型央企、国有金融企业以及互联网公司，目前融资金额已全部到位。本轮融资完成后，公司估值达到 30 亿美元。

平安好医生是一个互联网健康管理平台，以家庭医生与专科医生的在线诊疗服务作为切入口，配合大数据的挖掘、分析及应用，用线上、线下相结合的方式，为客户提供形式多样、内容丰富的个性化医疗及健康管理服务。作为平安集团医疗战略的核心产品，“平安好医生”这款于 2015 年 4 月上线的移动医疗 APP 围绕医网、药网及信息网形成三大产品线，涉及在线问诊、医患管理、药品 O2O、电子健康档案、慢病管理、儿童健康服务等医疗健康的多个细分领域。

在此次融资中，环球作为领投方的中国法律顾问，为其提供了包括尽职调查、法律意见等诸多事项的法律服务。环球的项目团队由合伙人刘成伟律师牵头，团队成员还包括陈泊林、叶欣、林婷婷等。

环球为中民国际对安徽省某医院集团的大金额投资提供法律服务

近日，中民国际控股有限公司（以下简称“中民国际”）完成了其对安徽省某医院集团的重组与投资。该医院集团的前身为安徽省某市的公立医院，后由现实际控制人对医院进行了改制、收购，并将医院设立为非营利性的民办非企业单位。而在此次重组和投资项目交割时，该医院集团已获批准变更为营利性医疗机构。

环球律师事务所作为中民国际的法律顾问，为其本次投资提供了全面的法律服务，包括法律方面的尽职调查、交易架构的设计、交易文件的起草和谈判等。环球的项目团队由合伙人赵博嘉律师牵头。

环球为化学品综合电商摩贝（MOLBASE）完成数千万美元 C 轮融资提供法律服务

2016 年 3 月 17 日，化学品电商综合服务平台摩贝（MOLBASE）宣布获得 C 轮融资，领投方为红杉资本中国基金、挚信资本，原投资方创新工场、复星昆仲、盘古创富跟投。融资金额达数千万美元。摩贝网是化学品领域首家披露获得 C 轮融资的创业企业，同时摩贝网也是获得融资次数最多的 B2B 化学品平台。

摩贝致力于打造全球最大的化合物数据和信息平台，优化产业链和激活化合物交易的定制市场、研发市场、外贸市场、库存市场，服务于生物医药和新材料产业，提供推广、交易撮合、融资、出口、物流等一站式综合服务。摩贝网 CEO 常东亮博士表示，此次融资后公司将加强布局和深化全国市场服务体系，整合交易、客户、金融、供应链等不同层面的数据，更精准地服务于化工相关企业的转型升级。

摩贝在 2012 年 1 月完成数百万元天使轮融资，投资机构为德沃基金。2014 年 1 月，完成数百万美元 A 轮融资，投资机构为挚信资本、创新工场；同年 11 月，完成数千万美元 B 轮融资，盘古创富领投。2015 年 6 月完成 B＋轮融资，复星昆仲领投。本次获得红杉资本、挚信资本等机构数千万美元 C 轮融资。

环球律师事务所是公司历次融资交易的法律顾问，为摩贝提供了全面的中国法律服务。就此次公司 C 轮融资交易，环球的项目团队由顾问律师孙胤翔牵头，团队成员还包括顾龙律师以及何璇律师。

环球为科济生物 B 轮融资提供法律服务

近日，科济生物医药（上海）有限公司（CARsgen Therapeutics）（“科济生物”）完成其 B 轮股权融资交割。科济生物为 CAR-T 细胞技术（CAR-T based autologous immunotherapy）尤其是实体瘤（solid tumor）CAR-T 细胞治疗的全球领先研发企业。创始人李宗海博士为上海交通大学医学院附属仁济医院博士生导师、上海市肿瘤研究所癌基因及相关基因国家重点实验室研究组长。科济生物已经于 2015 年在上海交大附属仁济医院开展了全球首个肝细胞癌的 CAR-T 细胞临床实验。

在此次融资中，领投方包括 KTB 和 A 股上市公司佐力药业的全资孙公司佐力创新医疗，跟投方为凯泰成长及上海嘉稹。本次融资将主要用于科济生物的 CAR-T 细胞临床实验及相关研发团队的增强。

环球在本项目中作为科济生物的法律顾问，为其本次融资提供了全程法律服务。环球的项目团队由合伙人刘展律师牵头，团队成员还包括顾问王嘉瑛律师、邓昭律师等。

环球为美力三生 A 轮 5,000 万人民币融资提供法律服务

美力三生成立于 2013 年 1 月，旗下有“生命滙”和“美力汇”两个业务平台，专注于为高端人群提供从产品到服务的一体化健康管理方案。美力三生的 CEO 陈力女士，曾担任宝洁公司亚太首席美尚科学家，集团核心成员有来自世界 500 强企业的高管和销售，也有欧美医学专业人士。环球律师事务所赵博嘉律师团队作为美力三生的常年法律顾问以及该次融资的公司法律顾问，协助美力三生完成 A 轮 5,000 万人民币融资。公司本轮融资的投资方为红杉资本和 A 股上市公司东方园林（002310）。

环球为北极光创投对卡尤迪生物的大额 B 轮投资提供法律服务

卡尤迪生物由李响女士创立于 2009 年，其独有的“一滴血快速核酸现场检测技术平台”，用分子诊断的方式，在一小时甚至十分钟的时间内，通过一滴指尖血，进行多种传染性疾病的检测以及数类癌症的早筛。公司此次 B 轮融资由北极光创投领投，赛富亚洲以及联想之星参与跟投。环球律师事务所赵博嘉律师团队协助北极光创投完成对卡尤迪生物的本轮投资。

环球为旦恩创投对五彩鹿的 Pre-A 轮投资提供法律服务

五彩鹿设立于 2004 年，是一家旨在为广泛性发育障碍（包括自闭症和其他发育障碍）以及有各种行为问题的儿童及其照护者提供教育与培训的机构。经过多年的积累发展，五彩鹿形成了具有自己特色的管理模式、培训模式、教学模式，成功训练了上千名自闭症和其他发展障碍儿童，逐渐成为国内最专业、最先进的儿童康复训练机构之一。环球律师事务所赵博嘉律师团队作为旦恩创投的法律顾问，协助旦恩创投设计、论证五彩鹿的重组方案，并协助旦恩创投完成对五彩鹿的 Pre-A 轮投资。

环球为方源资本等投资“杏仁医生”移动医疗平台约 2 亿人民币项目提供法律服务

移动医疗 APP 杏仁医生近日宣布获得新一轮 2 亿人民币的融资，此轮融资由方源资本领投，公司的早期投资人红杉中国和光速安振中国创投跟投。

方源资本是专注于中国市场规模最大的私募股权基金之一，旗下管理的资产接近 30 亿美元，来自全球顶级的机构投资者。杏仁医生是中国最大的医生专用平台。2014 年 9 月，杏仁医生 APP 正式对外发布，在 APP 设计上将其定位为专业高效的医患沟通管理工具。作为首款与微信集成的医生专用 APP，医生可以通过杏仁医生与其就诊的患者建立更深入紧密的联系，并提供特色的随诊、跟踪、交流、检索功能。

环球律师事务所的生命科学及医疗团队为方源资本等本轮投资人在交易中提供了全面的中国法律服务。本次交易的项目团队由环球常驻上海的合伙人周磊律师牵头，团队成员还包括资深顾问孙胤翔律师，以及顾龙和何璇律师。

环球简介

环球律师事务所（“我们”）是一家在中国处于领先地位的综合性律师事务所，为中国及外国客户 就各类跨境及境内交易以及争议解决提供高质量的法律服务。

历史. 作为中国改革开放后成立的第一家律师事务所，我们成立于 1984 年，前身为 1979 年设立的中国国际贸易促进委员会法律顾问处。

荣誉. 作为公认领先的中国律师事务所之一，我们连续多年获得由国际著名的法律评级机构 评选的奖项，如《亚太法律 500 强》（The Legal 500 Asia Pacific）、《钱伯斯杂志》（Chambers & Partners）、《亚洲法律杂志》（Asian Legal Business）等评选的奖项。

规模. 我们在北京、上海、深圳三地办公室总计拥有近 300 名的法律专业人才。我们的律师 均毕业于中国一流的法学院，其中绝大多数律师拥有法学硕士以上的学历，多数律师还曾学习或工作 于北美、欧洲、澳洲和亚洲等地一流的法学院和国际性律师事务所，多数合伙人还拥有美国、英国、德 国、瑞士和澳大利亚等地的律师执业资格。

专业. 我们能够将精湛的法律知识和丰富的执业经验结合起来，采用务实和建设性的方法解决法律问题。我们还拥有领先的专业创新能力，善于创造性地设计交易结构和细节。在过去的三十多年里，我们凭借对法律的深刻理解和运用，创造性地完成了许多堪称“中国第一例”的项目和案件。

服务. 我们秉承服务质量至上和客户满意至上的理念，致力于为客户提供个性化、细致入微 和全方位的专业服务。在专业质量、合伙人参与程度、客户满意度方面，我们在中国同行中名列前茅。在《钱伯斯杂志》2012 年举办的“客户服务”这个类别的评比中，我们名列中国律师事务所首位。

环球生命科学及医疗业务简介

作为该领域最佳律师事务所之一，环球生命科学及医疗业务组目前有十五名合伙人、三名顾问律师和超过 三十名律师和助理组成，我们对中国的生命科学及医疗领域及相关法律法规有着深刻的认识和专业的理解。

我们的经验已经覆盖了生命科学及医疗产业的所有领域，包括药品研发、临床实验研究、药品生产、生命科学、动物药品、生物制药、医疗器械、供应商及分销商、医院和其他医疗服务商，以及各类医药 健康领域的投资基金，为各类客户提供一站式的专业法律服务。我们还与行业相关的协会组织有紧密联系，并且作为有关委员会成员参与了相关行业行为准则的制定。

在新发布的《钱伯斯杂志》律所排名中，环球的生命科学及医疗团队连续七年（2012-2019）排名业内最佳律师事务所（Band 1），同时环球也曾五度获得 China Law & Practice 年度生命科学律师事务所大奖。环球生命科学及医疗法律团队被评价为“能力出众，团队精良，专业高效，服务领域广泛”并且“灵活并以客户为中心”。

版权与免责

免责. 本报告不代表环球律师事务所对有关问题的法律意见，任何仅依照本报告的全部或部分内容而做出的作为和不作为决定及因此造成的后果由行为人自行负责。如您需要法律意见或其他专家意见，应该向具有相关资格的专业人士寻求专业帮助。

联系我们. 如您欲进一步了解本报告所涉及的内容，您可以通过下列联系方式联系我们。

环球律师事务所（北京总部）

北京市朝阳区建国路81 号华贸中心1 号写字楼15 层&20 层 邮编：100025

电话：(86 10) 6584 6688

传真：(86 10) 6584 6666

电邮：global@glo.com.cn

环球律师事务所（上海）

上海市黄浦区湖滨路150 号企业天地5 号楼26 层 邮编：200021

电话：(86 21) 2310 8288

传真：(86 21) 2310 8299

电邮：shanghai@glo.com.cn

环球律师事务所（深圳）

深圳市南山区铜鼓路 39 号大冲国际中心 5 号楼 26 层 B/C 单元 邮编：518055

电话：(86 755) 8388 5988

传真：(86 755) 8388 5987

电邮：shenzhen@glo.com.cn

环球律师事务所

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987