立方律師
NEWSLETTER
LIFANG & PARTNERS 立方观评
No.266
2021.09

Contents

Latest Developments on Data Supplementation for Chemical or Pharmaceutical Patents in China

WANG Ying & LI Chunxuan, Lifang & Partners

CNIPA (China National Intellectual Property Administration) and the Chinese courts have been challenged for years for their strict practices on accepting post-filing data during prosecution, invalidation, and administrative litigation proceedings. Such practices render patent applications with broad scopes less likely to succeed or much more likely to be revoked during invalidation procedures. However, the Supreme People's Court's latest judicial interpretation and precedents set by the courts and CNIPA create new practices that give chemical and pharmaceutical patent holders better prospects of acquiring stable patent rights. Moreover, new practices on accepting post-filing data will add more value to chemical and pharmaceutical patents and further boost innovation in the chemical and pharmaceutical industries.

Latest Policy and Law Updates on Data Supplementation

A. China-US Economic and Trade Agreement

Data supplementation was one of the key issues in the China-US Economic and Trade Agreement ("*Agreement*") executed on January 15, 2020, because CNIPA had narrower criteria for accepting post-filing data for chemical and pharmaceutical patents than the US and the European Patent Office.

Article. 1.10 of the Agreement, which relates to Data Supplementation, states that "*China shall permit pharmaceutical patent applicants to rely on supplemental data to satisfy relevant requirements for patentability, including the sufficiency of disclosure and inventive step, during patent examination proceedings, patent review proceedings, and judicial proceedings*". Accordingly, Chinese legislators took steps in 2020 to implement the *Agreement*.

B. Provisions of the Supreme People's Court on Several Issues concerning the Adjudication of Administrative Cases on Granting and Affirming Patent Rights

To echo Article 1.10 of the *Agreement*, the Supreme People's Court promulgated *Provisions of the Supreme Court on Several Issues concerning the Adjudication of Administrative Cases on Granting and Affirming Patent Rights* ("*Provisions*"), which took effect on September 12, 2020. Article 10 of the Provisions specifically relates to data supplementation. Article 10 of the Provisions states that:

Where a drug patent applicant submits supplementary experimental data after the date of application and claims that the patent application should be proved as conforming to Article 22.3, Article 26.3 and other provisions of the Patent Law by relying on such data, the People's Court shall examine such data.

However, Article 10 of the Provisions only specifies that the court shall examine supplementary experimental data. However, the standards for

accepting supplementary data remain unclear.

C. Chinese Patent Examination Guideline

Later, on January 15, 2021, the amended Chinese Patent Examination Guidelines ("Guidelines") introduced seemingly clearer standards for accepting supplementary data for chemical and pharmaceutical patents.

The Guidelines specify that: (1) the examiner shall examine experimental data submitted by an applicant after the application date regarding Articles 22.3 (inventive step) and 26.3 (insufficient disclosure) of the Patent Law; and (2) the technical effect proved by supplementary experimental data must be obtainable by one skilled in the art based on disclosures in the patent application.

The Guidelines also give two examples to demonstrate the standards for post-filing data acceptance. One example concerns a patent application claiming to protect compound A with a specification that discloses the experimental method of measuring the activity of lowering blood pressure without disclosing experimental results. In such situations, post-filing data submitted by an applicant on the blood pressure lowering effects of compound A to overcome objections of insufficient disclosure are acceptable since such data is obtainable from the method disclosed in the specification. In the other example, the anti-tumor effects of Compound A and other compounds under the general formula are exemplified with solid data in the specification. The data supplemented by the applicant to show the inventive step of the patent by comparing the anti-tumor effect of Compound A with that in the prior art is acceptable.

However, there remains uncertainty on whether a court or CNIPA would allow an applicant or patentee to submit post-filing data to prove an asserted technical effect, which is merely mentioned but lacking data to confirm the effect in the specification. In many previous cases, supplemental data submitted after the filing date to prove such unconfirmed technical effects in the patent document was rejected. Such cases include AstraZeneca v. PRB, (2018) Jing Xing Zhong No. 6345 and Boehringer Ingelheim v. PRB, (2017) Jing Xing Zhong 2470 decided by Beijing High People's Court, and other cases.

The most recent cases decided by the Supreme People's Court and CNIPA present clearer standards on the acceptance of supplemental data filed by the patentee to prove such unconfirmed technical effects in patent documents.

Data Supplementation to Overcome Lack of Inventive Step Objections

AstraZeneca's ZL200610002509.5 patent, which concerned a crystalline form of a triazolo (4,5-d) pyrimidine compound known as "Ticagrelor", was invalidated for lacking an inventive step. During invalidation proceedings, the patentee submitted data showing metabolic stability and bioavailability prepared by the patentee's employee to show the surprising effects of the Ticagrelor. However, that data was not considered by the Patent Reexamination Board (PRB), which took the position that: (i) surprisingly high metabolic stability and bioavailability effects were merely asserted in the background of the patent without any data in the original patent document to prove these effects; and (ii) supple-

mental data was submitted after the priority date, and the results made by the patentee's employees were inevitably subjective. Therefore, the patent was invalidated for lacking an inventive step by the PRB, without considering the supplemental data. The Beijing Intellectual Property Court confirmed the PRB's decision.

Although the Beijing Intellectual Property Court's decision was upheld in the second instance in Supreme People's Court case (2019) Zhi Xing Zhong No. 33 in October 2020, the Supreme People's Court took a different view towards the acceptance of post-filing data. By referring to Article 10 of the *Provisions* as its legal basis, the Supreme People's Court clarified the standards for post-filing data acceptance as: (i) if the facts to be proved by the post-filing data are clearly recorded or implicitly made public in the specification, the applicant can be considered to have completed relevant research, and so, acceptance of the data would not violate the first to file principle; and (ii) supplementary data shows that the facts to be proved in the specification are true.

By adopting the above standards, the Supreme People's Court could consider the supplemental data submitted by the patentee because the metabolic stability and bioavailability effects had been recorded in the patent and later proved by the supplemental data. Although the Supreme People's Court upheld the decision of the first instance court because the supplemental data was not convincing enough to manifest surprising effects compared with those in the prior art, this was the first case to apply Article 10 of the *Provisions* and set a clear standard for post-filing data acceptance to be followed in similar future cases.

In a later invalidation case, Jingxin Pharmaceutical v. Richter Gedeon NYRT (Invalidation Decision No. 47087), decided by CNIPA in November 2020, the validity of the subject patent was upheld based on post-filing data submitted by the patentee. CNIPA's attitude of accepting post-filing data to prove the asserted technical effect followed the standards that applied in the above Ticagrelor case.

Data Supplementation to Overcome Insufficient Disclosure Objections

According to the *Guidelines*, a chemical product invention must be sufficiently disclosed by identifying the chemical product, at least one method of preparing the product, and proof supporting its anticipated uses or technical effects. Very few post-filing data submissions were accepted in the past due to insufficient disclosure of the preparation method or technical effects.

In administrative litigation (2014) Xing Ti Zi Ti No. 8, which concerned Pfizer's product Lipitor and was heard by the Supreme People's Court in 2015, the patentee submitted experimental reports during litigation to demonstrate that the Type I crystals for atorvastatin calcium trihydrate could be produced by one skilled in the art. The court intended to set a tone or establish a practical rule for accepting post-filing data under insufficient disclosure. That is, regarding the post-filing data for manifesting insufficient disclosure, if it can be proved that the invention can

be realized through the content disclosed in the specification with the knowledge and cognitive ability of one skilled in the art before the filing date, the supplemental data should be considered and should not be rejected simply because the data was submitted after the filing date. Moreover, when considering the acceptance of experimental evidence: (i) the experimental conditions and methods used in collecting the experimental evidence must be directly obtainable or easily thought of by one skilled in the art who reads the instructions before the filing date or the priority date; and (ii) matters must be considered based on the knowledge and cognitive ability of one skilled in the art.

In recent years, CNIPA examiners have become more prone to raising lack of inventive step objections instead of insufficient disclosure objections during the prosecution of inventions without substantial data to manifest their technical effects. In (2018) Jing 73 Xing Chu No. 2626, a case heard by the Beijing IP court in November 2020, the applicant submitted its prior application, filed before the filing date but published after the filing date of the patent application-in-suit, as evidence that the same chemical as that found in the patent application-in-suit had an SGLT2 inhibition effect. Therefore, the crystal form of the chemical, as claimed in the patent application-in-suit, obviously had such an effect. Such evidence was rejected by CNIPA but accepted by the Beijing IP Court because: (1) the evidence showed that the technical effect described in the patent application-in-suit is a technical contribution made before the filing date; and (2) the public could identify such an effect at the time when the patent application-in-suit was published. Therefore, accepting such experimental data would neither give the applicant protection beyond his technical contribution nor affect the public interest.

In summary, the standards set in the above cases are quite similar in that the technical effect or technical solution manifested by the supplemental data was obtainable from the original patent application by the patentee before the filing date, without contravening the first to file principle, and the acceptance of such data did not affect public interests.

Conclusion

It is good to see that CNIPA and courts no longer adhere to very stringent standards for accepting supplemental data. For technical effects merely asserted in the specification without any specific embodiment, supplementary data can be used to manifest the inventive step over the prior art using current standards. It should, however, be noted that the effects need to be recorded in the patent document so that data supplementation can prove such effects.

Although data can be supplemented to overcome insufficient disclosure objections when certain rules are met, we strongly recommend that applicants, insofar as is possible, fully disclose experimental data related to an invention, such as the technical effect and preparation process, in the original patent document.

The *Provisions* and cases decided by the courts have clarified standards for accepting post-filing data to a large degree. Acceptance of post-filing data during prosecution or invalidation proceed-

ings for chemical or pharmaceutical patents can also improve patent application grant rates and patent stability, which will reduce the risk of patents being invalidated. Clarifying the standards for accepting supplementary experimental data is a measure taken to support a long-awaited and expected boom in the pharmaceutical industry. Moreover, it will encourage innovation and significantly improve the transaction value of chemical and pharmaceutical patents.

WANG Ying
Partner of Lifang & partners
Practice Areas:
Intellectual Property
yingwang@lifanglaw.com

LI Chunxuan
Partner of Lifang & partners
Practice Areas:
Intellectual Property
chunxuanli@lifanglaw.com

Review of the Rules on PI Cross-border Transmission by Multi-national Corporations under the PIPL

QIN Ying & XIAO Pulingling, Lifang & Partners

On August 20, 2021, the Personal Information Protection Law of the People's Republic of China ("PIPL") was formally passed by the Standing Committee of the National People's Congress. As a fundamental law in the field of personal information ("PI") protection, it is of great legal significance both for individuals' information protection and for the compliance activities of corporate.

The significance of PI protection lies in its "identifiable" criteria and the nature of private subjects for the PI subjects. Improper processing of PI may bring great risks to personal property and personal safety, and even affect the credit system and economic security of companies and society.

Meanwhile, the globalization of commodities and economy drives the development of multinational corporations and the cross-border flow of PI. As a result, questions such as how to achieve overseas protection of PI, coordinate the conflict of different jurisdictions, and manage the extent and boundaries of PI cross-border transmission have become increasingly important.

This article would discuss the regulatory measures and corresponding responsibilities of multinational corporations in the context of PI cross-border transmission under the PIPL and other relevant laws and regulations governing data or PI protection, to provide some practical reference and support for multinational corporations.

I. The PI Cross-border Transmission Within Multinational Corporations is Clearly Subject to PIPL

Article 4 of the PIPL.

PI refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded excluding information that has been anonymized.

Processing of PI includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.

According to Article 4 of the PIPL, the act of transmission is a form of information processing, and is subject to the PIPL. However, the PIPL does not clarify whether the internal circulation of PI of multinational corporations falls within the scope of the targeted "transmission" activity. The Rules on the Cross-border Provision of PI under Chapter 3 of the PIPL focuses on the obligations of domestic data processors who act as PI providers in PI cross-border transmission. Note 2 (c) of Article 3.7 of the Information Security Technology - Guidelines for Data Cross-border transmission Security Assessment (the "Guidelines for Data Cross-border Transmission") provides that where the internal data of a network operator group is transmitting from onshore to offshore, it shall be deemed as data cross-border transmission if such transmission

involves PI and important data collected and generated during its onshore operation. Although the Guidelines for Data Cross-border Transmission is not an enforceable law but only a national standard, it clarifies a fundamental issue: the transmission of PI within a group from onshore to offshore shall be deemed as cross-border transmission. Based on the provisions of Article 4 of the PIPL and the Guidelines for Data Cross-border Transmission, it is obvious that the PI cross-border transmission within the group of multinational corporations shall be subject to the PIPL.

In practice, there are mainly two methods by which an onshore PI processor transmits PI to an overseas company within the same group:

- First, the onshore PI processor transmits the PI to an overseas server for processing directly with a data agreement;
- Second, the onshore PI processor stores the PI collected to the server of the data center of its overseas parent company or through the shared computer system between the parent company and its subsidiaries.

Both of the above two scenario will constitute PI cross-border transmission. We believe that PI cross-border transmission is not limited to the change of its physical location of the PI. Even if the central server in the above second scenario is located in China, if the overseas company has access to or control over the PI, such as modifying PI in the background or accessing PI for the purpose of maintaining the system, such behavior is likely to be considered as cross-border transmission. In addition, because the activities of “processing” is defined non-exhaustively in Article 4 of the PIPL, such state of "access" or "control" are also likely to be regarded as a form of "processing". Therefore, no matter from the perspective of "transmission" or "processing", the PI cross-border transmission by multinational corporations will be subject to the PIPL.

II. Extraterritorial Effect of the PIPL

Article 3 of the PIPL

This Law shall apply to any activity of processing of personal information of a natural person that is carried out within the territory of the People's Republic of China

This Law shall also apply to any activity of processing of personal information of any natural person located within the territory of the People's Republic of China that is carried out outside the territory of the People's Republic of China under any of the following circumstances:

(I) The purpose is to provide domestic natural persons with products or services;

(II) Analyzing and evaluating the behaviors of domestic natural persons;

(III) Other circumstances stipulated by laws and administrative regulations.

As for the applicable scope of the PIPL, legislators have adopted the approach of **combining territorial jurisdiction and protective jurisdiction**. As for the principle of territorial jurisdiction, the connecting point adopted by the PIPL is the "place where the behavior is conducted", that is, an entity that process PI within China shall be governed by the PIPL, no matter whether the said entity are domestic enterprises or not.

If the processing activity is conducted outside

the territory of China, the overseas entity shall assess whether it falls into the circumstances stipulated in Article 3.2 of the PIPL. The situations include both purposes criteria and act criteria, covering a wide range. Under the scenario of PI cross-border transmission of multinational corporations, the domestic enterprises will inevitably be subject to the PIPL due to their behavior of "transmission". The overseas entities usually provide domestic companies with R&D technical support, or act as information hubs to coordinate the data processing activities within the group, so they are likely to fall into the circumstances of "Where the purpose of the activity is to provide a product or service to that natural person located within China;" or " Where the purpose of the activity is to analyze or assess the behavior of that natural person located within China".

Even if the overseas entities have sufficient reasons to prove that it does not fall within the above two circumstances, the third circumstance of Article 3(2) acts as a miscellaneous provision, providing the authority more than enough discretion in practice.

It should be noted that the content and framework of PIPL have drawn lessons from Article 3 of the General Data Protection Regulation of EU ("GDPR")[1]. Although GDPR adopted the approach of combining territorial jurisdiction, personal jurisdiction, protective jurisdiction and public international law jurisdiction, through the principle of protective jurisdiction, in practice, both PIPL and GDPR has reached the extraterritorial effect of PI processing activities.

III. Specific Obligations of the Domestic and Overseas Entity

1. PI Cross-border Transmission Shall Complies with the General Requirements of the PIPL for PI Processing Activities.

First of all, as a type of PI processing activities, PI cross-border transmission should follow the general provisions of the PIPL, including but not limited to: (1) informing individuals of the identity and contact information of the personal information processor, the purpose and method of processing PI, and the types and retention period of the processed PI; (2) obtaining the individual consent of the data subject; and (3) before and following the transmission, the retention period of PI shall be the minimum period necessary for achieving the purpose of processing, etc.

Second, if the PI to be transmitted is classified as sensitive PI[2], the special provisions of Section II of Chapter II shall also apply.

Article 40 of the PIPL

Critical information infrastructure operators, or personal information processors whose processing of personal information reaches the threshold amount prescribed by the national cyberspace authority, shall store within the territory of the People's Republic of China the personal information collected or generated by them within the territory of the People's Republic of China. Where it is necessary to provide such information to an overseas recipient, a security assessment organized by the national cyberspace authority shall be passed; if a security assessment is not re-

quired as provided by law, administrative regulations or the national cyberspace authority, such provision shall prevail.

2. Special Requirements for PI Cross-border Transmission under the PIPL

2.1 Special requirements on the Nature and Quantity of PI Transmitted aboard

As stated in Article 40 of the PIPL, with respect to the (1) PI collected and generated by critical information infrastructure operators, and (2) PI cross-border transmission activities up to a certain amount, the PIPL stipulates that the principle of localized storage shall be applied. If it is necessary to transmit such data and PI aboard, it shall be subject to the security assessment organized by the Cyberspace Administration of China ("CAC").

- **Critical information infrastructure** refers to critical information infrastructure involving public communications and information services, energy, transportation, water conservancy, finance, public services, e-government and other important industries and fields, as well as other critical information infrastructure that may seriously endanger national security, national economy, people's livelihood, and public interests in the event of damage, malfunction, or leakage of PI. The requirement of localization of PI collected and generated by critical information infrastructure is to protect the security of PI. The Cybersecurity Review Measures and the Regulations on the Protection of the Security of Critical Information Infrastructure, which just came into effect on September 1, may apply as a reference to the determination of critical information infrastructure. The Lifang Team also summarized the criteria in the article *Review of Regulations on the Protection of the Security of Critical Information Infrastructure.*
- **PI up to the amount specified by CAC**: Currently, CAC has not yet defined this amount. As a reference, the Measures on the Security Assessment of PI and Important Data to be Transmitted Abroad (Exposure Draft) and the Cybersecurity Review Measures (Revised Draft for Comments) by the CAC require security assessment for the PI up to a certain amount.

Relevant Provisions	Thresholds for Security Assessment	Regulatory Requirements
Article 9 of the Measures on the Security Assessment of PI and Important Data to be Transmitted Abroad (Exposure Draft) (2017)	It contains or contains in aggregate the PI of more than 500,000 users; The data volume exceeds 1,000 GB	Network operators shall report to the competent authority or regulator of the industry to organize a security assessment if the data to be transmitted abroad
Article 6 of the Measures on the Cybersecurity Review (Revised Draft for Comments)	The PI of more than 1 million users	Operators who intend to go public abroad must apply to the Cybersecurity Review Office for cybersecurity review.

Although the above two provisions have not come into effect yet, it is understandable that the Although the above two provisions have not come into effect yet, it is understandable that the State is highly sensitive to the transmission of PI up to a certain scale and actively applies the localization principle. Therefore, in practice, if an inshore entity intending to transmit aboard the PI

of more than 500,000 users or whose size exceeds 1,000 GB, it is likely to be subject to the localization restriction.

In 2019, CAC issued the Measures for the Security Assessment of PI cross-border transmission (Exposure Draft) ("Measures"), but the Measures has not been formally published yet. Article 4 of the Measures requires network operators to submit: (1) an application form; (2) the contract signed by and between the network operator and the receiver; (3) an assessment report on the security risks for PI cross-border transmission and the relevant security measures; and (4) other materials required by CAC. Although operators are encouraged to refer to relevant regulations and guidelines in order to minimize regulatory risks, they still face the problem that no rules to follow in terms of specific obligations and procedures. Considering the rapid development of legislation on PI protection and its importance to national security, in the absence of clear guidance, it is advisable for multinational company to conduct the assessment of security risks for PI cross-border transmission and the relevant security measures before the cross-border transmission of PI, and keep the report of such assessment.

2.2 Preconditions for PI Cross-border Transmission

Due to the irreversibility of the flow of PI, the PIPL adopts a pre-supervision approach for the cross-border transmission of PI. Article 38 of the PIPL provides that where it is necessary for personal information to be provided by a personal information processor to a recipient outside the territory of the People's Republic of China due to any business need or any other need, at least one of the following conditions shall be met:

i. Where a security assessment organized by the national cyberspace authority has been passed in accordance with Article 40 of this Law;
ii. Where a certification of personal information protection has been given by a professional institution in accordance with the regulations of the national cyberspace authority;
iii. Where a contract in compliance with the standard contract provided by the national cyberspace authority has been concluded with the overseas recipient, establishing the rights and obligations of both parties; or
iv. Where any other condition prescribed by law, administrative regulations or the national cyberspace authority is met.

Security assessment or certification of PI protection shall be organized and arranged by the national cyberspace administration. As mentioned above, the relevant rules of security assessment are still in the consultation stage, and there is no reference to the certification of PI protection by professional institutions, which may be further clarified by CAC. Therefore, "enter into a contract with the overseas receiver" is a condition which is relatively practical and easy to satisfy. When conducting PI cross-border transmission, a multinational company shall require its domestic and overseas companies to enter into a contract to stipulate the rights and obligations of both parties with respect to PI processing and protection.

3. Other Requirements for PI Cross-border Transmission

Article 43 of the PIPL also stipulates the "principle of reciprocity" in PI cross-border

transmission. Any country or region that takes any discriminatory prohibition, restriction, or any other such measure against China in respect of personal information protection may be subject to reciprocal measures taken by China depending on the actual situation. Therefore, the PI cross-border transmission to such countries is likely to be restricted.

In addition, the formally passed PIPL has further improved the rules for PI cross-border transmission. Where there is any stipulation on the condition or any other stipulation for the provision of personal information to a recipient outside the territory of China in any international treaty or agreement concluded or acceded by China, such stipulation may apply. Meanwhile, the PIPL requires PI processors to take any necessary measure to ensure that the activities of the processing of the personal information provided by them carried out by overseas recipients meet the standards of personal information protection provided in this Law. We understand that such provision resolves the conflicting provisions in different jurisdictions regarding the cross-border transmission of PI, but at the same time, it impose the substantial obligation of cross-border transmission on domestic PI processors, which indirectly achieves the extraterritorial effect of the PIPL.

Annotation

[1]Article 3 of GDPR:

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[2]Sensitive personal information refers to personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal whereabouts, and other information of a natural person, as well as any personal information of a minor under the age of 14.

QIN Ying
Partner of Lifang & partners
Practice Areas:
Compliance
yingqin@lifanglaw.com

XIAO Pulingling
Associate of Lifang & partners
Practice Areas:
Antitrust and Unfair Competition
pulinglingxiao@lifanglaw.com

Subscribe to our WeChat community

扫码关注公众号“立方律师事务所”和“竞争法视界”

北京 | 上海 | 武汉 | 广州 | 深圳 | 韩国

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com
Tel：+8610 64096099
Email：info@lifanglaw.com
Fax：+8610 64096260/64096261