

Privacy Policy

Last revised: June 30, 2020

Please view our [HIPAA Notice of Privacy Practices](#) to learn more about how we use and disclose your protected health information or PHI, our legal duties with respect to your PHI, and your rights with respect to your PHI and how you may exercise them.

Tempus Labs, Inc. (“Tempus,” “our,” “us,” or “we”) respects the privacy of all visitors and users of its online services and is dedicated to maintaining the accessibility, confidentiality, and integrity of all such information. This Privacy Policy (“Policy”) applies to all visitors to and users of the Tempus website www.tempus.com and all other Tempus-owned websites, domains, services, applications, and products (“Services”).

Please read this Policy carefully. It explains what personal information we collect, why we collect it, how we use it, and

your choices related to your information.

By using our Services, you agree to this Policy. We may make changes from time to time, and it is your responsibility to periodically review this Policy for any changes. Your continued use of the Services after we make changes is deemed to be an acceptance of those changes.

Personal Information We Collect About You and How We Collect It

“Personal Information” is information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with you or your household. When you access and use the Services, we may collect the following categories of Personal Information from or about you:

- **Direct identifiers**, such as your name, address, email address, telephone number, or an IP address or other online identifier. We typically collect this information directly from you or commercially available sources (such as data aggregators, public databases and other third parties) in order to communicate with you, and provide you with access to certain information through our Services.
- **Other personal information**, such as identifiable health information, including genetic information, employment-related information, information about education and professional qualifications, including professional specialties, financial information, and demographic information like age, race, or gender. Additional information regarding our uses and disclosures of personally identifiable protected health information

(“**PHI**”) covered by the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (“**HIPAA**”) can be found in our Notice of Privacy Practices.

- **Internet activity and Service usage information**, such as the types of content you view or engage with, the features you use, the actions you take, and the time, frequency and duration of your activities, your browsing history, search history, and browser information. For example, we may log when you’re using and have last used our Services, and what content you view on our Services. We typically collect this information from our use of cookies and other data collection technologies to help us design our website, to identify popular features, and for other managerial purposes.
- **Commercial Information**, such as products and services purchased from us. We typically collect this information directly from you in order to fulfill your transactions and provide related customer service.
- **Location information**, such as information used to locate the device you use to access the Services. Location information may include: (i) the location of the device derived from GPS or WiFi use; (ii) the location derived from the IP address of the device or internet service used to access the Services, and (iii) other information made available by a user or others that indicates the current or prior location of the user. We typically collect this information from our use of cookies and other data collection technologies so that we may tailor our services to your location.
- **Profile and Inference Information**, such as information about your preferences and characteristics. We typically

collect this information directly from you and through our use of cookies and other data collection technologies in order to customize our communications and services to you.

How We Use Your Personal Information

Personal Information that you provide to us will be used as described in this Policy, our Notice of Privacy Practices, or in our Terms of Use.

We may use or disclose your Personal Information to:

- To provide you with information, products or Services that you request from us.
- To perform our contracts with you or your employer or business, or with your doctors or other healthcare providers.
- To provide you with notices and to facilitate communications deemed appropriate by us.
- To support, personalize, and develop our Services
- To comply with any legal or regulatory obligations.
- In any other way we may describe when you provide the Personal Information.
- For any other purpose permitted by law or with your lawful consent.

We may also deidentify, pseudonymize, or anonymize your Personal Information, which means that information that can be reasonably used to identify you will be removed. We aggregate the deidentified data into a multi-modal real-world dataset to empower research and improve patient care. We create and use such deidentified information as permitted by law or with your consent.

How We Share Your Personal Information

- **At Tempus.** We may share your Personal Information internally among our business units and our affiliates in order to provide you our Services and generally to improve our product and service offerings.
- **With your healthcare providers.** We may share your Personal Information with the doctors or other healthcare providers with whom you have a relationship in accordance with our agreements with those healthcare providers or consistent with applicable law. More information about our uses and disclosures of PHI can be found in our Notice of Privacy Practices
- **With vendors and other service providers.** We may share your Personal Information with service providers who perform services for us and act at our direction. These services may include activities such as cloud storage and services, fulfillment services, and other IT services. Our policy is to prohibit these service providers from using your Personal Information for purposes other than providing services to us.
- **In the event of a corporate transaction.** In the event we go through a business transition like a merger, acquisition, reorganization, or sale of all or a portion of our assets, we may disclose your Personal Information to the party or parties of such transaction.
- **To comply with our legal obligations or protect our rights.** We will disclose your Personal Information if we think doing so is necessary to investigate or prevent actual or expected fraud, criminal activity, injury or damage to us or others or when otherwise required by statute, regulation, subpoena, court order, or other law,

or if necessary to protect the rights, property, or safety of us, our employees, or others.

Cookies & Other Data Collection Technologies

A cookie is a small file placed on the hard drive of your computer. We use cookies if you have a Tempus account, use our Services, including our website and apps, or visit other websites and apps that use the Services. Cookies enable Tempus to offer the Services to you and to understand the information we receive about you, including information about your use of other websites and apps, whether or not you are registered or logged in.

You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting you may be unable to access certain parts of Tempus' Services. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you direct your browser to our website.

In addition, we may use third-party software, such as Google Analytics, to collect and process data. Google Analytics uses cookies to track your interactions with our Services, then collects that information and reports it to us, without identifying individual users. This information helps us improve our Services so that we can better serve users like you. More information about how Google uses data is located at www.google.com/analytics.

Our website does not currently recognize "Do Not Track" signals sent by some browsers.

Data Security

We use technical, physical, and administrative safeguards that are designed to improve the confidentiality, integrity and accessibility of your Personal Information and Protected Health Information. We incorporate secure storage and transmission technologies including strong encryption, firewalls, fine-grained access control and secure audit. We cannot, however, ensure or warrant the security of any information you transmit to us via the Services, and you do so at your own risk. We also cannot guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our technical, physical, or administrative safeguards.

Children's Privacy Policy

Our Services are not designed nor intended to be used or accessed by children under the age of 13. No one under age 13 may provide any information to or through the Services. We do not intentionally collect Personal Information from children through the Services. If you are under age 13, do not use or provide any information on or through the Services, including, but not limited to, your name, address, telephone number, e-mail address, user name or other. If we learn we have collected or received Personal Information from a child under age 13 without verification or parental consent, we will delete that information. If you believe that we may have collected any information, including Personal Information from or about a child under age 13, please contact us immediately at support@tempus.com.

Your California Rights

If you are a resident of California, you may be entitled to the privacy rights described below under the California

Consumer Privacy Act (“**CCPA**”). Please note that certain categories of Personal Information, such as PHI, are not covered by these CCPA privacy rights, but may be protected by HIPAA and other laws that provide similar protections.

The Right to Know. You have the right to request:

- the specific pieces of Personal Information we have about you
- the categories of Personal Information we have collected about you in the last 12 months
- the categories of sources from which that Personal Information was collected
- If we sold or disclosed your Personal Information in the last 12 months and the categories of your Personal Information that we sold or disclosed
- the categories of third parties with whom we share your Personal Information
- the purpose for collecting and selling Personal Information.

In general:

- Within the preceding 12 months, Tempus has collected the categories of personal information detailed in the section titled “Personal Information We Collect About You and How We Collect It” above.
- Tempus has not sold Personal Information about any adults or minors in the preceding 12 months.
- Tempus may disclose the categories of Personal Information that we collect to third parties as described above under “How We Share Your Personal Information.”

Specifically, Tempus has disclosed the following categories of Personal Information in the preceding 12 months: direct identifiers, other personal information, internet activity information, and commercial information.

The Right to Deletion. You have the right to request that Tempus delete the Personal Information that we have collected or maintain about you. We may deny your request under certain circumstances, such as if we need to comply with our legal obligations or complete a transaction for which your Personal Information was collected. If we deny your request for deletion, we will let you know the reason why.

Non-discrimination. Tempus will not discriminate against you in any way if you choose to exercise your rights under the CCPA. However, if we delete your Personal Information based on a request you make, understand that you may be unable to use or access certain features of our Services.

You may exercise your right to know and your right to deletion twice a year free of charge. To exercise your right to know or your right to deletion, contact us at 800-739-4137 or email us at privacy@tempus.com. We endeavor to respond to a verifiable consumer request within forty-five (45) days of receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

We will take steps to verify your identity before processing your request to know or request to delete. We will not fulfill your request unless you have provided sufficient information for us to reasonably verify you are the individual about whom we collected Personal Information. If you have an account with us, we will use our existing account authentication practices to verify your identity. If you do not have an

account with us, we may request additional information about you to verify your identity. We will only use the Personal Information provided in the verification process to verify your identity or authority to make a request and to track and document request responses, unless you initially provided the information for another purpose.

You may use an authorized agent to submit a request to know or a request to delete. When we verify your agent's request, we may verify both your and your agent's identity and request a signed document from you that authorizes your agent to make the request on your behalf. To protect your Personal Information, we reserve the right to deny a request from an agent that does not submit proof that they have been authorized by you to act on their behalf.

Other California Privacy Rights. California's "Shine the Light" law also gives California residents the rights to request certain information regarding our disclosure of their Personal Information to third parties for those third parties' direct marketing purposes. You may request information regarding the disclosure of your Personal Information to third parties for those third parties' direct marketing purposes by emailing privacy@tempus.com or writing us at the address in the Contact Information section below. Please indicate "California Rights" in the subject or attention line of your communication.

Your European Union Privacy Rights

If you are a resident of the European Union, you have certain data protection rights under the General Data Protection Regulation (GDPR).

Your Rights Under GDPR. Tempus is committed to providing individuals greater control over the processing of their personal data. You are entitled to certain rights under GDPR:

- **Right to Request Information.** You have the right to ask us questions about our processing of your Personal Data, including if you feel information is missing from this Privacy Notice.
- **Right to Access.** You have the right to request access to your Personal Data.
- **Right to Rectification.** You have the right to ask us to correct errors, or to complete omissions, in your Personal Data.
- ***Right to Erasure.** You may have the right to ask us to delete your Personal Data. Some people call this the “right to be forgotten.”
- ***Right to Object.** You may have the right to object to, and stop, our processing of your Personal Data.
- ***Right to Restriction of Processing.** You may have the right to limit our processing of your Personal Data.
- ***Right to Data Portability.** You may have the right to receive, or have us transmit to another person, a portable copy of your Personal Data.

The rights above with an asterisk (*) are subject to certain conditions or exceptions and may not be applicable under this Privacy Notice. If you want to know more about those conditions, or if you would like to exercise one or more of the rights above, please contact us at privacy@tempus.com. You can also call us at 800-739-4137, but we prefer that you reach us by email. Tempus will never discriminate against individuals who exercise their legal rights concerning their personal data.

In addition, you can always reach out to your local data protection authority for more information on your rights. The identity of your local data protection authority depends on where you live, so we are unable to identify it for you. If you live in Europe, we have found this link to be helpful:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

Our Legal Basis for Processing Personal Data Under GDPR.

We process personal data in order to perform our testing services and to bill for these services, to perform our contracts with you, and to meet our legal obligations. Additionally, our processing is necessary based on our legitimate interest of providing our healthcare and other services to you. It is likely that you provided your consent for our testing and for certain processing activities either directly to us or through your doctor.

International Transfers. As you may be aware, the United States has not been subject to a universal adequacy decision by the European Commission. This means that the European Commission has not determined that U.S. laws provide the same level of legal protections to individuals concerning their personal data and how it is used. In other words, processing in the U.S. may be undertaken with fewer privacy- and security-focused protections than in Europe, which may increase the risk of data breaches, losses of data, or similar events affecting personal data privacy and security. In any event, Tempus is firmly committed to data privacy and security and has implemented a number of measures that are intended to ensure all personal data (including your Personal Information) is protected just as strongly in the U.S. as it

might be in Europe, including entering into EU-approved model contract clauses with certain of our processors (including those vendors or service providers we've described above) and providing appropriate technical and organizational measures to secure your Personal Information (as discussed above). If you have any questions about cross-border processing, please don't hesitate to reach out to privacy@tempus.com.

Other International Visitors

This website and our Services are hosted in the United States and are intended for visitors located within the United States. Your use of the Services and provision of your information is subject to the laws and regulations of the United States and the State of Illinois. If you choose to use the Services from other regions of the world with laws governing data collection, use and disclosures that may differ from United States law, then you acknowledge and agree that (a) you are transferring your personal information outside of those regions to the United States, and (b) the laws and regulations of the United States regarding data privacy and security governing the use and disclosure of Personal Information and Protected Health Information may differ from those of your country of residence.

Changes to This Privacy Policy

It is our policy to post any changes that we make to our Privacy Policy on our website. If we make material changes to how we treat our users' Personal Information, we will update this Privacy Policy. The date our Privacy Policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable e-

mail address for you, and for periodically visiting our website and this Policy for changes. For any questions or comments regarding this Privacy Policy, please contact us at privacy@tempus.com.

Contact Information

Please contact us with any questions or comments about this Policy, your Personal Information or our Notice of Privacy Practices, or your consent choices by email at privacy@tempus.com or by mail to 600 West Chicago Avenue, Suite 510, Chicago, IL 60654 Attn: Privacy Officer.

Home	Applications	Products & Services	About Us	FAQ
Physician Login	Oncology	Genomic Profiling	Our Team	Media Kit
Patients	Neurology & Psychiatry	Data Licensing	Careers	Resources
Contact Us	Research Life Sciences	Clinical Trial Matching	Culture	
	Infectious Diseases	Companion Diagnostics	News	
		Additional Testing	Publications	

Notice of Privacy Practices

Last Modified April 15, 2019

Please view our [Privacy Policy](#) to learn more about our privacy practices for our websites and other services.

THIS NOTICE OF PRIVACY PRACTICES (“NOTICE”) DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. **PLEASE REVIEW IT CAREFULLY.**

Tempus Labs, Inc. (“Tempus,” “our,” “us,” or “we”) collects protected health information about you that is necessary to perform the genetic testing and other services we provide (“Services”). “Protected health information” or “PHI” is information about you, including demographic information, that may identify you and that relates to past, present, and/or

future physical or mental health condition and related health care services.

We reserve the right to change the terms of this Notice from time to time, and any change will apply to all PHI we maintain. The current version of this Notice is available on our website and upon request. It is your responsibility to periodically review this Notice for changes.

If you have any questions about anything in this Notice, please contact our privacy officer at privacy@tempus.com.

Our Responsibilities

Tempus is committed and required by law to maintain the privacy and security of your PHI. We are required to follow the terms of this Notice and, except as described in this Notice, will not disclose your PHI without your authorization. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information. If you provide us with authorization to use or disclose your PHI for a specific purpose and later change your mind, please let us know in writing.

Your Rights

You have certain rights when it comes to your PHI. You have the right to:

Ask that we limit how we use or share your PHI for treatment, payment, or our operations. We are not required to agree to your request and may say “no” if it could affect your care. If you pay for a service out-of-pocket in full, you can ask us not to share that information for the purposes of payment or our operations with your health insurer, in which

case we will say “yes” unless a law requires us to share that information.

Ask us to contact you in a specific and/or confidential way (for example, home or office phone) or to send mail to a different address. We will say “yes” to all reasonable requests.

Ask for an electronic or paper copy of your medical record and other information we have about you. We will provide a copy or a summary of your health information. We may charge a reasonable, cost-based fee associated with producing copies of your medical records and other information.

Ask us to correct your protected health information that you think is incorrect or incomplete. We may say “no” to this request if we believe the change would violate any law or other legal requirement or would otherwise cause the information to be incorrect, but if that is the case we will explain why in writing.

Ask for a list (accounting) of times we’ve shared your PHI in the six years prior to the date of your request, who we shared it with, and why. We will include all disclosures *except* those disclosures related to treatment, payment, and our health care operations, and certain other disclosures, such as disclosures you asked us to make. We will provide one accounting to you in any twelve (12) month period free of charge. We may charge a reasonable, cost-based fee associated with producing additional accountings in any twelve (12) month period in which you have already received a free accounting.

Ask for a paper copy of this Notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy.

Our Uses and Disclosures

Your PHI may be used and disclosed for treatment, payment, healthcare operations, and other purposes permitted or required by law. If we wish to use or disclose your PHI for other purposes, we would have to obtain your authorization. We may, however, use or disclose your PHI without specific authorization or permission for certain purposes, including:

Treatment. We may use and share your PHI to provide and coordinate your treatment with medical professionals responsible for your care. For example, we may use your PHI to perform tests, or send your test results to your health care provider.

Payment. We may use and share your health information to bill and receive reimbursement from health plans or other entities. For example, we may provide information about you to your health insurance plan so it will pay for the services you receive.

Health care operations. We may use and share your data to support the operations of our business or contact you when necessary. For example, we may retain a copy of your health information for auditing purposes or to improve our Services.

Business associates. There are some services provided to us through contracts with business associates (e.g., billing services), and we may disclose your PHI to our business associate so that they can perform the job we have asked

them to do. To further protect your PHI, we require our business associates to appropriately safeguard your information.

Communication with individuals involved in your care or payment for your care. We may disclose your PHI to a family member, other relative, close friend, or any other person you identify that is directly relevant to that person's involvement in your care or payment related to your care.

Protected health information of minors. As permitted by federal and state law, we may disclose PHI about minors to their parents or guardians.

Research activities. Researchers may be given limited access to your PHI so that they can develop research projects or identify patients who may potentially qualify to participate in research studies. We may otherwise use your PHI when it is in the form of a limited data set or once an institutional review board or privacy board has reviewed the research proposal and determined that your specific authorization or consent for the research use of your PHI is not needed in whole or in part.

Creating "de-identified" information. We may use your PHI to create "de-identified" information, which means that information that can be reasonably used to identify you will be removed. There are specific rules under the law about what type of information needs to be removed before information is considered de-identified. Once the information has been de-identified as required by law, it is no longer considered PHI, not covered by this Notice, and we may use it for any lawful purpose without further notice or compensation to you.

As required to comply with laws. We may disclose your PHI when required to do so by federal, state, or local law.

Law enforcement activity. We may disclose your PHI to law enforcement officers for law enforcement purposes as permitted by law or in response to a valid subpoena or court order.

Judicial and administrative proceedings. We may disclose your PHI in response to a court or administrative order, a subpoena, discovery request, or other lawful process by someone involved in a lawsuit or dispute with or against you.

Public health activities and threats to health and safety. We may disclose your PHI to public health or other legal authorities charged with preventing or controlling disease, receiving report of suspected abuse, neglect, or domestic violence, receiving reports of adverse reactions to medications or devices, notifying people of recalls of products, or otherwise preventing or reducing serious threats to the health and safety of you, others, or the public generally.

Health oversight activities. We may disclose your PHI to an oversight agency for activities authorized by law, including audits, investigations, and inspections necessary for licensure and for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Food and Drug Administration (FDA) activities. We may disclose your PHI to the FDA, or persons under the jurisdiction of the FDA, when the PHI is related to adverse events with respect to drugs, foods, supplements, products and product defects, or post marketing surveillance

information to enable product recalls, repairs, or replacement.

Military or veteran affairs. We may disclose your PHI as required by military command authorities if you are or were a member of the armed forces.

Specialized government functions. We may disclose your PHI to units of the government with specialized functions such as the U.S. Military or the U.S. Department of State in response to requests authorized by law.

Correctional institutions. We may disclose your PHI to a correctional institution or its agents for your health and the health and safety of other individuals if you are or become an inmate in the correctional institution.

Worker's compensation. We may disclose your PHI to the extent authorized by and the extent necessary to comply with laws relating to worker's compensation or other similar programs established by law.

Death. We may disclose your PHI to a coroner, medical examiner, or funeral director to identify a deceased person, determine the cause of death, or otherwise carry out their duties.

Organ tissue procurement organizations. We may disclose your PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for tissue donation and transplant.

Other Uses and Disclosures of PHI

We will obtain your written authorization before using or disclosing your PHI for purposes other than those described above, including uses and disclosures of psychotherapy notes or PHI for marketing purposes, and disclosures that would constitute a sale of PHI. You may revoke this authorization in writing at any time. Upon receipt of the written revocation, we will stop using or disclosing your PHI, except to the extent that we have already taken action in reliance on the authorization.

In some circumstances, your health information may be subject to additional state-level restrictions that limit or preclude some uses or disclosures described in this Notice. For example, many states have restrictions on the use or disclosure of certain categories of information like HIV/AIDS treatment, treatment for mental health conditions or developmental disabilities, or alcohol and drug abuse treatment. Similarly, state government health benefit programs may limit the disclosure of beneficiary information for purposes unrelated to the program. Some states have laws that specifically protect the privacy of your genetic information.

Reporting a Problem

If you believe your privacy rights have been violated, you may file a complaint with us directly or with the Secretary of the Department of Health and Human Services by filing a complaint with the Office for Civil Rights. We will not retaliate against you in any way for filing a complaint.

Contact Information

Please contact us with any questions, comments, or complaints about this Notice, your rights and PHI, our use and disclosure practices, or your authorization choices by email at privacy@tempus.com, by mail at 600 West Chicago Avenue, Suite 510, Chicago, IL 60654, or by calling us at 800-739-4137.

Home
**Physician
Login**
Patients
**Contact
Us**

Applica
Oncology
Neurology
&
Psychiatry
Research
Life
Sciences
Infectious
Diseases

Product
**&
Services**
Genomic
Profiling
Data
Licensing
Clinical
Trial
Matching
Companion
Diagnostics
Additional
Testing

**About
Us**
Our
Team
Careers
Culture
News
Publications

FAQ
**Media
Kit**
Resources