



## VACTRACK PRIVACY POLICY

Last updated March 01, 2024

This privacy notice for Patient First.AI INC (“we,” “us,” or “our”), describes how and why we might collect, store, use, and/or share (“**process**”) your information when you use our services (“**Services**”), such as when you:

- Visit our website at <http://vactrack.patientfirstai.com>, or any website of ours that links to this privacy notice
- Download and use our mobile application (Patient First.AI VAC TRACK ), or any other application of ours that links to this privacy notice
- Engage with us in other related ways, including any sales, marketing, or events

**Questions or concerns?** Reading this privacy notice will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com).

### SUMMARY OF KEY POINTS

*This summary provides key points from our privacy notice, but you can find out more details about any of these topics by clicking the link following each key point or by using our [table of contents](#) below to find the section you are looking for.*

**What personal information do we process?** When you visit, use, or navigate our Services, we may process personal information depending on how you interact with us and the Services, the choices you make, and the products and features you use. Learn more about [personal information you disclose to us](#).

**Do we process any sensitive personal information?** We may process sensitive personal information when necessary with your consent or as otherwise permitted by applicable law. Learn more about [sensitive information we process](#).

**Do we receive any information from third parties?** We may receive information from public databases, marketing partners, social media platforms, and other outside sources. Learn more about [information collected from other sources](#).

---

#### CONFIDENTIAL



**How do we process your information?** We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so. Learn more about [how we process your information](#).

**In what situations and with which parties do we share personal information?** We may share information in specific situations and with specific third parties. Learn more about [when and with whom we share your personal information](#).

**How do we keep your information safe?** We have organizational and technical processes and procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Learn more about [how we keep your information safe](#).

**What are your rights?** Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information. Learn more about [your privacy rights](#).

**How do you exercise your rights?** The easiest way to exercise your rights is by visiting [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com), or by contacting us. We will consider and act upon any request in accordance with applicable data protection laws.

Want to learn more about what we do with any information we collect? [Review the privacy notice in full](#).

## TABLE OF CONTENTS

- [1. WHAT INFORMATION DO WE COLLECT?](#)
- [2. HOW DO WE PROCESS YOUR INFORMATION?](#)
- [3. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)
- [4. HOW LONG DO WE KEEP YOUR INFORMATION?](#)
- [5. HOW DO WE KEEP YOUR INFORMATION SAFE?](#)
- [6. DO WE COLLECT INFORMATION FROM MINORS?](#)

---

### CONFIDENTIAL



7. WHAT ARE YOUR PRIVACY RIGHTS?

8. CONTROLS FOR DO-NOT-TRACK FEATURES

9. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

10. DO WE MAKE UPDATES TO THIS NOTICE?

11. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

12. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

## 1. WHAT INFORMATION DO WE COLLECT?

### Personal information you disclose to us

*In Short:* We collect personal information that you provide to us.

We collect personal information that you voluntarily provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

**Personal Information Provided by You.** The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal information we collect may include the following:

- names
- phone numbers
- email addresses
- mailing addresses
- contact preferences
- usernames
- passwords
- contact or authentication data
- phi
- dates
- fax numbers
- social security numbers

---

**CONFIDENTIAL**



- medical record numbers
- health plan beneficiary numbers
- account numbers
- certificate/license numbers
- vehicle identification numbers (vins)
- device identifiers and serial numbers
- web urls
- internet protocol (ip) addresses
- biometric identifiers (e.g., fingerprints, voiceprints)
- full face photographic images
- any other unique identifying number, characteristic, or code

**Sensitive Information.** When necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of sensitive information:

- health data
- genetic data
- biometric data
- data about a person's sex life or sexual orientation
- information revealing race or ethnic origin
- student data
- social security numbers or other government identifiers
- general health data
- previous and current treatments

**Application Data.** If you use our application(s), we also may collect the following information if you choose to provide us with access or permission:

---

**CONFIDENTIAL**



- *Geolocation Information.* We may request access or permission to track location-based information from your mobile device, either continuously or while you are using our mobile application(s), to provide certain location-based services. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Access.* We may request access or permission to certain features from your mobile device, including your mobile device's storage, camera, sensors, and other features. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Data.* We automatically collect device information (such as your mobile device ID, model, and manufacturer), operating system, version information and system configuration information, device and application identification numbers, browser type and version, hardware model Internet service provider and/or mobile carrier, and Internet Protocol (IP) address (or proxy server). If you are using our application(s), we may also collect information about the phone network associated with your mobile device, your mobile device's operating system or platform, the type of mobile device you use, your mobile device's unique device ID, and information about the features of our application(s) you accessed.
- *Push Notifications.* We may request to send you push notifications regarding your account or certain features of the application(s). If you wish to opt out from receiving these types of communications, you may turn them off in your device's settings.

This information is primarily needed to maintain the security and operation of our application(s), for troubleshooting, and for our internal analytics and reporting purposes.

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

## **Information collected from other sources**

***In Short:** We may collect limited data from public databases, marketing partners, and other outside sources.*

In order to enhance our ability to provide relevant marketing, offers, and services to you and update our records, we may obtain information about you from other sources, such as public databases,

---

**CONFIDENTIAL**



joint marketing partners, affiliate programs, data providers, and from other third parties. This information includes mailing addresses, job titles, email addresses, phone numbers, intent data (or user behavior data), Internet Protocol (IP) addresses, social media profiles, social media URLs, and custom profiles, for purposes of targeted advertising and event promotion.

## 2. HOW DO WE PROCESS YOUR INFORMATION?

*In Short: We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.*

**We process your personal information for a variety of reasons, depending on how you interact with our Services, including:**

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate delivery of services to the user.** We may process your information to provide you with the requested service.
- **To respond to user inquiries/offer support to users.** We may process your information to respond to your inquiries and solve any potential issues you might have with the requested service.
- **To send administrative information to you.** We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.
- **To request feedback.** We may process your information when necessary to request feedback and to contact you about your use of our Services.
- **To protect our Services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To evaluate and improve our Services, products, marketing, and your experience.** We may process your information when we believe it is necessary to identify usage

---

### CONFIDENTIAL



trends, determine the effectiveness of our promotional campaigns, and to evaluate and improve our Services, products, marketing, and your experience.

- **To comply with our legal obligations.** We may process your information to comply with our legal obligations, respond to legal requests, and exercise, establish, or defend our legal rights.

### 3. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

*In Short: We may share information in specific situations described in this section and/or with the following third parties.*

We may need to share your personal information in the following situations:

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

### 4. HOW LONG DO WE KEEP YOUR INFORMATION?

*In Short: We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). No purpose in this notice will require us keeping your personal information for longer than one (1) months past the termination of the user's account.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

### 5. HOW DO WE KEEP YOUR INFORMATION SAFE?

---

**CONFIDENTIAL**



***In Short:** We aim to protect your personal information through a system of organizational and technical security measures.*

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

## **6. DO WE COLLECT INFORMATION FROM MINORS?**

***In Short:** We do not knowingly collect data from or market to children under 18 years of age.*

We do not knowingly solicit data from or market to children under 18 years of age. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at [ernest.park@patientfirstai.com](mailto:ernest.park@patientfirstai.com).

## **7. WHAT ARE YOUR PRIVACY RIGHTS?**

***In Short:** You may review, change, or terminate your account at any time.*

**Withdrawing your consent:** If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

---

**CONFIDENTIAL**





## Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account settings and update your user account.
- Contact us using the contact information provided.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

If you have questions or comments about your privacy rights, you may email us at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com).

## 8. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track (“DNT”) feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this privacy notice.

## 9. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

***In Short:** If you are a resident of California, Colorado, Connecticut, Utah or Virginia, you are granted specific rights regarding access to your personal information.*

### **What categories of personal information do we collect?**

We have collected the following categories of personal information in the past twelve (12) months:

---

**CONFIDENTIAL**



# Patient**FIRST**

Office of the **Chief Information Security Officer**

Category	Examples	Collected
A. Identifiers	Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	YES
B. Personal information as defined in the California Customer Records statute	Name, contact information, education, employment, employment history, and financial information	YES
C. Protected classification characteristics under state or federal law	Gender and date of birth	YES
D. Commercial information	Transaction information, purchase history, financial details, and payment information	NO
E. Biometric information	Fingerprints and voiceprints	NO
F. Internet or other similar network activity	Browsing history, search history, online behavior, interest data, and interactions with our and other websites, applications, systems, and advertisements	NO
G. Geolocation data	Device location	NO

**CONFIDENTIAL**



H. Audio, electronic, visual, thermal, olfactory, or similar information	Images and audio, video or call recordings created in connection with our business activities	NO
I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level or job title, work history, and professional qualifications if you apply for a job with us	NO
J. Education Information	Student records and directory information	YES
K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	NO
L. Sensitive personal Information	Account login information, health data, biometric data, genetic data, sex life or sexual orientation, social security numbers, racial or ethnic origin and state id card numbers	YES

We will use and retain the collected personal information as needed to provide the Services or for:

- Category A – As long as the user has an account with us
- Category B – As long as the user has an account with us
- Category C – As long as the user has an account with us
- Category J – As long as the user has an account with us
- Category L – As long as the user has an account with us

Category L information may be used, or disclosed to a service provider or contractor, for additional, specified purposes. You have the right to limit the use or disclosure of your sensitive personal information.

---

## CONFIDENTIAL



We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation in customer surveys or contests; and
- Facilitation in the delivery of our Services and to respond to your inquiries.

### **How do we use and share your personal information?**

Learn about how we use your personal information in the section, [“HOW DO WE PROCESS YOUR INFORMATION?”](#)

### **Will your information be shared with anyone else?**

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Learn more about how we disclose personal information to in the section, [“WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?”](#)

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be “selling” of your personal information.

We have not disclosed, sold, or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. We will not sell or share personal information in the future belonging to website visitors, users, and other consumers.

### **California Residents**

California Civil Code Section 1798.83, also known as the “Shine The Light” law permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

---

#### **CONFIDENTIAL**



If you are under 18 years of age, reside in California, and have a registered account with the Services, you have the right to request removal of unwanted data that you publicly post on the Services. To request removal of such data, please contact us using the contact information provided below and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Services, but please be aware that the data may not be completely or comprehensively removed from all our systems (e.g., backups, etc.).

## **CCPA Privacy Notice**

This section applies only to California residents. Under the California Consumer Privacy Act (CCPA), you have the rights listed below.

The California Code of Regulations defines a “residents” as:

- (1) every individual who is in the State of California for other than a temporary or transitory purpose and
- (2) every individual who is domiciled in the State of California who is outside the State of California for a temporary or transitory purpose

All other individuals are defined as “non-residents.”

If this definition of “resident” applies to you, we must adhere to certain rights and obligations regarding your personal information.

### **Your rights with respect to your personal data**

#### **Right to request deletion of the data — Request to delete**

You can ask for the deletion of your personal information. If you ask us to delete your personal information, we will respect your request and delete your personal information, subject to certain

---

**CONFIDENTIAL**



# Patient**FIRST**

Office of the **Chief Information Security Officer**

---

exceptions provided by law, such as (but not limited to) the exercise by another consumer of his or her right to free speech, our compliance requirements resulting from a legal obligation, or any processing that may be required to protect against illegal activities.

## Right to be informed — Request to know

Depending on the circumstances, you have a right to know:

- whether we collect and use your personal information;
- the categories of personal information that we collect;
- the purposes for which the collected personal information is used;
- whether we sell or share personal information to third parties;
- the categories of personal information that we sold, shared, or disclosed for a business purpose;
- the categories of third parties to whom the personal information was sold, shared, or disclosed for a business purpose;
- the business or commercial purpose for collecting, selling, or sharing personal information; and
- the specific pieces of personal information we collected about you.

In accordance with applicable law, we are not obligated to provide or delete consumer information that is de-identified in response to a consumer request or to re-identify individual data to verify a consumer request.

## Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

We will not discriminate against you if you exercise your privacy rights.

## Right to Limit Use and Disclosure of Sensitive Personal Information

If the business collects any of the following:

- social security information, drivers' licenses, state ID cards, passport numbers
- account login information

---

### **CONFIDENTIAL**



- credit card numbers, financial account information, or credentials allowing access to such accounts
- precise geolocation
- racial or ethnic origin, religious or philosophical beliefs, union membership
- the contents of email and text, unless the business is the intended recipient of the communication
- genetic data, biometric data, and health data
- data concerning sexual orientation and sex life

you have the right to direct that business to limit its use of your sensitive personal information to that use which is necessary to perform the Services.

Once a business receives your request, they are no longer allowed to use or disclose your sensitive personal information for any other purpose unless you provide consent for the use or disclosure of sensitive personal information for additional purposes.

Please note that sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not covered by this right, as well as the publicly available information.

To exercise your right to limit use and disclosure of sensitive personal information, please email [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com) or visit: [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com).

#### Verification process

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. These verification efforts require us to ask you to provide information so that we can match it with information you have previously provided us. For instance, depending on the type of request you submit, we may ask you to provide certain information so that we can match the information you provide with the information we already have

---

**CONFIDENTIAL**



on file, or we may contact you through a communication method (e.g., phone or email) that you have previously provided to us. We may also use other verification methods as the circumstances dictate. We will only use personal information provided in your request to verify your identity or authority to make the request. To the extent possible, we will avoid requesting additional information from you for the purposes of verification. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes. We will delete such additionally provided information as soon as we finish verifying you.

#### Other privacy rights

- You may object to the processing of your personal information.
- You may request correction of your personal data if it is incorrect or no longer relevant, or ask to restrict the processing of the information.
- You can designate an authorized agent to make a request under the CCPA on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA.
- You may request to opt out from future selling or sharing of your personal information to third parties. Upon receiving an opt-out request, we will act upon the request as soon as feasibly possible, but no later than fifteen (15) days from the date of the request submission.

To exercise these rights, you can contact us by visiting [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com), by email at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com), or by referring to the contact details at the bottom of this document. If you have a complaint about how we handle your data, we would like to hear from you.

## Colorado Residents

This section applies only to Colorado residents. Under the Colorado Privacy Act (CPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

---

#### **CONFIDENTIAL**





- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

To submit a request to exercise these rights described above, please email [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com) or visit [infosec@patientfirstai.com](https://infosec.patientfirstai.com).

If we decline to take action regarding your request and you wish to appeal our decision, please email us at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com). Within forty-five (45) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

## **Connecticut Residents**

This section applies only to Connecticut residents. Under the Connecticut Data Privacy Act (CTDPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us

---

**CONFIDENTIAL**



- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

To submit a request to exercise these rights described above, please email [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com) or visit [infosec@patientfirstai.com](https://infosec.patientfirstai.com).

If we decline to take action regarding your request and you wish to appeal our decision, please email us at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com). Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

## Utah Residents

This section applies only to Utah residents. Under the Utah Consumer Privacy Act (UCPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising or the sale of personal data

To submit a request to exercise these rights described above, please email [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com) or visit [infosec@patientfirstai.com](https://infosec.patientfirstai.com).

## Virginia Residents

Under the Virginia Consumer Data Protection Act (VCDPA):

---

### **CONFIDENTIAL**



“Consumer” means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

“Personal data” means any information that is linked or reasonably linkable to an identified or identifiable natural person. “Personal data” does not include de-identified data or publicly available information.

“Sale of personal data” means the exchange of personal data for monetary consideration.

If this definition of “consumer” applies to you, we must adhere to certain rights and obligations regarding your personal data.

Your rights with respect to your personal data

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

Exercise your rights provided under the Virginia VCDPA

You may contact us by email at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com) or visit [infosec@patientfirstai.com](https://infosec.patientfirstai.com).

---

**CONFIDENTIAL**



# Patient**FIRST**

Office of the **Chief Information Security Officer**

---

If you are using an authorized agent to exercise your rights, we may deny a request if the authorized agent does not submit proof that they have been validly authorized to act on your behalf.

## Verification process

We may request that you provide additional information reasonably necessary to verify you and your consumer's request. If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request.

Upon receiving your request, we will respond without undue delay, but in all cases, within forty-five (45) days of receipt. The response period may be extended once by forty-five (45) additional days when reasonably necessary. We will inform you of any such extension within the initial 45-day response period, together with the reason for the extension.

## Right to appeal

If we decline to take action regarding your request, we will inform you of our decision and reasoning behind it. If you wish to appeal our decision, please email us at [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com). Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may contact the [Attorney General to submit a complaint](#).

## **10. DO WE MAKE UPDATES TO THIS NOTICE?**

***In Short:** Yes, we will update this notice as necessary to stay compliant with relevant laws.*

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.

## **11. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?**

---

**CONFIDENTIAL**

Patient First.AI | RISK MANAGEMENT FRAMEWORK  
Patient First.AI, 129 Franklin Street, Apt 414, Cambridge MA 02139 | Page 20 of 21

©2024 Airius, LLC



# Patient**FIRST**

Office of the **Chief Information Security Officer**

---

If you have questions or comments about this notice, you may contact our Data Protection Officer (DPO), Ernest M. Park, by email at [ernest.park@patientfirstai.com](mailto:ernest.park@patientfirstai.com), by phone at 9173363440, or contact us by post at:

Patient First.AI INC  
Ernest M. Park  
857 Post Rd suite 234  
Fairfield, CT 06824  
United States

If you have any further questions or comments, you may also contact us by post at the following corporate address:

Patient First.AI INC  
Batten Hall, 125 Western Ave  
Allston, MA 02134  
United States  
Phone: 9173363440

## **12. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?**

You have the right to request access to the personal information we collect from you, change that information, or delete it. To request to review, update, or delete your personal information, please visit: [infosec@patientfirstai.com](mailto:infosec@patientfirstai.com).

This privacy policy was created using Termly's [Privacy Policy Generator](#).

---

**CONFIDENTIAL**

Patient First.AI | RISK MANAGEMENT FRAMEWORK  
Patient First.AI, 129 Franklin Street, Apt 414, Cambridge MA 02139 | Page 21 of 21