



Privacy Policy

Last updated January 12, 2022

Docket® (“Docket”) is an mobile-optimized application that connects American healthcare consumers to personal and family health data. This policy outlines how we use and protect your data. Thank you for using Docket.

Introduction

Docket Health, Inc. (“Docket,” “we,” or “us”) is dedicated to respecting the privacy rights of our customers, visitors, and other users of dockethealth.com (the “Site”) and related websites, applications, services, and mobile applications provided by Docket and on/in which this Privacy Policy is posted or referenced (collectively, the “Services”). This Privacy Policy (“Privacy Policy”) outlines our commitment to the protection of privacy. This Privacy Policy is only applicable to the Services. This Privacy Policy does not apply to any other website or digital service that you may be able to access through the Services. Your use of the Services is governed by this Privacy Policy and the Agreement (as the term “Agreement” is defined in our Terms of Use). Any capitalized term used but not defined in this Privacy Policy shall have the meaning in the Agreement.

BY USING THE SERVICES, YOU AGREE TO THE PRACTICES AND POLICIES OUTLINED IN THIS PRIVACY POLICY AND YOU HEREBY CONSENT TO THE COLLECTION, USE, AND SHARING OF YOUR INFORMATION AS DESCRIBED IN THIS PRIVACY POLICY. IF YOU DO NOT AGREE WITH THIS PRIVACY POLICY, YOU CANNOT USE THE SERVICES. IF YOU USE THE SERVICES ON BEHALF OF SOMEONE ELSE (SUCH AS YOUR CHILD) OR AN ENTITY (SUCH AS YOUR EMPLOYER), YOU REPRESENT THAT YOU ARE AUTHORIZED BY SUCH INDIVIDUAL OR ENTITY TO ACCEPT THIS PRIVACY POLICY ON SUCH INDIVIDUAL’S OR ENTITY’S BEHALF.

Personal Information

When you access the Services, we may ask you to voluntarily provide us certain information that personally identifies (or could be used to personally identify) you (“Personal Information”). Personal Information includes, but is not limited to, the following: (a) contact data such as your email address and phone number; (b) demographic data such as your gender, your date of birth, and your address including ZIP Code; and (c) other information that you voluntarily choose to provide to us including without limitation your Social Security Number, unique identifiers such as passwords, and Personal Information in emails or letters that you send to us.

You may still access and use some of the Services if you choose not to provide us with some Personal Information, but certain features may not be accessible to you as a result.



Traffic Data

We also may automatically collect certain data elements when you use the Services, such as (a) IP address; (b) domain server; (c) type of device(s) used to access the Services; (d) web browser(s) used to access the Services; (e) referring webpage or other source through which you access the Services; (f) geolocation information; and (g) other statistics and information associated with the interaction between your browser or device and the Services (collectively “Traffic Data”). Depending on applicable law, some Traffic Data may be Personal Information. We may also collect additional information, which may be Personal Information, as otherwise described to you at the point of collection or pursuant to your consent.

HIPAA and PHI

Under a federal law called the Health Insurance Portability and Accountability Act (“HIPAA”), some of the demographic, health, and/or health-related information that Docket collects as part of providing the Services may be considered “protected health information” or “PHI.” Specifically, when Docket receives identifiable information about you from you and/or on behalf of your Healthcare Providers and/or health department, this information is treated by Docket as PHI. HIPAA provides specific protections for the privacy and security of PHI and restricts how PHI is used and disclosed.

Today, Docket primarily relies on email addresses and phone numbers on-file with state immunization registries to verify your identity in order to vend personal and/or family immunization records. You are responsible for ensuring that your personal and/or family immunization records on-file with the state are accurate and complete. Docket cannot guarantee that an estranged or former spouse, for example, would not have access to your and/or your child’s immunization records. Please contact your health department to ensure the phone numbers and email addresses on-file with your state’s immunization registry belong only to you. Docket recommends that you do not share your passwords and/or Docket verification PINs needed in order to access your personal and/or family immunization records.

DOCKET ENABLES PATIENT USERS TO VOLUNTARILY AND SELECTIVELY TRANSMIT PHI TO TRUSTED THIRD PARTIES.

How We Collect Information

We collect information (including Personal Information and Traffic Data) when you use and interact with the Services, and in some cases from third-party sources. Such information includes (but is not limited to): when you use the Services’ interactive tools, send us an email, or otherwise contact us.



How We Use Information

We use the information we collect, including Personal Information, to provide and continuously improve the Services. When Docket users use the Services to query state immunization registries to access personal and/or family immunization records, Docket will collect user-reported information (e.g. First Name, Last Name, Date of Birth, Sex, cellphone number, and/or email). Docket retrieves and stores information from state immunization registries such as but not limited to immunization records (including line-level detail about shots such as when and where immunizations were administered, immunization manufacturer, and other relevant clinical information), immunization forecasting schedules, allergies, contradictions, immunities, home address, and renderings of official state-issued immunization reports and certificates. Docket primarily stores immunization data for the user's enjoyment. Docket reports deidentified immunization-related data (e.g. number of immunization records obtained using Docket) to state immunization registries and other public health partners. We may use information that is neither Personal Information nor PHI (including non-PHI Personal Information that has been de-identified and/or aggregated) to better understand who uses Docket and how we could enhance our products and services. Docket indicates within the application what user-reported data is required in order to provide the Services.

Disclosure of Information

We may disclose certain information that we collect from Patient Users. Docket will not disclose Personal Information without your consent. For example, we may disclose certain information (e.g. COVID-19 immunization records) to third parties at the user's request when the user presents their SMART[®] Health Card QR code to a verifier. We do not sell email addresses to third parties. We may, however, choose to share your email addresses with our business partners to enable them to help Docket customize our advertising.

We may use information that is neither Personal Information nor PHI (including non-PHI Personal Information that has been de-identified and/or aggregated) to better understand who uses Docket and how we could enhance our products and services. We may also need to disclose your Personal Information or any other information we collect if we determine in good faith that such disclosure is needed to: (a) comply with applicable law, regulation, court order, or other legal process; (b) protect the rights, property, or safety of Docket or another party; (c) enforce the Agreement or other agreements with you; or (d) respond to claims that any posting or other content violates third-party rights.

Public Information

Any information that you may reveal in a review posting or online discussion or forum is intentionally open to the public and is not in any way private. We strongly recommend that



you carefully consider whether or not to disclose any Personal Information in a public posting or forum. If you decide to visit a third-party website, you are subject to the privacy policy of the third-party website as applicable.

Information Security

Your privacy is important to us. As such, we endeavor to follow generally accepted standards to protect Personal Information submitted to us, both in storing and during transmission. Personal Information submitted to Docket is encrypted. Although we make good faith efforts to store Personal Information in a secure operating environment, we do not and cannot guarantee the security of your Personal Information.

If we become aware that your Personal Information has been disclosed in a manner not in accordance with this Privacy Policy, we will use reasonable efforts to notify you of the nature and extent of the disclose (to the extent we know that information) as soon as reasonably possible and as permitted or required by applicable law.

Information Provided by or on Behalf of Children

The Services are not intended for use by children under the age of 13. Docket does not knowingly collect information from children, not are the Services directed to children. By accessing, using and/or submitting information to or through the Services, you represent that you are not younger than age 13.

If we learn that we have received any information directly from a child under age 13 without his/her parent's consent, we will use that information only to respond directly to that child (or his/her parent or legal guardian) to inform the child that he/she cannot use the Services and subsequently we will delete that information. If you are between age 13 and the age of majority in your place of residence, you may use the Services only with the consent of or under the supervision of your parent or legal guardian.

If you are a parent or legal guardian of a minor child, you may, in compliance with the Agreement, use the Services on behalf of such minor child. Any information that you provide us while using the Services on behalf of your minor child will be treated as Personal Information.

Controlling Personal Information

Registered Patient Users may view and modify certain data elements, including Personal Information, submitted to Docket.

Docket reserves the right to retain information from closed accounts, including to comply



with law, prevent fraud, resolve disputes, enforce the Agreement, and take other actions permitted by applicable law.

Immunization Records

If you choose to utilize the Services to search state and local immunization registries, you authorize Docket to query state immunization registries identified in the application and certify that you are authorized to access any relevant immunization records you obtain through Docket. Docket utilizes user-provided data (i.e. First Name, Last Name, Date of Birth, Sex, and your verified cellphone or email addresses) to search state and local immunization registries. Docket verifies your cellphone and/or email addresses via multi-factor authentication. If you believe that anybody has unauthorized access to any of your cellphone numbers or email addresses, you must rectify the situation immediately by either: (a) changing all relevant passwords or; (b) contacting your state or local immunization registry. If you believe that an estranged spouse, partner, or anybody not authorized to access your child's records has access to your child's records through Docket, you must contact your state or local immunization registry immediately to resolve any custody-related issues.

Additional Disclosures for California Residents

This section applies to California residents when and if the California Consumer Privacy Act is applicable to our Site and Services about whom we have collected Personal Information, including through the use of our Site or Services, by purchasing or utilizing our Service, or by communicating with us electronically, in paper correspondence, or in person. For purposes of this section, the term "Personal Information" includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household.

We may disclose the following types of Personal Information to third parties for a business or commercial purpose, as further described: identifiers, medical and health insurance information, protected classifications under applicable law, commercial information, biometric information, internet or similar network activity, geolocation data, sensory data, professional or employment-related information, alerts for upcoming or overdue immunizations, and inferences from other Personal Information. Functionality within the Docket platform enables consumers to consolidate and share Personal Information with third parties. You may be entitled by applicable law to exercise the following rights with respect to your Personal Information:

- **Right to Know.** You have the right to request what Personal Information we collect, use, disclose, and/or sell, as applicable. Please note that Docket clearly indicates within the app what data is collected in order for Docket to perform the Services.



- Right to Delete. You have the right to request that we delete the Personal Information that we have collected about you. Users have the ability to delete their information under Settings & Info within the app.
- Right to Opt-out of the Sale of Personal Information. You have the right to request to be opted-out from the sale of your Personal Information. Please note that Docket does not sell user-provided information with third parties without your consent.
- Right to Non-Discrimination. You have the right not to receive discriminatory treatment by us for the exercise of the privacy right described herein.

You may also authorize someone to exercise the above rights on your behalf. If we have collected information on your minor child (e.g. immunization records), you may exercise the above rights on behalf of your minor child. In addition, residents of California also have the right to request once per calendar year certain information with respect to types of Personal Information (as defined by California law) we share with third parties for those third parties' direct marketing purposes, as the identities of the third parties with whom we have shared such information during the immediately preceding calendar year.

The above rights are subject to our ability to reasonably verify your identity and authority to make these requests by providing verifiable information such as the following:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we have collected Personal Information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it. We cannot respond to your request if we cannot verify your identity or authority to make the request and confirm the Personal Information relates to you.

In addition, the above rights are subject to various exclusions and exceptions under the law, and, under certain circumstances, we may be unable to implement your request.

COVID-19 Immunization Records

Through partnership with public health agencies, Docket offers consumer access to COVID-19 immunization records. As such, Docket only accesses personal and sensitive data required directly to support COVID-19-related efforts. Specifically, Docket uses this data to facilitate consumer access to personal and family immunization records.

Camera

Docket supports the capability for users to select a profile picture. This functionality is entirely optional. Docket users that choose to select a profile picture will need to engage their



phone's camera and/or saved photos. The profile picture capability may not be available to certain users based on the specific application version installed on the user's phone.

External File Storage

Docket supports the capability for users to share and/or save a PDF copy of their personal and family immunization records. As such, Docket may require access to read and/or write to your phone's file storage.

Biometric Login

Docket supports biometric login (e.g. Apple Face ID, Touch ID) as an optional feature for added security. If activated, Docket may store Device Identifiers. Device Identifiers include, but are not limited to, the following: (a) IMEI; (b) serial number; and (c) device name. Information collected to enable biometric login is not used by Docket for any other purposes. You do not need to enable biometric login in order to use the Services.

Privacy Policy Updates

We will notify you of any material changes to this Privacy Policy. Your continued use of the Services after changes to this Privacy Policy constitutes your acceptance of the amended Privacy Policy. The amended Privacy Policy supersedes all previous versions. **IF YOU DO NOT AGREE TO FUTURE CHANGES TO THIS PRIVACY POLICY, YOU MUST STOP USING THE SERVICES AFTER SUCH CHANGES OCCUR.**