Privacy Policy: Your Privacy Rights

This Policy is Effective as of 23rd September, 2020

Last Revision Date: 23rd September, 2020

Scope and Purpose

This privacy policy describes the practices of athenahealth, Inc., ("athenahealth", "our", "we", or "us") with regard to information that we obtain, either directly or indirectly through you and/or third-parties, through your use of the athenaOne mobile application, including all associated content and/or documentation (collectively, (as may be renamed, rebranded or incorporated into our other offerings), "App"). App is a mobile application that is designed to facilitate healthcare providers ("Providers") ability to track and manage patient encounters and records and facilitates the transmission of data to and from an underlying electronic health record platform (the "Platform"). The term "you" refers to a Provider end user of App.

This policy does not apply to (i)athenahealth.com or Epocrates.com or any other mobile application offered by us; (ii) information that we obtain outside of App; (iii) applications of third parties to which we provide links or (iv) third party Platforms. We do not control and are not responsible for the privacy practices of, or the data available on or through, the applications of third parties or third-party Platforms, and we urge you to evaluate the soundness of these practices for yourself.

Please note that this policy also does **not** apply to information that:

- You have given us your consent to share or use information about you;
- We believe that we need to share information about you to provide a service that you have requested from us;
- We are required by law to disclose information; or
- We believe that it is necessary to protect our rights or to avoid liability or violations of the law.

We urge you to read this Privacy Policy so that you understand our commitment to you and your privacy, and how you can participate in that commitment. By using App, you consent to athenahealth's collection, use, disclosure, transfer and storage of information relating to you as set forth in this Privacy Policy.

WHAT INFORMATION DO WE COLLECT?

Information you provide to us

The types of information that we process may include:

- Your name and contact information, App credentials, specialty, email address, practice id, practice name, biometric information when used to access the App (i.e. fingerprint), photograph of yourself that you may upload into the App and other information you enter into the App;
- User preferences (Ex. Default department, search filters selected in the App);
- Support cases reported by you within the App;
- Your response to surveys / feedbacks requested within the App;
- Content created as a result of your use of dictation functionality; and
- Video content provided by you through your use of the App.

Information Automatically Collected

- Whenever you use the App, we may automatically collect data about your device such as your user id, user name, device Info (device id, iOS version, model name, device resolution, device token, device free ram), App diagnostic logs (App state, audit / access logs), IP address (country, city, time zone- based on IP address).
- Information about your use of App including, but not limited to, your usage patterns, screens visited, etc.

HOW DO WE USE YOUR INFORMATON?

athenahealth uses the information collected to provide App and to improve upon the App functionality. We may also use information collected from you in order to:

- provide you with any other information, products or services that you request from us;
- track the popularity of features on the application to guide the development of new features;
- send you related information, including confirmations, technical notices, updates, security alerts, and support and administrative messages.

SHARING YOUR INFORMATION

athenahealth may share your information (i) with other entities if needed to comply with laws or to respond to lawful requests and legal process; (ii) to protect the rights and property of our agents, customers, and others, including to enforce our agreements, policies and terms of use; (iii) with your employer or other entity that contracts for App with athenahealth on your behalf; (iv) in an emergency to protect the personal safety of athenahealth, its customers, or any person; (v) with contractors, service providers and other third parties we use to support our business and who are bound by contractual obligation to keep information confidential and use it only for the purposes for which we disclose it to them; (vi) for improving upon App functionality or (vii) with our subsidiaries or affiliates.

Finally, your information may be shared in connection with, or during negotiation of any merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of athenahealth's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding.

Security Measures Taken to Protect Personal Information by Us

Security of all information is of the utmost importance for athenahealth. athenahealth uses technical, physical and administrative safeguards to protect the security of your personal information from unauthorized disclosure.

Data Retention and Storage

athenahealth retains your information for business purposes, for as long as your account is active or as long as is reasonably necessary to provide you with our products and services, or as otherwise set forth in the App's Terms of Use. athenahealth will also retain your information as reasonably necessary to comply with our legal obligations, resolve disputes and enforce our agreements. We may also retain cached or archived copies of your information for a reasonable period. Notwithstanding the above, athenahealth reserves the right to erase the content of any messages at any time.

Collection of Information from Children

athenahealth recognizes the importance of protecting the privacy and safety of children. Our website and services are directed towards the general audience and are not directed towards children. We do not knowingly collect information about children under the age of 16 or minors otherwise defined in local law or regulation without verifiable parental consent.

Privacy Notice for California Residents

This **Privacy Notice for California Residents** supplements the information contained in the above referenced privacy policy and applies solely to all visitors, users, and others who reside in the State of California ("consumers" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (CCPA) and any terms defined in the CCPA have the same meaning when used in this Notice.

Where noted in this Notice, the CCPA temporarily exempts personal information reflecting a written or verbal business-to-business communication ("**B2B personal information**") from some its requirements.

Information We Collect

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer, household, or device ("**personal information**"). Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:

- health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA);

In particular, we have collected the following categories of personal information from its consumers within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	YES
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES
J. Non-public education	Education records directly related to a student maintained by an educational institution or party acting on its behalf,	NO

information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	YES

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from you. For example, from your use of the App and its functionality.
- Indirectly from you. For example, from observing your actions on our App.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following purposes:

- To fulfill or meet the reason you provided the information. For example, when you provide your personal information in connection with your use of the App, we will use that information to provide you with functionality We may also save your information to improve the App and its future fucntionality.
- To provide, support, personalize, and develop our Website, products, and services and the App.
- To create, maintain, customize, and secure your account with us.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To personalize your Website or App experience and to deliver content and product and service offerings relevant to your interests.
- To help maintain the safety, security, and integrity of our Website, products and services, the App, databases and other technology assets, and our business.
- For testing, research, analysis, and product development, including to develop and improve our Website, products, services and the App.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us about our users or Providers is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract

We share your personal information with the following categories of third parties:

- Service providers.

Disclosures of Personal Information for a Business Purpose

In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

Category A: Identifiers.

Category B: California Customer Records personal information categories.

Category E: Biometric information.

Category F: Internet or other similar network activity.

Category G: Geolocation data.

Category H: Sensory data.

Category I: Professional or employment-related information.

Category K: Inferences drawn from other personal information.

We disclose your personal information for a business purpose to the following categories of third parties:

- Service providers.

Sales of Personal Information

In the preceding twelve (12) months, we have not sold personal information.

Your Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion 0), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information for a business purpose, a list including:
    - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

We do not provide these access and data portability rights for B2B personal information.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion 0), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing

business relationship with you, fulfill the terms of a written warranty conducted in accordance with federal law, or otherwise perform our contract with you.

2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We do not provide these deletion rights for B2B personal information.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us at 888-807-2076.
- www.athenahealth.com/consumer-privacy-request

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative, which may include:
    - Name, address and email address.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time we will inform you of the reason and extension period in writing.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

Other California Privacy Rights

California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our App that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email at consumerprivacyrequests@athenahealth.com or write us at: Compliance Department, athenahealth, Inc. Watertown, MA 02472.

Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will post the updated notice on the App and update the notice's effective date. **Your continued use of our App following the posting of changes constitutes your acceptance of such changes**.

Contact Information

If you have any questions or comments about this notice, the ways in which athenahealth collects and uses your information described here and in the above referenced **Privacy Policy**, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

- Calling us at 888-807-2076.
- Completing the form at www.athenahealth.com/consumer-privacy-request
- Via mail at:
    - athenahealth, Inc.
    - Attn: Chief Compliance Officer
    - 311 Arsenal Street
    - Watertown, MA 02472