

Athens Administrators

Privacy Policy

Last Revision: 5/30/19

Table of Contents

Privacy Policy 3

- What personal information do we collect from the people that visit our website or app?... 3**
- When do we collect information? 3**
- How do we use your information? 3**
- How do we protect visitor information?..... 3**
- Do we use ‘cookies’? 4**
- We use cookies to: 4**
- If users disable cookies in their browser:..... 4**
- Third Party Disclosure 4**
- Third party links..... 5**
- Google..... 5**
- California Online Privacy Protection Act 5**
- According to CalOPPA we agree to the following:..... 5**
- How does our site handle do not track signals? 6**
- Does our site allow third party behavioral tracking? 6**
- COPPA (Children Online Privacy Protection Act) 6**
- Fair Information Practices..... 6**
- CAN SPAM Act 7**

HIPPA Privacy Practices Notification..... 8

- UNDERSTANDING YOUR HEALTH RECORD AND INFORMATION 8**
- HOW WE MAY USE AND DISCLOSE PROTECTED HEALTH INFORMATION ABOUT YOU 8**
- OTHER ALLOWABLE USES OF YOUR HEALTH INFORMATION 8**
- OTHER USES OF HEALTH INFORMATION 9**
- YOUR RIGHTS REGARDING HEALTH INFORMATION ABOUT YOU 9**
- CHANGES TO THIS NOTICE 10**
- COMPLAINTS 10**
- Contacting Us..... 11**
- Document Change Approval Requirements..... 11**
- Revision History and Approval Matrix 11**

Privacy Policy

This privacy policy has been compiled to better serve those who are concerned with how their 'Personally identifiable information' (PII) is being used online. PII, as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personally Identifiable Information in accordance with our website.

What personal information do we collect from the people that visit our website or app?

When ordering or registering on our site, as appropriate, you may be asked to enter your name, email address, phone number, social security number, PHI, PII or other details to help you with your experience.

When do we collect information?

We collect information from you when you Information is submitted into the SIMS Claim Management System or enter information on our site.

How do we use your information?

We may use the information we collect from you when you register, or use certain other site features in the following ways:

- To allow us to better service you in responding to your customer service requests.
- To allow our customers to administer insurance claims

How do we protect visitor information?

Our website is scanned on a regular basis for security holes and known vulnerabilities in order to make your visit to our site as safe as possible.

We use regular Malware Scanning.

Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential. In addition, all sensitive/credit information you supply is encrypted via Secure Socket Layer (SSL) technology. All sensitive information is encrypted in transit, in flight, and at rest.

We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information.

For your convenience we will store your PHI / PII information for more than 60 days in order to allow for the proper administration of insurance claims.

Do we use 'cookies'?

Yes. Cookies are small files that a site or its service provider transfers to your computer's hard drive through your Web browser (if you allow) that enables the site's or service provider's systems to recognize your browser and capture and remember certain information.

We use cookies to:

- Authenticate and store log-in and session information

You can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off all cookies. You do this through your browser (like Internet Explorer) settings. Each browser is a little different, so look at your browser's Help menu to learn the correct way to modify your cookies.

If users disable cookies in their browser:

If you disable cookies off, some features will be disabled. It will turn off some of the features that make your site experience more efficient and some of our services will not function properly.

Third Party Disclosure

We do not sell, or trade, to outside parties your personally identifiable information.

Third party links

We do not include or offer third party products or services on our website.

Google

We have not enabled Google AdSense in our SIMS Claims Administration System. We reserve the right to enable Google AdSense on our public website in the future.

California Consumer Privacy Act

CCPA is the first state law in the nation to require commercial websites and online services to post a privacy policy. The law's reach stretches well beyond California to require a person or company in the United States (and conceivably the world) that operates websites collecting personally identifiable information from California consumers to post a conspicuous privacy policy on its website stating exactly what information is being collected and those individuals with whom it is being shared, and to comply with this policy. – See more at: <https://oag.ca.gov/privacy/ccpa>

According to CCPA we agree to the following:

Users can visit our site anonymously

Once this privacy policy is created, we will add a link to it on our home page, or as a minimum on the first significant page after entering our website.

Our Privacy Policy link includes the word 'Privacy', and can be easily be found on the page specified above.

Users will be notified of any privacy policy changes:

- On our Privacy Policy Page

Users are able to change their personal information:

- By emailing us
- By calling us
- By logging in to their account

How does our site handle do not track signals?

We do not honor do not track signals and do not track, plant cookies, or use advertising when a Do Not Track (DNT) browser mechanism is in place. We do not honor them because our application is dependent on cookies in order to maintain session data as well as login information

Does our site allow third party behavioral tracking?

It is also important to note that we do not allow third party behavioral tracking

COPPA (Children Online Privacy Protection Act)

When it comes to the collection of personal information from children under 13, the Children’s Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, the nation’s consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children’s privacy and safety online.

We do not specifically market to children under 13.

Fair Information Practices

The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur:

We will notify the users via email once the scope of the breach has been determined

We will notify the users via in site notification once the scope of the breach has been determined

We also agree to the individual redress principle, which requires that individuals have a right to pursue legally enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or a government agency to investigate and/or prosecute non-compliance by data processors.

CAN SPAM Act

The CAN-SPAM Act is a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have emails stopped from being sent to them, and spells out tough penalties for violations.

We collect your email address in order to provide you with services related to your claim(s).

To be in accordance with CANSPAM we agree to the following:

If at any time you would like to unsubscribe from receiving future emails, you can email your Examiner and we will promptly remove you from **ALL** email correspondence.

HIPPA Privacy Practices Notification

THIS NOTICE DESCRIBES HOW YOUR MEDICAL INFORMATION MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

This Facility is required by law to provide you with this Notice so that you will understand how we may use or share your information from your Designated Record Set. The Designated Record Set includes financial and health information referred to in this Notice as “Protected Health Information” (“PHI”) or simply “health information.” We are required to adhere to the terms outlined in this Notice. If you have any questions about this Notice, please contact privacy@systemasoft.com.

UNDERSTANDING YOUR HEALTH RECORD AND INFORMATION

Each time you utilize our application, a record of your stay is made containing health and financial information. Typically, this record contains information about your condition, the treatment provided and payment for the treatment. We may use and/or disclose this information to:

- Manage and administer claim information on behalf of our clients

Understanding what is in your record and how your health information is used helps you to:

- ensure it is accurate
- better understand who may access your health information
- make more informed decisions when authorizing disclosure to others

HOW WE MAY USE AND DISCLOSE PROTECTED HEALTH INFORMATION ABOUT YOU

The following categories describe the ways that we use and disclose health information. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall into one of the categories.

OTHER ALLOWABLE USES OF YOUR HEALTH INFORMATION

- **Business Associates**. There are some services provided by our application through contracts with business associates. Examples include medical directors, outside attorneys. When these services are contracted, we may disclose your health information so that they can perform the job we’ve asked them to do. To protect your health information, however, we require the business associate to appropriately safeguard your information.
- **As Required By Law**. We will disclose health information about you when required to do so by federal, state or local law.
- **To Avert a Serious Threat to Health or Safety**. We may use and disclose health information about you to prevent a serious threat to your health and safety or the health and safety of the public or another person. We would do this only to help prevent the threat.
- **Workers’ Compensation**. We may disclose health information about you for workers’ compensation or similar programs. These programs provide benefits for work-related injuries or illness.
- **Reporting** Federal and state laws may require or permit The Company to disclose certain health information related to the following:
 - ***Public Health Risks***. We may disclose health information about you for public health purposes, including:
 - Prevention or control of disease, injury or disability
 - Reporting births and deaths;

- Reporting child abuse or neglect;
 - Reporting reactions to medications or problems with products;
 - Notifying people of recalls of products;
 - Notifying a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease;
 - Notifying the appropriate government authority if we believe a resident has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.
- *Judicial and Administrative Proceedings:* If you are involved in a lawsuit or a dispute, we may disclose health information about you in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.
 - *Reporting Abuse, Neglect or Domestic Violence:* Notifying the appropriate government agency if we believe a resident has been the victim of abuse, neglect or domestic violence.
- **Law Enforcement.** We may disclose health information when requested by a law enforcement official:
 - In response to a court order, subpoena, warrant, summons or similar process;
 - To identify or locate a suspect, fugitive, material witness, or missing person;
 - About you, the victim of a crime if, under certain limited circumstances, we are unable to obtain your agreement;
 - About a death we believe may be the result of criminal conduct;
 - About criminal conduct at The Company; and
 - In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.
 - **National Security and Intelligence Activities.** We may disclose health information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

OTHER USES OF HEALTH INFORMATION

Other uses and disclosures of health information not covered by this Notice or the laws that apply to us will be made only with your written permission.

YOUR RIGHTS REGARDING HEALTH INFORMATION ABOUT YOU

Although your health record is the property of The Company, the information belongs to you. You have the following rights regarding your health information:

- **Right to Inspect and Copy.** With some exceptions, you have the right to review and copy your health information.

You must submit your request in writing to itsupport@athensadmin.com. We may charge a fee for the costs of copying, mailing or other supplies associated with your request.

- **Right to an Accounting of Disclosures.** You have the right to request an “accounting of disclosures”. This is a list of certain disclosures we made of your health information, other than those made for purposes such as treatment, payment, or health care operations.

You must submit your request in writing to itsupport@athensadmin.com. Your request must state a time period which may not be longer than six years from the date the request is submitted and may not include

dates before January 1, 2010. Your request should indicate in what form you want the list (for example, on paper or electronically). The first list you request within a twelve month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Request Restrictions.** You have the right to request a restriction or limitation on the health information we use or disclose about you. For example, you may request that we limit the health information we disclose to someone who is involved in your care or the payment for your care. You could ask that we not use or disclose information about a surgery you had to a family member or friend.

We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

You must submit your request in writing to itsupport@athensadmin.com In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

- **Right to Request Alternate Communications.** You have the right to request that we communicate with you about medical matters in a confidential manner or at a specific location. For example, you may ask that we only contact you via mail to a post office box.

You must submit your request in writing to itsupport@athensadmin.com We will not ask you the reason for your request. Your request must specify how or where you wish to be contacted. We will accommodate all reasonable requests.

CHANGES TO THIS NOTICE

We reserve the right to change this Notice. We reserve the right to make the revised or changed Notice effective for health information we already have about you as well as any information we receive in the future. In addition, if material changes are made to this Notice, the Notice will contain an effective date for the revisions and copies can be obtained by contacting The Company administrator.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with The Company or with the Secretary of the Department of Health and Human Services. To file a complaint with The Company, contact itsupport@athensadmin.com All complaints must be submitted in writing. **You will not be penalized for filing a complaint.**

Contacting Us

If there are any questions regarding this privacy policy you may contact us using the information below.

www.athensadmin.com

PO Box 4029

Concord, CA 94524

United States

itsupport@athensadmin.com

Document Change Approval Requirements

The Athens Administrators Director of IT is responsible for approving any changes to this document.

Revision History and Approval Matrix

Description	Author	Date
V1.0 – Draft using new layout	Don Barnwell	1/2/2018
V2.0 – Updated per CCPA and GDPR	Don Barnwell	5/30/2019