Guide to Sharing Information with Third-party Applications

Your Ability to Share Information with Third-party Applications

As a Lasso Healthcare member, you have the right to easily access your health information, such as claims and encounter information including cost, using a third-party application of your choice. We maintain a secure, standards-based Patient Access Application Programming Interface ("API") that you can request to connect to via a third-party application on your phone, tablet, or computer. The ability to access your health information is one way Lasso Healthcare is committed to innovating your healthcare experience and giving you the necessary tools to play an active role in your healthcare journey.

If you choose to share your health information with a third-party application, you should be aware of privacy and security considerations before allowing access to your data. When you allow a third-party application to access your health information, Lasso Healthcare will share all of the information that we maintain about you in the Patient Access API. Third-party applications may have less strict privacy and security standards than Lasso Healthcare when it comes to securing your health information. Use the information within this guide to help you navigate the privacy and security decisions you will face when you allow data access to third-party applications.

Considerations for Data Collection and Use by Third-party Applications

Choosing to share your health information with a third-party application is an important decision that requires your understanding of the third-party application's Privacy Policy and Terms of Use and the considerations you should make before allowing access. Once you agree to allow a third-party application to access to your health information, the information may no longer be governed by the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules. In accordance with the HIPAA Privacy and Security Rules, covered entities such as Lasso Healthcare, your doctors, and healthcare billing services must comply with the Rule's requirements and implement safeguards to protect the privacy and security of health information. You can find more information related to HIPAA covered entities on pages 6 and 7.

When you register as a user of a third-party application the first step you should take before allowing access is to read the Privacy Policy and Terms of Use of the third-party application. Once you have read the Privacy Policy and Terms of Use, and if you still have questions, review the information in sections A – F below to help you make an informed decision on sharing your health information.

When you review the Privacy Policy and Terms of Use, make sure the third-party application clearly answers the following questions:

- What health data will this third-party application collect?
- Will this third-party application collect non-health data from my device, such as my location?
- Will my data be stored in a de-identified or anonymized form?
- How will this third-party application use my data?
- Will this third-party application disclose my data to third parties?
- Will this third-party application sell my data for any reason, such as advertising or research?

- Will this third-party application share my data for any reason? If so, with whom? For what purpose?
- How can I limit this third-party application's use and disclosure of my data?
- What security measures does this third-party application use to protect my data?
- What impact could sharing my data with this third-party application have on others, such as my family members?
- How can I access my data and correct inaccuracies in data retrieved by this third-party application?
- Does this third-party application have a process for collecting and responding to user complaints?
- If I no longer want to use this third-party application, or if I no longer want this third-party application to have access to my health information, how do I terminate the third-party application's access to my data?
- What is the third-party application's policy for deleting my data once I terminate access? Do I have to do more than just delete the application from my device?

If the third-party application does not clearly answer these questions or does not have a Privacy Policy or Terms of Use, you may want to reconsider allowing the third-party application access to your health information. In addition to reviewing the third-party application's Privacy Policy and Terms of Use to help answer these questions, you can also use the sections below to gain additional understanding about the privacy and security considerations to look for before allowing access.

A. Personal Data Collection

When you register as a user, a third-party application should list the personal data they will collect within their Privacy Policy and Terms of Use. Personal data may include information such as:

- Your name,
- Email address,
- Gender,
- Date of birth,
- A unique account password,
- Location of residence,
- Information about your state or driver's license, or
- Personal well-being activities (e.g., exercise activities)

Personal data may be collected to improve your experience using the third-party application and the accuracy of the information the third-party application is attempting to share with you.

Consider whether or not you are willing to allow a third-party application to store this information. You should give extra attention to any of the third-party application's Privacy Policy information about de-identifying

your personal data for research purposes. When a third-party application de-identifies your data, it ensures that any of your data that may be shared with business partners or used for research purposes will not be associated with you.

B. Data Use

Third-party applications should not collect or use your personal data without telling you. When a third-party application has access to your data, it should only use it for reasons stated within the application's Privacy Policy. If the third-party application wants to use your personal data in ways outside of the Privacy Policy or Terms of Use, then the third-party application should ask for your additional, separate consent.

Lasso Healthcare encourages you to review the Privacy Policy for use of personal data and give special attention to any information related to the sale of your personal data that may be found within a third-party application's Privacy Policy or Terms of Use. Third-party applications that access your health information should not sell your data, and if you do not see a statement regarding prohibition of selling your information within the Privacy Policy, you may decide against sharing your health information.

C. Privacy Rights

Consider the rights you have as a user of the third-party application. The Privacy Policy and Terms of Use should include information about whether or not you have the right to: correct your personal data, restrict the processing of your data, access your personal data, and erase your personal data. If a third-party application's Privacy Policy or Terms of Use does not define your rights and how to exercise them, or you are concerned by a lack of user rights, it may be in your best interest not to share your health information with the third-party application.

D. Retention of your Personal Data

A third-party application will likely retain your personal data while your account is active but should also clarify how it stores your data when your account is inactive or after it is deleted. If a third-party application keeps your data stored when you are no longer active, you may consider whether or not the third-party application's retention policy justifies the continued use of your health information.

E. Security of Your Personal Data

A third-party application should take all reasonable and appropriate measures to protect your personal data and health information from loss, theft, misuse, unauthorized access, disclosure, alteration, and destruction. Health information contains sensitive personal identifiers that should remain secure when sharing with a third-party application. Review the third-party application's Privacy Policy and Terms of Use to assess the policy for the security of your personal data and health information. If a third-party application does not share information about the steps it takes to secure your personal data, you may want to avoid sharing your health information with the third-party application.

F. Third-party Application Developer Contact Information

Before allowing access to your health information, you should make sure a third-party application has listed contact information in the event you have questions about their policies or the use of your data and health information.

Lasso Healthcare's Third-party Application Privacy Policy Attestation Process

To further help inform you about a third-party application's practices for handling your healthcare information, Lasso Healthcare has a process to request that third-party applications attest to important Privacy Policy standards. As part of this process, an attestation status is determined by the third-party application's voluntary and self-reported certification to Lasso Healthcare that it will follow best practices for collecting, storing, using and sharing your health information.

When you use a third-party application to connect to Lasso Healthcare's Patient Access API, you will be presented with a choice to "Allow Access" or "Do Not Allow Access" for the third-party application to access your health information. In order to allow Lasso Healthcare to proceed in sharing your health information with a third-party application, you must select "Allow Access" when prompted. To support you in making the important decision to allow access to a third-party application, Lasso Healthcare will share the attestation status on record for the third-party application you are using. There are three attestation statuses that a third-party application may be assigned:

- Positive attestation status – The positive attestation status message means that the third-party application you are requesting to share your health information with has notified Lasso Healthcare that it has a Privacy Policy in place that includes recommended provisions to protect and responsibly use your data.
- No attestation on record status – If a third-party application is not known to Lasso Healthcare or has not yet responded to Lasso Healthcare's Privacy Policy attestation request, then the no attestation on record status will be assigned. If presented with this attestation status for the third-party application of your choosing, Lasso Healthcare advises you to contact us at (800) 918-3859 (TTY: 711) so that we may initiate a request for the third-party application to attest to important privacy standards. You may also consider revisiting the third-party application's sign-in page to approve access at a later date to see whether the third-party application has since returned the Privacy Policy attestation form.
- Negative attestation status – The negative attestation status message means that the third-party application you are requesting to share your health information with has notified Lasso Healthcare that it does not have privacy and security standards that meet Lasso Healthcare's recommended provisions to protect and responsibly use your data. If a third-party application has a negative attestation status on record, Lasso Healthcare advises you to consider the potential risks of sharing your health information with the third-party application.

Lasso Healthcare members ultimately have control to make decisions about sharing their health information. Lasso Healthcare will not block you from sharing your health information with a third-party application of your choosing, regardless of the third-party application's attestation status. If you are interested in using a third-party application that does not include Lasso Healthcare as a supported health plan within the third-party application's connection options, you may request that Lasso Healthcare initiates a registration process with that application by calling us at (800) 918-3859 (TTY: 711).

If you have chosen to share your health information with a third-party application via the Lasso Healthcare Patient Access API in the past, and no longer wish to allow the third-party application to continue to access your health information, please call Lasso Healthcare at (800) 918-3859 (TTY: 711).

Federal Oversight of Third-party Applications and Filing Complaints

Lasso Healthcare is committed to protecting your health information and hopes you will use this guide to make informed decisions about sharing your health information with third-party applications. Allowing a third-party application to access your health information will often mean that your health information leaves the protections of HIPAA. Use the information below to further understand which businesses and organizations are governed by HIPAA or other regulating entities and how to file a complaint against the appropriate governing body. If you have questions about filing privacy complaints with the Federal government, follow the instructions included in sections B – C below.

A. Understanding HIPAA Covered Entities

The Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule is a federal law that establishes national standards which require covered entities to protect your health information and prohibits those entities from disclosing your health information without your consent or knowledge. Covered entities are the individuals and organizations that are subject to the HIPAA privacy rule and are listed below:

- Health Plans – your health insurance provider (e.g., Lasso Healthcare)
- Healthcare Clearinghouses – an entity that process nonstandard health information that they receive from a healthcare provider into a standard format or data content and forwards the processed transaction to a Health Plan, or vice versa (e.g., Billing Services, Repricing Companies)
- Healthcare Providers – any healthcare provider (e.g., Doctors, Clinics) who electronically submit HIPAA transactions for which the U.S. Department of Health and Human Services ("HHS") has adopted as a standard
- Business Associates – individuals or organizations using or disclosing your health information to provide services or business functions to a covered entity (e.g., third-party administrator that assists a health plan with claims processing)

Lasso Healthcare is considered a HIPAA covered entity (a Health Plan) and abides by the national standards to protect your medical records and other personal health information. However, if you request to send your information to a third-party application, your health information is usually no longer governed by the same privacy standards as required by HIPAA unless the third-party application meets the definition of one of the covered entities listed above.

B. The Office of Civil Rights' responsibility to oversee compliance with HIPAA

HIPAA gives you certain rights and choices to request your health information, correct your health information and request confidential communications of your health information, among other options to

manage your healthcare. You can refer to Lasso Healthcare's Privacy Policy to review your specific rights and choices as required by HIPAA. Covered entities, including Lasso Healthcare, must respect your authority to control your health information as required by HIPAA.

If you believe a HIPAA covered entity is discriminating against or violating your rights as described by HIPAA, you may file a complaint against the covered entity to the US Office of Civil Rights ("OCR") at the US Department of Health and Human Services Office For Civil Rights | Complaint Portal Assistant.

Although the OCR is responsible for overseeing HIPAA covered entities, it no longer has the authority to address complaints against non-covered entities. Section C, below, describes situations in which you can file a complaint against a third-party application that you have shared your health information with.

U.S. Office of Civil Rights Contact Information:

Address	U.S. Department of Health and Human Services 200 Independence Avenue, SW Room 509F, HHH Building Washington, D.C. 20201
Email	OCRMail@hhs.gov
Toll-free phone number	(800) 368-1019
TDD toll-free	(800) 537-7697

C. The Federal Trade Commission's responsibility to take action against unfair or deceptive practices regarding health information management

The Federal Trade Commission ("FTC") is the nation's leading consumer protection agency. The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. When you share your healthcare data with a third-party application, the health information that Lasso Healthcare will share with the third-party application is not likely covered by HIPAA or under the authority of the OCR, but instead under enforcement of the FTC. Unless explicitly stated within a third-party application's Privacy Policy as being a HIPAA covered entity, the FTC Act applies to third-party application developers, technology companies and social media sites. Using its authority, the FTC may bring an enforcement action against a third-party application that has access to your health information if, for instance, the third-party application departs from its Privacy Policy practices.

If you believe a third-party application has violated their Privacy Policy or Terms of Use or misled you in its privacy and security standards, you should file a complaint at ReportFraud.ftc.gov

U.S. Federal Trade Commission Contact Information:

Address	Federal Trade Commission Headquarters 600 Pennsylvania Avenue, NW Washington, D.C. 20580
Phone number	(202) 326-2222
TTY	1-866-653-4261

Appendix A

Key Terms and Definitions to understand the data that may be associated with your health information available through Lasso Healthcare's Patient Access API.

a. **Claim**: Used by providers and insurers to exchange the financial information, and supporting clinical information, regarding the provision of health care services with payers and for reporting to regulatory bodies and firms which provide data analytics.
b. **Coverage:** The insurance or medical plan or a payment agreement.
c. **EOB:** "Explanation of Benefits" is a statement that is sent once a claim is processed and explains the processing of the claim.
d. Member: Demographics and other administrative information about an individual receiving care or other health-related services.
e. **Organization:** The healthcare entity that has provided care or other services.
f. **Provider:** A person or group of individuals who help in identifying or preventing or treating illness.