

LEGAL

PRIVACY POLICY

Effective October 16, 2026. Last updated October 24, 2026. How Excalibur collects, uses, protects and shares information on this website, in AskMerlin and in the services we provide to healthcare organizations.

IN SHORT:

- ◆ We do not sell personal information, patient information or client data. Ever.
- ◆ This website is for learning about Excalibur and reaching us. It is not a channel for patient information. Please do not send protected health information through the forms or by email.
- ◆ When we work for a healthcare provider, we handle protected health information as a HIPAA business associate, under a Business Associate Agreement, only for the services we were engaged to perform.
- ◆ AskMerlin, our analytics platform, is governed by client agreements, role-based access and client data segregation. Identifiable client or patient data is not used to train generalized AI models.
- ◆ The site sets no advertising or cross-site tracking cookies. If analytics are enabled, we say so below and you can opt out.
- ◆ You can ask what we hold about you, ask us to correct or delete it, and opt out of marketing at any time, using the contact details at the end.

THIS POLICY AT A GLANCE

Who you are to us decides what we hold, why, who else touches it and for how long. The sections below give the detail.

IF YOU ARE A	WE MAY HOLD	WE USE IT TO	IT MAY BE PROCESSED BY	WE KEEP IT
Website visitor who contacts us	Name, title, organization, work email, phone, facility type, interest, message; server logs	Respond, schedule the conversation you asked for, keep a record of the inquiry	Web3Forms (form delivery), our hosting provider	Inquiry records up to 3 years; server logs 90 days
Client user of AskMerlin	Business contact details, credentials, permissions, login and audit logs, usage, device and network diagnostics	Provision and secure accounts, enforce role-based access, troubleshoot, investigate misuse	Hosting, security and technology providers under contract	Life of the account plus the audit period the client agreement sets
Patient of a client provider	Demographics, account and insurance data, claims, balances, payments, diagnosis and procedure codes	Only the revenue cycle services the provider engaged us to perform, under a Business Associate	The provider, its designated recipients, and subcontractors bound by a BAA	As the client agreement and law require, then returned or destroyed

WHO WE ARE AND WHAT THIS POLICY COVERS

Excalibur Data Driven Performance Management (Excalibur DDPM, Excalibur, we, our, us) is a healthcare finance and revenue cycle performance management, analytics and outsourcing firm headquartered at 417 Monument Road, Unit 2, Grand Junction, Colorado 81507.

This Privacy Policy describes how we collect, use, protect and share information through this website (excaliburrcm.com, excaliburrcm.health and excalibur-ddpm.com), through our AskMerlin analytics platform and its applications (including B41C, The Grail, The Lady of the Lake, Gwen, the Analytics Portal, Wizards and Scrolls, and any future module), and in the course of the revenue cycle, analytics, consulting and outsourcing services we provide to healthcare providers and other clients.

Where we process information on behalf of a client under a services agreement or a Business Associate Agreement, that agreement and applicable law govern and take precedence over this policy. This policy does not replace a healthcare provider's own Notice of Privacy Practices.

INFORMATION WE COLLECT

Website visitors. When you request a Readiness Assessment or contact us, we collect what you give us: name, title, organization, work email, phone, facility type, area of interest and your message. Our hosting provider also records standard server logs (IP address, browser and device type, pages viewed, referring page, date and time) for security and reliability.

Clients and AskMerlin users. To administer and secure the platform we process business contact details, usernames and account identifiers, authentication and permission information, login timestamps, session and audit logs, application usage, and device, browser and network diagnostics. This information lets us provision accounts, enforce role-based access, troubleshoot and investigate suspected misuse.

Information we process for clients. In delivering revenue cycle services, we may access patient demographic and account information, insurance eligibility, coverage, claims and remittance data, balances, payment histories and statements, diagnosis and procedure codes where authorized and necessary, denial and account notes, and related financial and operational data. Much of this is protected health information. We process it only within the scope of the client's instructions, the governing agreement and applicable law.

Workforce, applicants and vendors. We process employment, recruiting and vendor contact information for hiring, contract administration, internal operations and compliance. Those relationships may be covered by additional notices.

We do not knowingly collect information from children. This website is directed to businesses and healthcare organizations, not to individuals under 18.

HOW WE USE INFORMATION

We use information only for purposes reasonably related to the services we were engaged to provide and the operation of our business: performing contracted revenue cycle, analytics, consulting and outsourcing services; providing reporting, dashboards and insights through AskMerlin; responding to your inquiries and scheduling conversations you asked for; administering user accounts and enforcing access controls; operating, securing, maintaining and improving our systems; detecting and responding to security incidents, fraud and misuse; keeping business records; and meeting contractual, legal, regulatory and audit obligations.

Access to information is not permission to use it. We do not use information for an unrelated purpose simply because it is technically available to a team member, an administrator or an application.

Marketing. If you give us your business contact details we may send you information about Excalibur services and insights. Every marketing email includes an unsubscribe link, and you can opt out at any time by contacting us. We do not add anyone to a newsletter without asking.

HIPAA AND PROTECTED HEALTH INFORMATION

Where Excalibur acts as a business associate under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we handle protected health information in accordance with the HIPAA Privacy, Security and Breach Notification Rules, the HITECH Act and the terms of the governing Business Associate Agreement. We use and disclose protected health information only as permitted or required by that agreement and by law, apply appropriate safeguards, report qualifying security incidents and breaches within the required timeframes, and require the same protections from any subcontractor permitted to access it.

Where a client agreement or Business Associate Agreement is stricter than this policy, the stricter terms govern.

This website is not a system for patient information. Please do not submit patient names, account numbers, medical or billing details through the contact form or by email. If you are a patient with a question about your account, statement or records, contact the healthcare provider that treated you; they hold your records and can respond to your request.

PATIENT COMMUNICATIONS AND COLLECTIONS

Some of the services we provide on a healthcare provider's behalf involve contacting patients directly: mailing statements, answering billing questions, offering payment plans, resolving insurance and payment discrepancies, and following up on balances. When we do, we act for the provider, we identify ourselves and the provider we represent, and we use the contact details and preferences the provider holds for you.

Channels and consent. We may contact you by mail, phone, text message, email or a patient portal, as the provider's agreement and applicable law allow. We text or email only where you or the provider have given us a number or address for that purpose, and you can withdraw consent at any time: reply STOP to any text, use the unsubscribe link in any email, or tell the representative you speak with. Message and data rates may apply. We do not contact patients at times or places we know to be inconvenient, and we honor requests to stop calling a particular number.

Call recording. Calls with our patient services team may be recorded and monitored for quality, training, accuracy and compliance. You will hear a notice at the start of the call where the law requires one. Recordings are protected as client information and kept only as long as the client agreement and law require.

Collections. Where an account has been placed with us for collection and our activity is subject to the Fair Debt Collection Practices Act, Regulation F or a state collection law, we comply with those laws: we provide the required validation information, we honor disputes and requests for verification, we communicate only as permitted, and we never misrepresent who we are, what is owed or what will happen if a balance is not paid. If you believe a balance is wrong, tell us or the provider in writing; we will investigate before continuing.

Financial assistance. If you cannot pay, ask. Nonprofit hospitals are required to offer financial assistance, and most of the providers we work with have charity care and payment plan options. We will tell you how to apply.

Your records. The provider remains the owner and custodian of your medical and billing records. Requests to access, correct or restrict those records go to the provider; we will help them respond as the agreement and law require.

WE DO NOT SELL INFORMATION. HOW WE SHARE IT

Excalibur does not sell, rent or license personal information, patient information or client data to anyone, for money or for anything else of value. We do not disclose client or patient data for third-party advertising or unrelated commercial purposes, and we have no business model based on doing so.

We share information only when it is authorized and reasonably necessary: **to provide contracted services**, with the authorized recipients a client has designated; **with service providers** such as hosting, security, communications and technology vendors who work under contractual confidentiality and security obligations, and under a Business Associate Agreement where they may access protected health information; **at a client's documented direction**; **to comply with law**, valid legal process or a lawful order, limiting the disclosure to what is required and notifying the affected client where permitted; **to protect security and rights**, including investigating incidents or preventing unlawful activity; and **in a corporate transaction** such as a merger, acquisition or sale of assets, in which case the information remains subject to this policy and the governing agreements.

Service providers receive no independent right to use client or patient information for their own purposes. Messages sent through the contact form on this website are relayed to us by Web3Forms, a form delivery service that processes the business contact details you enter for the sole purpose of delivering them to Excalibur; do not include patient information in the form.

ASKMERLIN PLATFORM PROTECTIONS

AskMerlin is delivered as part of Merlin as a Service and is governed by the client agreement in place. Access to every application is assigned by role, legitimate business need and client authorization. Each client's data is segregated; access to one client's information never implies access to another's.

Users may not share credentials, circumvent controls, export data to unapproved systems, or use platform data for personal or unrelated purposes. Data extraction, transformation, loading and reporting are limited to authorized sources and permitted purposes, and client data is not combined across clients in any way that would breach permissions or law.

Artificial intelligence. Identifiable client data and protected health information are not used to develop, train or improve generalized artificial intelligence or machine learning models for independent commercial purposes. Any analytics, automation or AI capability inside AskMerlin operates only on the data, and for the purposes, the governing agreement allows.

Aggregated and de-identified data. Where law and the client agreement permit, we may use aggregated statistics or properly de-identified information for benchmarking, service evaluation and improvement. Removing names alone does not make information de-identified; we apply the standards applicable to the data concerned, and we do not re-identify information where that is prohibited.

Client or patient information is not used in training materials, demonstrations or test environments without authorization and safeguards; synthetic or de-identified data is used wherever practical.

HOW WE PROTECT INFORMATION

We maintain administrative, technical and physical safeguards appropriate to the sensitivity of the information, including role-based access and authentication, user provisioning and periodic permission review, encryption in transit and at rest where appropriate, security monitoring, logging and incident investigation, workforce confidentiality obligations and training, vendor oversight, backup and recovery, and policies for remote work and approved devices.

No system can be guaranteed to be completely secure. We commit to reasonable safeguards and to the obligations in our agreements and under law, and we ask you to protect your own credentials and to report anything that looks wrong.

HOW LONG WE KEEP INFORMATION

We keep information for as long as reasonably necessary to fulfill the purpose it was collected for, to provide contracted services, to meet legal, regulatory and audit obligations, to maintain required business records, and to resolve disputes and enforce agreements. For client information, retention, return and destruction follow the client agreement, the Business Associate Agreement and the client's documented instructions.

As a guide: website contact submissions are kept while we are in conversation with you and for a reasonable period afterward, or until you ask us to delete them; server logs are kept for a limited period under our host's retention schedule; engagement records are typically kept for the engagement plus seven years. When information is no longer needed and may lawfully be disposed of, we delete, destroy or return it. Closing an account does not always mean immediate deletion; some records must be retained, and copies may remain in protected backups until they are securely cycled out.

COOKIES, ANALYTICS AND TECHNICAL TRACKING

This website uses only what it needs to work. Your Day, Night or Night Sky theme choice is stored in your own browser (local storage) and never leaves it. We set no advertising cookies and no cross-site tracking.

We may use Google Analytics, loaded through Google Tag Manager, to understand which pages are read and how visitors arrive. Where enabled, it is configured without advertising features. You can opt out with Google's browser add-on or by blocking cookies in your browser; the site will still work. Fonts are served from Google Fonts, which receives a standard font request from your browser.

AskMerlin and the client portal use cookies and similar technologies strictly for authentication, session management, security and preferences.

Links to LinkedIn, Facebook, Indeed and other third-party sites, and any content embedded from them, are governed by those companies' privacy policies, not this one.

YOUR CHOICES AND RIGHTS

Depending on where you live, you may have the right to know what personal information we hold about you, to access it, to correct it, to delete it, to restrict or object to certain uses, to receive a copy in a portable format, and to be free from discrimination for exercising those rights. Residents of states with comprehensive privacy laws (including Colorado, California, Virginia, Connecticut, Utah, Texas, Oregon and others) may exercise those rights by contacting us. We will verify your identity, respond within the time the applicable law allows, and explain any exception that applies.

Marketing. Use the unsubscribe link in any marketing email, or contact us, to stop receiving marketing. We will still send service and account communications you need.

Text messages. If you give us a mobile number and agree to receive text messages, we will text you only about the matter you asked about. Message and data rates may apply. Reply STOP to stop and HELP for help. Your consent to texting is never shared with third parties for their marketing.

Patient records. Where we process information on behalf of a healthcare provider, that provider decides on and responds to patient requests. We will assist them as the agreement and law require. Patients seeking access to or correction of their records should contact their provider.

Do Not Track and opt-out preference signals. Because we do not sell or share personal information for cross-context advertising, there is nothing for such signals to switch off; we honor them where the law requires.

HOW TO MAKE A PRIVACY REQUEST

Use any of the contact routes at the end of this page. Tell us who you are, how to reach you, and what you want us to do (access, correct, delete, restrict, port, opt out of marketing, or stop a channel of contact). You may use an authorized agent; we will ask for proof of their authority.

Verification. We confirm you are who you say you are before acting, usually by matching the details you give us against what we hold, and sometimes by asking for one more piece of information. We never ask for a full Social Security number, a card number or a password to verify a request.

Timing. We acknowledge requests within 10 business days and respond within 45 days, extending once by a further 45 days where a request is complex and telling you why. There is no charge for a first request in any twelve-month period.

If we decline. Some requests cannot be honored in full: records we must keep under HIPAA, tax, employment or contract law; information that belongs to a client provider; or requests we cannot verify. We will explain the reason and, where state law gives you the right, how to appeal our decision. If you are unsatisfied with an appeal you may contact your state Attorney General.

Patients. Requests about medical or billing records go to the provider that treated you; we forward any we receive within 5 business days and tell you we have done so.

SECURITY INCIDENTS

Suspected loss, unauthorized access, misuse or disclosure of information can be reported at any time through the contact details below. We assess every report, contain and investigate, preserve evidence, correct the cause, and provide the notices that law and our agreements require, to clients, individuals and regulators, within the required timeframes.

CHANGES TO THIS POLICY

We revise this policy as our services, platforms and legal obligations evolve. Each version carries its effective and last-updated dates at the top of this page. Where law or an agreement requires it, we will give notice of material changes. No revision of this policy can authorize a use or disclosure of protected health information that a Business Associate Agreement or the law prohibits.

VERSION HISTORY

- October 24, 2026** Added the policy-at-a-glance table, the patient communications and collections section, the privacy request process, the Web3Forms disclosure, and the covered domains excaliburrcm.com and excaliburrcm.health. Printable version published.
- October 16, 2026** First publication on the website, replacing the internal Privacy Policy and Data Protection document.

HOW TO REACH US ABOUT PRIVACY

Questions, requests to access, correct or delete your information, marketing opt-outs and reports of suspected incidents all come to the same place. Please do not include patient information in your message.

EMAIL

info@excalibur-ddpm.com

Subject: Privacy

PHONE

877-505-1454

Monday to Friday, Mountain Time

MAIL

Excalibur Data Driven Performance Management

Attn: Privacy

417 Monument Road, Unit 2

Grand Junction, CO 81507

Clients with questions about a Business Associate Agreement or AskMerlin data handling should contact their engagement lead or the Chief Revenue Cycle Officer.