Adverse Event AI Privacy Policy (Updated May 2026)

This Privacy Policy outlines the types of information we collect from website visitors, clients, and other third parties through www.adverseevent.ai (the "Site"), a web-based platform offered by EXPERT GRAPH LLC ("EXPERT GRAPH," "we," "us," or "our") that helps users analyze FDA adverse event data and prepare draft FDA Form 3500A documents and ICH E2B(R3) XML files (the "Services").

In this Policy we set out how we collect and use personal information gathered through the Site, with whom we might share it, the means by which we keep it secure, and the choices you ("You") have about the information You choose to share with us.

If You have any questions about the privacy practices of Adverse Event AI or our Privacy Policy, please send an email to team@adverseevent.ai.

Scope of this Privacy Policy

This Privacy Policy applies to personal information we collect through the Site and Services. This Privacy Policy does **not** apply to: (a) information about patients or other third parties that You or Subscriber upload, paste, type, or otherwise input into the Services as part of preparing a Form 3500A document, an E2B(R3) XML file, or any other adverse event report ("User-Provided Case Data"); (b) information You receive from us as part of any Generated Output. Our handling of User-Provided Case Data is governed instead by the Adverse Event AI User Agreement, the applicable Subscription Agreement, and, where one is in place, the Business Associate Agreement between EXPERT GRAPH LLC and Subscriber. See the section below titled "How we handle User-Provided Case Data" for additional detail.

Personal information we collect and what we use it for

The types of personal information we collect depend on the purpose for which You provide it to us. We only collect what is necessary for the purposes set out below and we do **not** sell or rent Your personal information to any third parties, nor do we use Your personal information for targeted advertising by third parties.

a) Clients / authorized users

In Your capacity as an authorized user or contact for our products and services, we collect limited personal information about You, such as Your name, email address, employer/organization, professional role (for example, drug safety, pharmacovigilance, regulatory affairs, or quality assurance), and in some cases phone number, physical address, and other personal information You choose to enter in the profile section of the Site. We also collect Your IP address and a log of Your activity on the Site (described in the section below titled "Activity logs and public-data queries"). In those instances where You are paying for a subscription service, we collect billing contact information and payment details; payment card numbers are processed by a third-party payment processor and are not stored on our servers.

What we use it for. We use the personal information to administer and support the contracts and relationships we have with You and the authorized users of the Services, to provide updates about the Services, to deliver product and customer support, to manage billing and other client inquiries, to maintain security and detect misuse, to comply with our legal and regulatory obligations, and, where permitted, to send You information about other products and services that may be of interest to You.

b) Website visitors

If You are accessing the Site to learn more about Adverse Event AI and our products and services, to inquire about employment with EXPERT GRAPH LLC, or for any similar purpose, the information we collect may include name, IP address, physical and email addresses, phone number(s), and information about Your professional role, submitted via an online registration or request form, as well as usage information about Your interaction with the Site and any newsletters or other communications You agree to receive following Your visit to the Site.

If You are an EU, UK, or other jurisdiction's data subject whose local law requires consent, our Site provides You the opportunity to consent to our use of Your personal information prior to submitting any personal information; Adverse Event AI will only use Your personal information if You consent to such use or if we have another lawful basis to do so.

What we use it for. We use the personal information (and any preferences indicated by You, where appropriate) to send You the information You have requested, to respond to Your inquiries, to provide information about the Services, and to operate, secure, and improve the Site.

c) Adverse Event AI suppliers and service providers

We collect limited personal information, such as name, email, and in some cases Your IP address, phone number, and postal business address from You as the contact for the supplier or service provider of the business products and services being provided to Adverse Event AI.

What we use it for. We use the personal information to administer and support the contracts we have with You or Your employer. We also use this information to contact You for purposes of dealing with support, billing, and inquiries about Your products and services.

d) Candidates

If You are accessing the Site to inquire about employment with EXPERT GRAPH LLC, the information we gather may include, but is not limited to: Your name, physical and email addresses, phone number(s), and if You are submitting an employment application and related information through the Site, Your username/password and any additional employment-related information that You choose to provide.

What we use it for. We use this information to process and manage Your application for employment with EXPERT GRAPH LLC.

How we handle User-Provided Case Data (adverse event content)

Adverse event reports, by their nature, may contain limited information about identifiable patients, healthcare providers, and products. When You or Subscriber upload, paste, type, or otherwise provide content to the Services in order to analyze it or to prepare a Form 3500A document, an E2B(R3) XML file, or any other Generated Output, that content is "User-Provided Case Data." User-Provided Case Data may include, depending on what You choose to provide: patient initials, age, sex, weight, and other demographic information; case narratives describing the adverse event; medical history and concomitant medications; suspect product information; reporter and healthcare-provider contact information; and other information required by FDA Form 3500A or the ICH E2B(R3) data elements.

No server-side storage of User-Provided Case Data. The Services are designed to process User-Provided Case Data in memory only during Your active session. We do not persist User-Provided Case Data, draft Form 3500A documents, or draft E2B(R3) XML files to our databases or long-term storage after Your session ends. Generated Outputs are produced on the fly and

delivered to You for download; they are not stored on our servers. If our application crashes during a session, User-Provided Case Data held in memory at that time is discarded, not written to disk.

You control Your working data. To support iterative work (for example, returning the next day to refine a draft), the Services allow You to save Your working state as a JSON file to Your own computer and to upload that file in a future session to resume where You left off. That JSON file is stored on Your device, not on our servers. You are solely responsible for keeping that file secure, controlling who has access to it, and backing it up. Because we do not retain a copy, we cannot recover Your working data for You if Your local file is lost, corrupted, or deleted.

AI processing. Where the Services use third-party artificial intelligence or large language model APIs to analyze case data, we configure those APIs so that Your User-Provided Case Data is not retained by the provider beyond the time needed to return a result and is not used by the provider to train its models. We rely on the provider's contractual commitments to that effect.

Limited operational exceptions. Even with this design, certain transient processing is unavoidable for any web service: User-Provided Case Data is necessarily present in memory and in network traffic while we are processing it; it may appear briefly in error diagnostics if something goes wrong during processing; and our infrastructure providers (such as Amazon Web Services and Google Cloud) may retain network-level metadata in accordance with their own policies. We configure our logging to avoid capturing User-Provided Case Data content where reasonably feasible, and we require our subprocessors to use any data they handle solely to provide infrastructure to us.

Our handling of User-Provided Case Data is also governed by the following commitments:

- Purpose limitation. We use User-Provided Case Data only to (a) provide the Services to You and Subscriber, including running analyses You request and preparing Generated Outputs at Your direction; (b) provide customer and technical support to the extent You voluntarily share data with us as part of a support request; (c) maintain the security and integrity of the Services; and (d) comply with applicable law and lawful requests from regulators.
- No sale; no advertising. We do not sell User-Provided Case Data, and we do not use it for advertising of any kind.
- No filing on Your behalf. We do not submit, transmit, file, or deliver Generated Outputs (or any User-Provided Case Data contained in them) to FDA, to the FDA Safety Reporting Portal, to the FDA Electronic Submissions Gateway, or to any other regulatory authority on Your behalf. You and Subscriber remain solely responsible for any submission to FDA or other regulators.
- No model training on Your data. We do not use User-Provided Case Data to train any artificial intelligence or machine learning model, whether our own or a third party's.
- Your responsibility. You and Subscriber are responsible for ensuring that You have all rights, consents, and authorizations necessary to provide User-Provided Case Data to us and to permit our use of it as described in this Privacy Policy and the User Agreement; for de-identifying or pseudonymizing User-Provided Case Data to the maximum extent consistent with Your regulatory reporting needs before submitting it to the Services; and for the security of any JSON working files You save to Your own device.

Activity logs and public-data queries

Although we do not store the contents of User-Provided Case Data or the contents of Generated Outputs, we do maintain two categories of records that are tied to Your account: activity logs and public-data queries. We disclose them separately here so You understand exactly what we retain.

Activity logs. We maintain logs of activity on the Site that record, for each action You take, information such as: Your account identifier, the date and time of the action, Your IP address, the type of action performed (for example, "uploaded a working file," "generated a draft Form 3500A," "downloaded an E2B(R3) XML file," "signed in," "changed account settings"), and basic metadata about the action (such as file size or whether the action succeeded). Activity logs do not contain the substantive content of User-Provided Case Data, the substantive content of Generated Outputs, or the substantive content of public-data queries. We use activity logs to (a) operate, secure, and troubleshoot the Services; (b) detect and investigate misuse, abuse, and unauthorized access; (c) provide an audit trail that You or Subscriber may use to demonstrate use of the Services for Your own internal compliance, quality, or audit purposes; and (d) comply with applicable law and respond to lawful requests from regulators. We retain activity logs for up to twelve (12) months, after which they are deleted, except where a longer retention period is required by law or where the records are subject to a legal hold.

Public-data queries. The Services allow You to search and analyze adverse event data that is publicly available from sources such as FAERS, MAUDE, and VAERS. When You run such a search or analysis, we record the query You submitted (for example, the product name, time range, event terms, or other parameters You entered) together with the metadata described above (account identifier, date and time, IP address). We retain public-data queries only because they are queries against public data; they do not contain User-Provided Case Data. The results returned to You by a public-data query are generated on the fly from the public data sources and are not stored on our servers after Your session ends. We use public-data queries only to (a) provide the Services to You; (b) operate, secure, and troubleshoot the Services; (c) detect and investigate misuse and abuse; and (d) comply with applicable law and respond to lawful requests from regulators. We do not analyze public-data queries to improve our products or features, do not sell public-data queries, do not share them with advertisers, do not publish "top searches" or similar content derived from individual users' queries, and do not use public-data queries to train artificial intelligence or machine learning models for any party. We retain public-data queries for up to twelve (12) months, after which they are deleted, except where a longer retention period is required by law or where the records are subject to a legal hold.

Confidentiality of queries. We recognize that public-data queries may themselves be commercially sensitive (for example, the fact that a particular user is researching a particular product may be of interest to competitors). We treat queries associated with identified accounts as Confidential Information of the relevant Subscriber and limit internal access to authorized personnel with a legitimate need to access them.

HIPAA and protected health information

The Services are not designed, intended, or marketed to receive, store, or process Protected Health Information ("PHI") as that term is defined under the U.S. Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), and its implementing regulations. EXPERT GRAPH LLC is not a "covered entity" under HIPAA. EXPERT GRAPH LLC does not act as a "business associate" of any covered entity unless EXPERT GRAPH LLC and Subscriber have entered into a written Business Associate Agreement covering specified Services and specified data. If You or Subscriber is a covered entity or business associate and intends to submit PHI to the Services, You must enter into a written Business Associate Agreement with EXPERT GRAPH LLC before doing so. In the absence of such an agreement, You should not submit PHI to the

Services; You and Subscriber are responsible for the consequences of any submission of PHI in breach of this Privacy Policy.

Links to other websites

Adverse Event AI may provide links to other websites from the Site, including links to FDA, government, and other third-party resources. We encourage You to read those websites' individual privacy policies before providing any of Your personal information to them. EXPERT GRAPH LLC is not responsible for those websites, their policies, or their practices.

Personal information: How long do we keep it

Adverse Event AI retains personal information only for as long as necessary for the uses we have set out above, plus any additional period required to comply with our tax, accounting, regulatory, legal, and recordkeeping obligations. Specific retention rules are as follows:

- **Account information** (name, email, employer, role, billing contacts) is retained for the duration of Your account and for a reasonable period thereafter to handle wind-down, billing reconciliation, and dispute resolution, after which it is deleted or de-identified.
- **User-Provided Case Data and Generated Outputs** are not retained on our servers after Your session ends, as described in the "How we handle User-Provided Case Data" section above.
- **Activity logs and public-data queries** are retained for up to twelve (12) months and then deleted, as described in the "Activity logs and public-data queries" section above.
- **Records required by law** (such as tax records, accounting records, and records subject to legal hold) are retained for the period required by applicable law, even if that period is longer than the periods above.

Individual jurisdictions have different retention requirements, and Adverse Event AI is bound to keep certain personal data in accordance with these local requirements.

Personal information: How we store and process it

All personal information we gather from You may be processed and stored in any one of our company locations and may subsequently be transferred to other countries for further processing, storage, and/or use by either Adverse Event AI or third parties acting on Adverse Event AI's behalf. Our staff who need to access personal information to perform their roles will have access to it and have agreed to comply with Adverse Event AI's policies on data protection.

Adverse Event AI uses a small number of third parties to provide services on its behalf. These services may include, but are not limited to, hosting websites, providing customer support, processing transactions, performing statistical analysis of our services, and providing systems and software for administrative functions such as billing, accounting, and procurement. In such cases, Adverse Event AI remains controller of the personal data, the third parties only process the data in accordance with our instructions, and we are responsible for ensuring such third parties are compliant with all applicable data protection regulations in relation to their processing activities.

Adverse Event AI utilizes servers from Google Cloud and Amazon Web Services (AWS) to host our platform and store our data, each of which maintains industry-standard certifications (including ISO 27001). Adverse Event AI's data servers currently reside within the United States, and by

using our platform You understand and agree that Your personal information may be stored on Google Cloud and/or AWS servers located in the United States. More information about AWS's compliance can be found at https://aws.amazon.com/compliance/ and more information about Google Cloud's compliance can be found at https://cloud.google.com/security/compliance/.

International transfers

If You are accessing the Services from outside the United States, You acknowledge that Your personal information and any User-Provided Case Data You submit may be transferred to, processed in, and stored in the United States, which may have data protection laws that differ from those of Your country. Where required, we rely on appropriate safeguards (such as standard contractual clauses) to provide adequate protection for personal information transferred internationally.

Protection of Your personal information

We have technical, security, and organizational measures in place (and require our service providers to do so as well) reasonably designed to protect against unauthorized access to, or unauthorized alteration, disclosure, or destruction of, personal information and User-Provided Case Data. The measures we use are appropriate to the nature, scope, and purpose for which we use the data we collect, and include access controls, encryption in transit and at rest where appropriate, internal reviews of our data collection, storage, and processing practices, and physical security measures to guard against unauthorized access to systems where we store data. We maintain processes designed to enable us to respond to data subject requests as required under applicable law, to address complaints, and to comply with breach reporting procedures and incident management plans.

Adverse Event AI operates secure data networks protected by industry-standard firewall and password protection systems. Our security and privacy policies are periodically reviewed and enhanced as necessary, and only authorized individuals have access to the information provided.

Further information on our security and incident management is available from team@adverseevent.ai.

Use of cookies on the Site and in our products and services

We use cookies and similar technologies to set user preferences, keep You signed in, maintain session state, secure the Site, and improve the quality of Site navigation and the products and services we offer through it. We may also use analytics cookies to understand how the Site is used in aggregate. Where required by law, we obtain Your consent before placing non-essential cookies. You can control cookies through Your browser settings.

How to update Your personal information or make a data subject request

Clients / Suppliers. If You need to update Your personal information or make a Data Subject Request (as described below), please email us at team@adverseevent.ai and Your email will be directed to the correct EXPERT GRAPH LLC team to take action with respect to Your request.

Website visitors. If You need to update Your preferences or personal information or make a Data Subject Request, please email us at team@adverseevent.ai or follow the instructions contained in any email we have sent to You to unsubscribe or change Your preferences.

Candidates. Data Subject Requests or questions related to Your personal information submitted in connection with employment inquiries or job applications should be sent to

team@adverseevent.ai and Your email will be directed to the correct EXPERT GRAPH LLC team to take action with respect to Your request.

User-Provided Case Data. Requests to access, correct, or delete User-Provided Case Data should generally be directed to Subscriber, which controls the User-Provided Case Data uploaded to its account. We will reasonably cooperate with Subscriber to fulfill such requests. If You believe Your information has been submitted to the Services by a Subscriber and You wish to exercise rights with respect to that information, You may contact us at team@adverseevent.ai and we will refer Your request to the relevant Subscriber.

What about children's privacy?

The Site and Services are intended for use by professionals in drug safety, pharmacovigilance, regulatory affairs, and related fields, and are not directed to children. Adverse Event AI does not knowingly collect personal information from children under the age of 16. If You believe a child has provided us with personal information, please contact us at team@adverseevent.ai and we will take appropriate steps to delete the information.

What is a Data Subject Request?

Some local regulations grant individuals in those localities certain rights in respect of the personal data held by companies, including but not limited to rights of access, correction, deletion, portability, and objection to processing under laws such as the EU General Data Protection Regulation, the UK General Data Protection Regulation, the California Consumer Privacy Act (as amended by the California Privacy Rights Act), and comparable U.S. state laws. Data Subject Requests are inquiries seeking to exercise these types of rights.

Your consent

If You are submitting personal information from a U.S. IP address, You consent to the collection and use of any personal information and any related information in the manner described in this Privacy Policy. If You are an EU, UK, or other jurisdiction's data subject and we do not already have the right to use Your personal information – for example, to perform under a contract with You – our Site provides You the opportunity to consent to our use prior to submitting it. Adverse Event AI will only use Your personal information if it is authorized to do so, and that use will be consistent with this Privacy Policy.

Changes to the Privacy Policy

EXPERT GRAPH LLC reserves the right to change this Privacy Policy at any time by posting a new Privacy Policy on the Site. Where the change is material, we will provide additional notice as required by law. We encourage You to review our Privacy Policy on a regular basis so that You will be aware of any changes to it.

Contact us

Adverse Event AI is offered by EXPERT GRAPH LLC. If You have any questions about this Privacy Policy or our privacy practices, please contact us by email at team@adverseevent.ai.