



Privacy, Consent, and Data Security:

What Everyone Should Know Before Providing Sensitive Information in AI Tools

This article was written by SNA member [Jennifer Marie McInerney](#) of the [McInerney Law Firm](#) in Vestavia, Alabama. The firm's primary practice areas include special needs planning, wills and trusts, estate administration, trust administration, guardianships, and conservatorships.

If you're caring for a family member with a disability, or navigating Medicaid, Supplemental Security Income (SSI), an Individualized Education Program (IEP), or a complex estate, you've probably turned to a search engine - or, increasingly, an AI chatbot - at some point during a stressful evening to ask, "What does this mean?" or "What should I do next?"

That instinct is logical. These tools are fast, available at our fingertips, and don't make you feel rushed the way a phone call sometimes does. But there's a tradeoff most of us never stop to think about: the moment you type your child's diagnosis, your bank account balance, your Social Security number, or the details of a benefits application into an AI tool, that information has left your hands, and where it goes next depends entirely on which tool you used and how it was built.

This is not a reason to avoid these tools. It is a reason to think about privacy, consent, and data security more deliberately, especially when the information involves a family member who can't advocate for their own privacy.

Why Is This Category of Information Different?

Most individuals have an intuitive sense that they should not email their credit card number to a stranger. But that instinct gets blurred with AI tools, partly since the conversation feels private, like a journal or a conversation with a knowledgeable friend. Despite how it feels, the reality is that it is not quite either of those things.

There are several categories of information and corresponding questions that arise regularly in special needs and elder law planning, and each carries its own kind of exposure when typing them into an AI tool:

- **Medical and diagnostic information.** A diagnosis, a medication list, a level of functioning, and/or an IQ score. These are the kinds of details that when combined with a name, can be sensitive enough to affect employment, insurance, or simply an individual's privacy if it were exposed online.
- **Financial details.** Account numbers, balances, Social Security numbers, details about an inheritance or a trust. These are the types of information identity thieves want most and are exactly the information individuals often disclose by asking for an AI tool to help figure out a Medicaid spend-down.

- **Benefits and eligibility information.** SSI and Medicaid details, case numbers, and household income. This information is protected under specific federal and state privacy rules while they are within a government agency's systems, but those protections don't automatically follow once an individual re-types the information into a web-based tool.
- **Educational records.** IEPs, evaluations, and school placement details. These kinds of information are protected when schools manage, store, and handle them, since schools are bound by the Federal Educational Rights and Privacy Act (FERPA). However, an AI chatbot is not a school, and FERPA doesn't extend to what individuals discuss within these tools.
- **Disability-related details about a specific person.** This is perhaps the most important category, and it raises a consent issue, not just a privacy one. A parent typing out a detailed description of a child's diagnosis, behavior, and daily needs is making a privacy decision on behalf of someone who has no say in it (much like parents posting their children's images and other personal information on social media). The same is true when an adult child types out detailed medical or cognitive information about an aging parent. The person whose information is being shared often cannot or does not consent and may never know the conversation or disclosure occurred.

None of this means a parent or caregiver did something wrong by asking an AI tool a question. It does mean the stakes for *how* you ask are much higher than they would be if you were asking about a recipe or a vacation itinerary.

The Consent Problem

Privacy law and professional ethics are generally built around the idea that an individual controls their own sensitive information, or that someone with legal authority (a guardian, a healthcare power of attorney, a parent of a minor) makes that decision on their behalf deliberately and with accountability. AI chatbots sit outside that framework entirely.

When an individual types details about a loved one's disability, diagnosis, or finances into a free AI tool, there's no formal consent process, no audit trail of who agreed to what, and often no real understanding of where that information might end up. This is a meaningfully different situation than, for example, sharing the same information with a doctor's office or a special needs attorney, both of which operate under defined confidentiality obligations and accountability structures if something goes wrong. An AI chatbot generally has neither.

What Actually Happens to What You Input

Here is the part that catches most people by surprise: with many free, consumer-facing AI tools conversations may be stored, reviewed, and in some cases used to improve or train future versions of the underlying AI model. This is true unless an individual has specifically opted out *and* only where the tool offers that choice at all. Retention periods, who can access stored conversations, and whether data is used for training all vary significantly from one tool to the next, and the answer for any specific product can change without notice as a platform updates its policies.

A few things are true across most of these tools. Broadly speaking – there is usually no confidentiality protection equivalent to attorney-client privilege or HIPAA. Talking to an AI chatbot about a child's diagnosis is not the same, legally, as talking to their doctor or attorney.

Nothing about the conversation is automatically privileged or protected just because the subject matter is sensitive.

Free tools tend to have fewer privacy controls than paid or business-tier products. Many AI companies offer business or enterprise versions of their tools with stronger data agreements, specifically because organizations handling sensitive client data, including law firms, need those protections. The free version most families use by default usually is not built with the same guarantees.

Once typed, a person has generally lost control over deletion. Most tools allow a conversation to be deleted from the user's own view, but whether that conversation has already been used, copied, or retained elsewhere by that point depends entirely on the company's specific practices and protocols.

Practical Habits That Lower the Risk Without Giving Up the Convenience

Families don't have to stop using these tools to get useful guidance. A few good habits now can go a long way towards protecting privacy and preserving meaningful consent over sensitive information:

- **Ask the general question, not the personal one.** "How does Alabama calculate the Medicaid look-back period?" This gets the same useful answer as describing a parent's full financial history, without putting account numbers or a Social Security number into a chat box. Save the specific numbers for a phone call or secure document upload with an actual attorney or financial advisor.
- **Strip identifying details before pasting anything.** When working through a letter, a benefits appeal, or a family situation, swap in a placeholder name, round the numbers, and remove account or case numbers before uploading it to an AI chatbot. The underlying question and the help received in response usually does not depend on the real name being there.
- **Be especially cautious with information about a child or an adult who can't consent.** A spouse typing out their own medical history is one thing. A parent typing out a detailed profile of a child's disability, behavior, and daily needs, or an adult child describing an aging parent's cognitive decline, is a decision being made for someone else. It is worth pausing on that information specifically, since the person most affected by the disclosure has no opportunity to weigh in.
- **Check whether the tool offers a privacy or "don't train on my data" setting and use it.** Many tools now offer this as a toggle in account settings. It is not a perfect guarantee, but it is a meaningfully different posture than leaving the default setting in place.
- **Treat anything involving account numbers, Social Security numbers, or login credentials as off-limits entirely.** There is no version of "help me organize my finances" that requires typing in a full account number. If a tool seems to need that information, it doesn't; there is almost always a way to ask the question without it.
- **When the matter is consequential, bring it to a professional instead of a chat window.** Researching general background on special needs trusts, ABLE accounts, or Medicaid rules is a reasonable use of an AI tool. Submitting specific financial details, a child's full diagnostic history, or the actual language of a legal document is a different

category of task, one where a secure client portal, an encrypted document upload, or a phone call serves a family better than a chat box.

The Bigger Picture

None of these is a reason for families to avoid getting fast, accessible answers when they need them. These tools genuinely help people understand confusing systems faster than they could otherwise. The goal is not caution for its own sake; it is making sure the convenience does not come at the cost of exposing the individuals least able to protect themselves: a child with a disability, an aging parent, a family member who never agreed to have their medical history typed into a chat window.

A simple rule of thumb covers most of it: if you would not want that exact sentence, name, diagnosis, account number and all, forwarded to a stranger, do not type it into a free AI tool either. Ask the general question there, and save the specific, sensitive, and consent-sensitive details for the people who are bound to protect them.

About This Article

We hope you find this article informative, but it is not legal advice. You should consult your own attorney, who can review your specific situation and account for variations in state law and local practices. Laws and regulations are constantly changing, so the longer it has been since an article was written, the greater the likelihood that the article might be out of date. SNA members focus on this complex, evolving area of law. To locate a member in your state, visit [Find an Attorney](#).

Sharing Guidelines

The Special Needs Alliance encourages sharing this article in its entirety with proper attribution to the SNA. When possible, please link to the original article on the Special Needs Alliance website. If republishing or distributing this content, please keep the article unaltered and include the author's byline and this notice.

When **referencing this content**, please use the following credit line:

"Source: Special Needs Alliance – www.specialneedsalliance.org"