Meeting Notes Pro
by Northern Catalyst

Privacy & Security Guide

How We Protect Your Client Data

www.northerncatalyst.ca

The Promise We Make

Your clients' privacy is our priority.

This guide explains exactly how Meeting Notes Pro handles your data. In plain English, no technical jargon required.

When you use Meeting Notes Pro to process meeting transcripts:

- Your clients' personal information is removed on your computer before anything is transmitted
- Only sanitized text travels to the cloud for AI processing
- No client data is stored on external servers

What Happens When You Upload a Transcript

Step 1: The transcript stays on your computer

When you upload a meeting transcript (whether it's a Word document, PDF, or text file), it's read directly by the app on your computer. Nothing is sent anywhere yet.

Step 2: We find and protect personal information, right on your device

Meeting Notes Pro scans your transcript using an AI that runs entirely on your computer (no internet needed). It looks for things like:

- Names
- Email addresses
- Phone numbers
- Social Insurance Numbers
- Account numbers
- Addresses

How Your Data Stays Protected

Step 3: Personal details are replaced with placeholder codes

Before anything leaves your computer, we swap out personal information with simple placeholders:

Original Transcript	What gets sent to the cloud
Sarah Johnson	[NAME_001]
sarah.j@email.com	[EMAIL_001]
(416) 555-0123	[PHONE_001]

The real information? It's encrypted and stored safely on your computer using bank-grade encryption - the same standard trusted by financial institutions.

Step 4: You review and approve

You always see exactly what will be sent before it goes anywhere. The text will look something like:

"Meeting with [NAME_001] on December 5th. Client interested in RRSP options. Follow up at [EMAIL_001]."

If something looks off, you can stop right there.

Step 5: Only the sanitized text travels to the cloud

After you approve, the placeholder text (not your clients' real information) is sent for AI processing via AWS Bedrock. The AI reads text like "[NAME_001] wants retirement advice". It has no idea who [NAME_001] actually is, because that information never left your computer.

Step 6: You get your polished notes back

The AI returns professional meeting notes using the same placeholders. Then, right on your computer, we swap the placeholders back to the real names. The final document is created locally.

Where Does Everything Happen?

What	Where
Reading your transcript	Your computer
Finding personal information	Your computer
Removing and replacing PII	Your computer
Storing the real names (encrypted)	Your computer
Your approval	Your computer
AI processing	AWS Bedrock (via encrypted private network)
Creating final documents	Your computer

How We Handle AI Processing

Meeting Notes Pro uses AWS Bedrock to access Claude, an AI assistant made by Anthropic.

Here's what you should know:

Your data travels securely

- All transmission uses TLS 1.3 encryption over AWS's private network
- AWS Bedrock has no data retention. Prompts and responses are not stored
- The AI only ever sees sanitized text with placeholder codes, never real client information

Why this matters

Even though AI processing happens in the cloud, your clients' personal information was already removed on your computer. The AI processes text like "[NAME_001] discussed retirement planning"—it cannot identify any real person because the mapping between [NAME_001] and an actual name exists only on your local machine.

Our Infrastructure

Meeting Notes Pro is built on Amazon Web Services (AWS). Here's how that benefits you:

AWS's security credentials

Our infrastructure is built on AWS, which maintains ISO 27001, SOC 2, and has been assessed by the Canadian Centre for Cyber Security (CCCS).

Data at rest stays in Canada

All stored data - including logs and configurations on AWS - remains in the Canada (Montreal) region (ca-central-1).

No data retention on processing servers

AWS Bedrock does not store your prompts or responses. Each request is processed and immediately discarded.

Security At Every Step

On Your Computer

In Transit

When sanitized data travels to AWS:

- TLS 1.3 encryption protects everything in transit (same security as online banking)
- No personal information is included, only placeholder codes like [NAME_001]
- Data travels over AWS's private network, not the public internet

In the Cloud

- No client data is stored on external servers
- AWS Bedrock processes requests without retention
- Only sanitized, non-identifiable text is ever transmitted

You’re Always In Control

Before Processing

- You see exactly what will be sent to the cloud
- You must approve before anything leaves your computer
- You can cancel at any time

Your Data, Your Choice

- Delete individual client records whenever you want
- Clear your entire database from the Settings page
- Uninstall the app to remove all local data
- There's no client data stored in the cloud to worry about

Nothing Stored Externally

We don't keep copies of your transcripts or generated notes on external servers. Each AI request is processed and immediately forgotten. The only cloud record is your license information, stored in AWS Canada (Montreal).

Common Questions

"What if something gets missed?"

Our detection is highly accurate, but that's why you always review before anything is sent. If you spot something the system missed, simply don't proceed.

"What if my computer is stolen?"

Your data is encrypted. Without your Windows login, thieves can't read it. For extra protection, we recommend enabling Windows BitLocker and using a strong password.

"What if AWS gets hacked?"

Attackers would only find meaningless text like "[NAME_001] requested advice." The mapping that connects [NAME_001] to an actual person exists only on your computer and that data is encrypted.

"How long do you keep my information?"

On your computer: until you delete it.
In the cloud: we don't store your content. Each request is processed and discarded.
Your license details for Meeting Notes Pro are kept in AWS Canada (Montreal).

"Does my data leave Canada?"

Your clients' personal information never leaves your computer. It's removed locally before anything is transmitted. The sanitized text (containing only placeholders) is processed via AWS Bedrock, which may route through AWS's global network for AI computation.

However, no data is stored outside Canada, and the transmitted data contains no identifiable information. The AWS architecture has been evaluated for use by federally regulated financial institutions.

For Your Records

If you need to document our security approach for compliance purposes:

Aspect	Detail
Privacy approach	PII removed locally before any transmission
Local encryption	Bank-grade encryption with extensive key derivation
Data at rest	Stored in Canada (AWS ca-central-1 Montreal)
Transit security	TLS 1.3 over AWS private network
AI provider	Claude (Anthropic) via AWS Bedrock
Data retention	None—AWS Bedrock does not store prompts or responses
AWS credentials	ISO 27001, SOC 2, assessed by CCCS (these are AWS certifications)

The Simple Summary

1. Personal information is removed on your computer: encrypted locally, never transmitted

2. Only placeholder codes go to the cloud: the AI never sees real names or details

3. No client data stored externally: AWS Bedrock processes without retention

4. You approve everything: nothing happens without your say-so

5. You control your data: delete anything, anytime

Questions?

We're here to help. Reach out anytime:

Email: support@northerncatalyst.ca

Website: northerncatalyst.ca

This document is provided for informational purposes. For specific compliance questions, please consult with your compliance officer or legal advisor.