

AI Voice Agent Security and Compliance Checklist

Before an AI voice agent takes real calls, check five areas: HIPAA and a BAA for health data, a SOC 2 report, a GDPR processing agreement, PCI DSS for card payments, and call recording and robocall consent rules, including the FCC's 2024 ruling on AI voices.

Updated October 29, 2026

An AI voice agent hears, records and stores what callers say. Callers often say private things. Use this checklist before the agent takes real calls. It is not legal advice. Ask your lawyer how each rule applies to you.

1. Health data: HIPAA and the BAA

Applies when: you are a US covered entity or business associate, and calls include protected health information (PHI).

- ☐ The vendor signs a business associate agreement (BAA) before any PHI reaches it.
- ☐ The BAA covers the vendor's subcontractors: model, speech and telephony providers.
- ☐ The BAA states how the vendor reports a breach.
- ☐ The BAA states that the vendor returns or destroys PHI at the end of the contract.

The rules for the contract are in 45 CFR 164.504(e). The contract must require the vendor to "use appropriate safeguards". It must require the vendor to report uses or disclosures that the contract does not allow, including breaches. It must also make subcontractors agree to the same restrictions.

Check the cost. On 2026-10-29, Vapi listed its HIPAA add-on at \$2,000 a month, with a BAA. Retell AI listed "HIPAA / BAA" and "Custom BAA" in its plan table. Ask which plan includes it.

2. Security controls: SOC 2

- ☐ The vendor gives you its current SOC 2 report under NDA.
- ☐ The report covers the systems that handle your calls.
- ☐ You read the exceptions and the controls the report expects you to run.
- ☐ You ask whether the report covers the vendor's sub-processors.

A SOC 2 report is an examination by a CPA firm. The AICPA describes it as covering controls relevant to security, availability, processing integrity, confidentiality or privacy. A badge on a website is not a report. Ask for the report.

3. Personal data: GDPR

Applies when: you process personal data of people in the EU, or you are established in the EU.

- ☐ You sign a data processing agreement under GDPR Article 28.
- ☐ The vendor processes call data only on your documented instructions.
- ☐ You approve sub-processors in writing, and the vendor tells you about changes.
- ☐ The vendor deletes or returns all personal data at the end of the service.
- ☐ You know where the data is stored and how it moves outside the EU.

Article 28 requires these terms. It also requires the processor to allow and contribute to audits.

4. Card payments: PCI DSS

Applies when: the agent hears, stores or sends card numbers.

- ☐ Decide whether the agent should take card numbers at all.
- ☐ If it does, ask the vendor for its PCI DSS attestation.
- ☐ Make sure recordings and transcripts do not store card numbers.
- ☐ Ask whether the vendor redacts card numbers from logs.

The PCI Security Standards Council says PCI DSS applies to "Entities that store, process, or transmit cardholder data". Retell AI, for example, lists a PII removal add-on at \$0.01 per minute. Ask what each vendor removes and where.

5. Call recording consent

- ☐ Tell callers that the call is recorded.
- ☐ Tell callers that they are speaking with an AI.
- ☐ Check the consent rules in every state or country you call.

US federal law (18 U.S.C. 2511(2)(d)) allows a recording when one party to the call consents. Some states and countries set stricter rules. Follow the strictest rule that applies to your callers.

6. Outbound calls: the TCPA and AI voices

Applies when: the agent makes calls to people in the US.

On February 2, 2024, the FCC adopted Declaratory Ruling FCC 24-17 (CG Docket No. 23-362). It was released on February 8, 2024. The FCC confirmed that the TCPA's restrictions on an "artificial or prerecorded voice" cover "current AI technologies that generate human voices". This includes voice cloning.

What the ruling says callers must do:

- ☐ Get the prior express consent of the called party, unless the call has an emergency purpose or an exemption applies.
- ☐ Identify the entity responsible for the call.
- ☐ For telemarketing or advertising, offer the opt-out methods the FCC rules require.
- ☐ Keep records of consent and opt-outs.

7. Data handling in the contract

- ☐ Retention period for recordings, transcripts and logs.

- ☐ A clear answer on whether your call data trains models.
- ☐ Encryption in transit and at rest.
- ☐ Single sign-on and role-based access for your team.
- ☐ Export and deletion at the end of the contract.

Vapi, for example, lists data retention of 14 days on its free tier, 30 days on Core and 180 days on Pro. Retention differs by vendor and plan. Ask.

Rules and prices change. Check the source and the vendor page before you rely on them.

Frequently asked questions

Do AI voices count as robocalls in the US?

Yes, under the TCPA. In Declaratory Ruling FCC 24-17, adopted on February 2, 2024, the FCC confirmed that the TCPA's rules on an artificial or prerecorded voice cover current AI technologies that generate human voices. Such calls need prior express consent unless an emergency purpose or exemption applies.

Does a vendor need to sign a BAA?

If the vendor creates, receives, keeps or sends protected health information for a US covered entity, HIPAA requires a business associate contract. The contract terms are in 45 CFR 164.504(e).

Is a SOC 2 report a certification?

No. It is a report by a CPA firm on a service organisation's controls. The AICPA describes SOC 2 as covering controls relevant to security, availability, processing integrity, confidentiality or privacy.

Is this checklist legal advice?

No. It lists the questions to ask. Ask your lawyer how each rule applies to your calls and your locations.

Sources

[FCC, Declaratory Ruling FCC 24-17, Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts, CG Docket No. 23-362 \(fetched 2026-10-29\)](https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf) — <https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf>

[eCFR, 45 CFR 164.504, Uses and disclosures: organizational requirements \(fetched 2026-10-29\)](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504) — <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504>

[GDPR Article 28, Processor \(gdpr-info.eu\) \(fetched 2026-10-29\)](https://gdpr-info.eu/art-28-gdpr/) — <https://gdpr-info.eu/art-28-gdpr/>

[PCI Security Standards Council, PCI DSS \(fetched 2026-10-29\)](https://www.pcisecuritystandards.org/standards/pci-dss/) — <https://www.pcisecuritystandards.org/standards/pci-dss/>

[AICPA and CIMA, SOC services for service organizations \(fetched 2026-10-29\)](https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2) — <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2>

[Cornell LII, 18 U.S. Code 2511, Interception and disclosure of wire, oral, or electronic communications \(fetched 2026-10-29\)](https://www.law.cornell.edu/uscode/text/18/2511) — <https://www.law.cornell.edu/uscode/text/18/2511>

[Vapi, Pricing \(fetched 2026-10-29\)](https://vapi.ai/pricing) — <https://vapi.ai/pricing>

[Retell AI, Pricing \(fetched 2026-10-29\)](https://www.retellai.com/pricing) — <https://www.retellai.com/pricing>