GUIDE · OCTOBER 2026

SB 1188 and offshore engineering: a vendor checklist for health tech leaders

What Texas SB 1188 means for offshore developers, test data and vendor contracts

Published by TAK Devs
Published October 27, 2026 · Last checked October 27, 2026

Contents

/01 What does an SB 1188 gap cost a health tech company?

/02 What does Texas SB 1188 require, and since when?

/03 Can offshore developers access Texas patient records?

/04 What should you ask a software vendor before they touch Texas patient data?

/05 How do you keep real patient data away from offshore engineers?

/06 What did TAK Devs build for UpliftCare, a HIPAA-aligned telehealth marketplace?

/07 Frequently asked questions

/08 How this paper was checked

/09 References

/00

Executive summary

THE SHORT ANSWER

Texas Senate Bill 1188 (SB 1188) requires covered entities to keep electronic health records physically in the United States or a U.S. territory from January 1, 2026, according to the Texas Legislature's enrolled text . Offshore read-only access is unsettled. The safest setup keeps production data in US regions and gives offshore engineers synthetic data only.

A clinic security review can end a pilot with one question: where does patient data live? Texas gave providers a legal reason to ask it.

This paper is for CEOs and COOs of US digital health companies that sell into Texas and build with offshore or distributed engineering teams. It covers the rules, the open questions, a seven-question vendor checklist and a development setup that keeps the question easy to answer.

TAK Devs serves US clients from Islamabad and the United States, so the offshore question is ours too. We wrote this paper to answer it plainly.

Three findings

01 From January 1, 2026, Texas requires covered entities to keep electronic health records physically in the United States or a U.S. territory, including records held by cloud and subcontracted providers, per the Texas Legislature's enrolled text[1].

02 Law firms split on offshore access. Goodwin[2] calls read-only access unclear, while McDonald Hopkins[3] reads access as permitted if nothing is stored, cached or copied abroad.

03 The cheapest control is architecture. Keep production data in US regions, give offshore engineers synthetic data, and make production access US-based, narrow and logged.

/01

What does an SB 1188 gap cost a health tech company?

A Texas clinic asks where your patient data lives. You answer with a region name and a diagram, or you answer with a pause. The pause ends pilots.

Texas SB 1188, the 2025 law on electronic health records (EHRs), gives clinics a legal reason to ask. It adds Chapter 183 to the Texas Health and Safety Code and makes each covered entity responsible for where its records are physically kept. Under Section 183.011 of the enrolled bill[1], the Texas Attorney General can seek injunctive relief and civil penalties capped by intent.

$5,000	$25,000	$250,000
cap per negligent violation	cap per knowing or intentional violation	cap per violation that knowingly or intentionally used protected health information for financial gain

The caps apply to violations that occur in a single year, however long a violation lasts within that year. Agencies can act too. A regulatory agency may discipline a covered entity that violates the chapter three or more times, up to license suspension or revocation, and must investigate any credible allegation (Sections 183.009 and 183.010[1]).

You may not be the covered entity. Your clinic customer probably is. But Goodwin[2] notes that the Texas definition reaches businesses that assemble, collect, analyze, use, evaluate, store or transmit protected health information (PHI), and can be read to reach entities outside Texas that process Texas patients' data. The storage rule also names third-party

and subcontracted computing facilities and cloud providers (Section 183.002(a)[1]). If you sit in a clinic's data chain, the clinic needs your answers to prove its own compliance.

The rule also looks backward. It applies to storage on or after January 1, 2026, regardless of the date a record was prepared (Section 2(b)[1]). Legacy records count.

Federal law will not rescue a thin questionnaire. Paubox[4], a healthcare email security vendor, notes that the Health Insurance Portability and Accountability Act (HIPAA) has no explicit restriction on offshore data storage. A review built only on HIPAA can miss the Texas question. A review that adds it will not.

The loss usually arrives as a failed review, not a fine. The sources we reviewed on October 27, 2026 did not include published Texas agency guidance or a reported enforcement action on SB 1188. That makes the clinic's lawyer, not the regulator, your first examiner.

A reviewer can reduce SB 1188 to four plain questions: which region holds the data, who has access, what leaves the region, and what engineers test with. The checklist below answers all four.

/02

What does Texas SB 1188 require, and since when?

Texas SB 1188 is a 2025 Texas law that adds Chapter 183 to the Texas Health and Safety Code and sets rules for electronic health records, including where they are kept. The law took effect on September 1, 2025. Its storage rule applies to storage on or after January 1, 2026 (Texas Legislature[1]).

Texas is not alone. Florida has had its own rule since July 1, 2023, according to McDermott Will & Emery[5]. Under Florida Statutes section 408.051[6], a provider that uses certified electronic health record technology must keep patient information stored offsite, including with a cloud vendor, in the continental United States, its territories or Canada. McDermott reads the statute as covering physical storage, not access, and notes that some commentators read it more broadly.

HHS now lists July 2027 for final action on its proposed update to the HIPAA Security Rule, Alston & Bird reports[7], after a May 2026 target passed. Treat that as a planning date. It can move.

TABLE 1. SB 1188 DUTIES THAT REACH VENDORS. SOURCE: TEXAS LEGISLATURE, ENROLLED TEXT, 2025.

Section	What the text requires	Why a vendor cares
183.002(a)	Covered entities must ensure EHRs under their control that contain patient information are physically maintained in the United States or a US territory. This includes records held by third-party or subcontracted computing facilities and cloud providers.	Your hosting, backups and subcontractors are in scope.
183.002(b)	EHR information of Texas residents is accessible only to people who need it for treatment, payment or health care operations within the scope of their employment.	An engineer needs a job reason to see a record.
183.002(c)	Covered entities must apply reasonable and appropriate administrative, physical and technical safeguards to EHR information.	Safeguards must be working controls.
183.009 to 183.011	Investigations, discipline after three or more violations, and Attorney General injunctions and civil penalties.	Your customer carries the penalty.

/03

Can offshore developers access Texas patient records?

Nobody can answer yes or no with authority today. The text of SB 1188 limits where records are stored and who may see them. It does not say whether a person outside the United States may view a record that sits on a US server.

The drafting history adds one clue. Katten Muchin Rosenman[8] reports that an earlier draft required Texas residents' records to be inaccessible to anyone outside the United States, and that the enacted version dropped that language. In its place, covered entities must keep records accessible only to people who need them for treatment, payment or health care operations, and must apply reasonable safeguards.

- McDonald Hopkins[3]: offshore storage is banned, but offshore access is still permitted with safeguards, as long as it leaves no stored, copied or cached data on non-US servers or devices.
- Goodwin[2]: unclear whether the US storage rule bars offshore processing through read-only access. Be ready to limit processing to the United States.
- Hall Render[9]: ambiguous whether the ban covers only storage or also offshore view-only access. Review remote access and business associate services.
- Katten: safeguards would likely need system-level limits on downloading or copying remotely accessed records.

We read the split as a risk map, not a permission slip. A clinic's lawyer will pick the cautious reading, because it is the cheaper one to defend. **Design so the honest answer to "can offshore engineers see production records?" is no.**

Two more questions stay open. First, the text does not mention de-identified data, so whether a de-identified or synthetic dataset counts as patient information is a question for counsel. Second, the law tells agencies to adopt implementing rules as necessary (Section 183.012[1]), and the sources we reviewed on October 27, 2026 did not include any. Watch for them.

/04

What should you ask a software vendor before they touch Texas patient data?

Put these seven questions to every development vendor, including your own team. Ask them in order. A vague answer to question one is a finding.

SEVEN QUESTIONS FOR A VENDOR THAT MAY TOUCH TEXAS PATIENT DATA

- [x] **Where is production data hosted, by region?**
  Get the cloud provider, the region name and the account layout in writing. The Texas rule reaches third-party and subcontracted computing facilities and cloud providers, so the vendor's hosting is in scope (Section 183.002(a)[1]). A good answer names a US region and shows a diagram. A weak one says "the cloud" or "we will check". Ask for the answer in a document your lawyer can read.

- [x] **Who can access it, and from where?**
  Ask for the roles that can reach production, the country each person works from, and the reason each role needs access. The law limits record access to people who need it for treatment, payment or health care operations within the scope of their employment (Section 183.002(b)[1]). Engineers building features rarely meet that test. A good answer is a short list with named approvers.

- [ ] **Is anything cached or logged outside the US, including backups and error trackers?**

  Records leave through side doors. McDonald Hopkins[3] warns that access must not result in storage, copying or caching on non-US servers or devices. Ask about backups, replicas, disaster recovery, log pipelines, error trackers, analytics tools, support tickets and engineers' laptops. Each needs a region and an owner. A good answer includes a scrubbing rule for logs.

- [ ] **What data do engineers test with?**

  This question decides most of the others. If engineers test with copies of real records, real records live in development, on laptops and in screenshots. Ask for the source of every test dataset. The best answer is synthetic data generated without copying real patients. A masked production copy needs scrutiny: HHS[10] says even properly de-identified data keeps a small but non-zero risk of identification.

- [ ] **How are access logs produced for a review?**

  A clinic will ask for evidence, not assurances. Ask who can see the logs, how long they are kept, whether they record reads as well as changes, and how fast the vendor can report on one patient or one engineer. McDonald Hopkins[3] points to least-privilege access, audit logging and regular reviews of roles, logs and audit trails. Test it: ask for last month's production access report.

- [ ] **Which subcontractors touch the environment?**

  List every company with a login, an integration or a support role: hosting, monitoring, error tracking, email, analytics, QA vendors, freelancers. The statute names subcontracted computing facilities, and Hall Render[9] tells covered entities to review business associate services. A good answer is a full list with a region and a contract for each. Ask when the list last changed.

- [ ] **What does the contract say about storage location and audit rights?**

  Put the answers in the contract. McDonald Hopkins[3] advises updating vendor contracts and data processing agreements to require US-only storage and appropriate access controls. Look for four clauses: storage in named US regions, no storage or caching elsewhere, notice before any subcontractor change, and a right to audit. If the vendor will not sign them, you have your answer.

Score each answer as documented, verbal only or missing. Two or more weak answers among questions one to four mean production data should stay out of that vendor's reach until the gaps close. Questions five to seven decide whether you can prove it afterward, which is what a clinic reviewer will ask you to do.

/05

How do you keep real patient data away from offshore engineers?

Make it a design rule: engineers work where no real patient exists. Production sits in a US region. Everything engineers touch every day holds synthetic data. The rest of the setup follows from that split.

1. **Split the environments**
   Run production in a named US region. Run development, test and staging in separate accounts with no network path to production data and no restore from production backups.

2. **Seed with synthetic data**
   Generate test records from the schema, with invented names, dates and notes. Do not copy production and mask it. HHS[10] explains that the Safe Harbor method must remove 18 types of identifiers, in free text as well as structured fields. Free-text notes are where identifiers hide.

3. **Close the production door**
   Give production access only to named, US-based, role-limited accounts, approved per task and logged. Katten[8] expects safeguards to include system-level limits on downloading and copying remotely accessed records.

4. **Scrub what leaves**
   Strip patient data from logs, error reports and support tickets before they leave the US region. Keep error trackers and analytics on US data regions. Treat screenshots as copies.

5. **Review and prove**
   Review access every quarter, keep read logs, and keep a one-page diagram that matches reality. Update it whenever a subcontractor changes.

TEST IT WITH ONE BUG

Ask an engineer to reproduce a production bug. If step one is “send me the record”, the setup has a hole. If step one is “show me the pattern in the logs”, it works.

Ask counsel whether your synthetic and de-identified datasets fall outside what SB 1188 calls patient information. The text is silent. Teams that want an outside review can use TAK Devs security and compliance services.

/06

What did TAK Devs build for UpliftCare, a HIPAA-aligned telehealth marketplace?

UpliftCare came to TAK Devs at the idea stage: no technical architecture, no defined roadmap and a three-month deadline to win investors and pilot clinics. The case study[11] describes a digital marketplace that connects patients, verified therapists and healthcare institutions through a secure, HIPAA-aligned platform.

3 months
from ideation to deployment

6 sprints
to deliver a full product

10+
specialists in a cross-functional team

4
core modules: user, therapist, admin and institutional

70%
reduction in onboarding time through automated credential verification

TAK Devs began with discovery: interviews with therapists, patients and institutional stakeholders, personas and user journeys, a roadmap ranked by priority, a HIPAA-aligned architecture, an AWS deployment plan, and a full documentation set that included requirements and high-level design. Engineering then delivered four connected portals, real-time video, payments, scheduling, insurance data management and verification workflows, with CI/CD pipelines and automated testing.

The result was a live MVP. According to the case study[11], it supported investor presentations and pilot onboarding, therapists and clinics were onboarded during the beta phase, and patients held active sessions during

it. Automated credential verification cut onboarding time by 70%.

Why this matters for a Texas review: a marketplace like this holds identities, sessions and insurance data, which is exactly what a clinic reviewer probes. A documented architecture and a diagram let you answer checklist questions one to three with specifics. That documentation is the kind of artifact a security review asks for.

A limit worth stating: the UpliftCare case study is about HIPAA-aligned architecture, not Texas data residency. It does not claim SB 1188 coverage, and neither does this paper. What it shows is how we work: architecture and documentation come before code, and security decisions are made at the start of the build. Read the full UpliftCare case study for the whole build.

/07

Frequently asked questions

Does Texas SB 1188 ban offshore developers?

No. The law does not mention offshore developers. It requires covered entities to keep electronic health records physically in the United States and to limit access to people who need it for treatment, payment or health care operations. Whether offshore read-only access is allowed is unsettled, so the cautious path keeps production data out of offshore reach.

When did the SB 1188 storage rule start?

The law took effect on September 1, 2025. The storage rule applies to storage on or after January 1, 2026, whatever date the record was prepared. That means older records held in an offshore system after that date are covered too, according to the Texas Legislature's enrolled text[1].

What are the penalties under SB 1188?

The Texas Attorney General can seek injunctions and civil penalties capped at $5,000 per negligent violation, $25,000 per knowing or intentional violation, and $250,000 per violation involving knowing or intentional use of protected health information for financial gain. Agencies can discipline entities after three or more violations (Texas Legislature[1]).

Can engineers test with synthetic data under SB 1188?

The text does not address synthetic or de-identified data. HHS[10] says properly de-identified information is no longer protected health information under the HIPAA Privacy Rule, but Texas law is separate. Synthetic data generated without copying real records is the lower-risk choice. Confirm the reading with counsel.

Does Florida have a similar health record storage rule?

Yes. Since July 1, 2023, Florida has required providers using certified electronic health record technology to keep offsite patient information, including data held by cloud vendors, in the continental United States, its territories or Canada (Florida Statutes[6]). Commentators differ on whether remote offshore access is also barred.

Send us your architecture

A clinic security review can end a pilot with one question: where does patient data live? Send us your architecture. We will mark where a review will push back, before the clinic does.

Book an architecture review

Read the full UpliftCare case study

TAK Devs is a custom software and AI development company with headquarters in Islamabad and a presence in the US, serving clients in the US and Europe. We own the full software lifecycle: strategy, UI/UX, development, QA, cloud and maintenance. ISO 9001 and ISO 27001 certified. Developing Futures.

/08

How this paper was checked

We opened every source below on October 27, 2026 and checked each figure against the page it comes from. Legal readings are attributed to the named law firm or official page, and statute figures come from the Texas Legislature's enrolled text of SB 1188. The sources we reviewed did not include published Texas agency guidance or a reported enforcement action on offshore access. Planning dates, such as HHS's July 2027 target, can move. This paper is general information, not legal advice. TAK Devs is not a law firm: ask counsel before you rely on any reading here.

> General information, not legal advice.

/09

References

[1] **Texas Legislature Online**. SB 1188, 89th Legislature, enrolled version bill text. 2025. https://capitol.texas.gov/tlodocs/89R/billtext/html/SB01188F.htm

[2] **Goodwin Procter LLP**. New Texas Law Regulates Use of EHRs and AI Tools. Aug 29, 2025. https://www.goodwinlaw.com/en/insights/publications/2025/08/alerts-otherindustries-hltc-new-texas-law-regulates-use

[3] **McDonald Hopkins LLC**. S.B. 1188 Texas EHR Law: Data Localization AI and Access Requirements. Aug 25, 2025. https://www.mcdonaldhopkins.com/insights/news/s-b-1188-texas-ehr-law-data-localization-ai-and-access-requirements

[4] **Paubox, Inc.**. How Texas S.B. 1188 transforms healthcare data protection beyond HIPAA. Sep 15, 2025. https://www.paubox.com/blog/how-texas-s.b.-1188-transforms-healthcare-data-protection-beyond-hipaa

[5] **McDermott Will & Emery**. Guarding the Gateway: Florida Tightens Grip on Electronic Health Records Storage. 2023. https://www.mwe.com/?p=244777

[6] **The Florida Senate**. Florida Electronic Health Records Exchange Act, Section 408.051. 2024 Florida Statutes, including 2025C. https://www.flsenate.gov/laws/statutes/2024/408.051

[7] **Alston & Bird LLP**. HHS Office for Civil Rights Delays HIPAA Security Rule Until 2027. Jul 10, 2026. https://www.alston.com/en/insights/publications/2026/07/hhs-delays-hipaa-security-rule-2027

[8] **Katten Muchin Rosenman LLP**. New Texas Law on Storage of Health Care Data. Sep 18, 2025. https://quickreads.ext.katten.com/post/102l604/new-texas-law-on-storage-of-health-care-data

[9] **Hall, Render, Killian, Heath & Lyman, P.C.**. New Texas Law on EHR Data Localization and AI. Aug 19, 2025. https://hallrender.com/2025/08/19/new-texas-law-on-ehr-data-localization-and-ai/

[10] **HHS Office for Civil Rights**. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule. Content last reviewed Feb 3, 2025. https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification

[11] **TAK Devs**. UpliftCare Builds a Complete Telehealth Marketplace in 3 Months. Updated Oct 7, 2026. https://takdevs.com/case-studies/upliftcare-builds-a-complete-telehealth-marketplace-in-3-months/