XAMUN POSITION PAPER · NO. 12 · V1.0 · NOVEMBER 2026

Where a UAE clinic's data, and its AI, are allowed to live.

What UAE law and the Abu Dhabi and Dubai regulators say about where patient data, and the AI that reads it, may be stored and processed.

Arup Maity, Co-Founder and CEO, Xamun Technologies · xamun.ai/whitepaper-uae-clinic-data-and-ai

Can a UAE clinic send patient data to an AI model hosted outside the UAE?
Not by default. Article 13 of Federal Law No. 2 of 2019 bars storing, processing, generating or transferring health data outside the UAE for health services provided here, except in ten cases a 2021 ministerial resolution lists. Abu Dhabi's DoH and Dubai's DHA go further: cloud hosting, backups and the compute behind AI must sit inside the UAE.

Summary of the argument

Since May 2019, Article 13 of Federal Law No. 2 of 2019 has said that health data connected with health services provided in the UAE may not be stored, processed, generated or transferred outside the country, except in cases set by decision. Ministerial Resolution No. 51 of 2021 lists ten such cases. Most need the patient's written approval and encryption, and several need a copy kept in the UAE. None of them describes routine processing by an overseas software or AI provider.

The emirate regulators go further. Abu Dhabi's cyber security standard (ADHICS) requires cloud environments, backups and disaster recovery to sit inside the UAE, covers anonymised and pseudonymised copies too, and limits access to people in the UAE. Its Responsible AI Standard says the compute and storage behind an AI system must be in the UAE. Dubai's DHA policies say the same about cloud providers, backups included.

For a clinic using AI, the test is the whole path the data takes: where the model runs, where prompts and logs are kept, where backups go, and where the people who support it sit. The paper sets out the federal rule and its exceptions, where the PDPL and the DIFC and ADGM laws do and do not reach, the Abu Dhabi and Dubai rules, what this means for hosted models, a checklist for a clinic owner, and the points to confirm with your regulator.

> **The question is not where your software company is. It is where the patient's data goes, every copy of it, including the one the AI reads.**

1 · The federal rule: patient data stays in the UAE

Federal Law No. 2 of 2019 on the use of information and communications technology in health fields (the "ICT Health Law") was issued on 6 February 2019 and came into force in May 2019. Article 2 applies it to all ICT uses in health fields in the UAE, free zones included. Law-firm

summaries list who that catches: clinics and hospitals, insurers, health IT suppliers and cloud providers.

Article 13 is the rule this paper is about. Health data and information connected with health services provided in the UAE may not be stored, processed, generated or transferred outside the country, except in the cases set by a decision of the health authority in coordination with the Ministry of Health and Prevention. The rest of the law sets the duties around it:

- **Confidentiality and integrity (Article 4).** Keep health data confidential, share it only in authorised cases, protect it from unauthorised change or deletion, and keep it available to the people entitled to it.
- **No non-health use (Article 16).** Patient data may not be used for purposes other than health, except with the patient's written consent or in listed cases such as insurance verification, scientific research without identifying the patient, public health, or a court or health authority request.
- **Retention (Article 20).** Keep health data for at least 25 years from the patient's last health procedure.
- **Penalties.** Breaching Article 13 carries a fine of AED 500,000 to AED 700,000. The health authority can also issue warnings, fines of AED 1,000 to AED 1,000,000, and suspend or cancel access to the central health data system (Article 25).

The executive regulation, Cabinet Resolution No. 32 of 2020, adds working rules. Among them: patient consent before health information is disclosed to anyone unless the law allows it, encryption of emails and messages that carry patient information, and reporting of suspicious activity that may affect confidentiality. Law-firm summaries note that it did not explain how Article 13 applies in practice; the ministerial resolution in section 2 did that.

2 · The ten exceptions, and what they do not cover

Ministerial Resolution No. 51 of 2021, issued on 28 April 2021, lists the cases in which health data may be stored or transferred outside the UAE. The table summarises them in our words, from a law-firm summary of the resolution. Read the resolution itself before you rely on one.

Exception	When it applies	Main conditions
1 · Treatment abroad	A patient treated outside the UAE, where the data is needed for that treatment	Written approval of the patient or their representative; shared only with that entity; encrypted
2 · Samples abroad	Samples sent to laboratories outside the UAE	Written approval; shared only with that entity; encrypted
3 · Research	Scientific research that complies with UAE law and is approved by the health authority	Anonymised; encrypted; sent to the highest safety standards; used for research only
4 · Insurance	Data insurers and claims managers need to provide cover	Insurer operates in the UAE; anonymised; patient's written consent; not "fully transferred"; encrypted

Exception	When it applies	Main conditions
5 · Cooperating bodies	Organisations cooperating with federal or emirate government	Written approval; encrypted; anonymised; **copy kept in the UAE**
6 · Personal devices	Simple devices the public use to record vital signs (blood pressure, blood sugar, oxygen saturation)	None specified
7 · Pharmacovigilance	Data about side effects, under good pharmacovigilance practice	Written approval; encrypted; **copy kept in the UAE**
8 · Authority approval	Data an emirate health authority approves for transfer and storage abroad	**Copy kept in the UAE**; not confidential for security, public interest or public health reasons; no medical secrets disclosed without written consent
9 · Remote care	Data used to provide remote health services	Physician's access limited in time; reports or images sent only to that physician; patient's written consent
10 · Patient's request	The patient or their representative asks for the data to be transferred abroad	Written approval; shared only with that entity; encrypted; **copy kept in the UAE**

Two things follow for a clinic. First, nearly every exception is tied to a specific patient, a specific recipient and a specific purpose. None describes a clinic's everyday records, or the prompts its staff send to an AI model, being processed abroad as a matter of routine. Second, where an exception does apply, several still require a copy to stay in the UAE, so the clinic's own record is never only overseas.

Exceptions 8 and 10 are the ones most often raised for software. Number 8 needs a decision from the emirate's health authority, so it is a question for DoH or DHA, not one a vendor can answer. Number 10 starts with the patient asking. A consent line in a registration form is not the same thing. That is our reading; confirm it with your regulator or a lawyer before you build on it.

3 · Where the PDPL fits

The federal Personal Data Protection Law, Federal Decree-Law No. 45 of 2021, took effect on 2 January 2022. Law-firm summaries agree on two exclusions that matter here. It does not apply to health personal data that has its own legislation regulating its protection and processing, which for clinical records is the ICT Health Law. And it does not apply in free zones with their own data protection law, such as the DIFC and ADGM.

Where the PDPL does apply, health information is in its "sensitive personal data" category, which covers data about a person's physical, psychological, mental, genetic or sexual condition, including the health care services they received. Its cross-border rules allow transfers to countries the UAE Data Office approves, or on other grounds such as consent.

For a clinic, the practical reading is this. The PDPL's transfer rules do not open a route around Article 13: patient records are governed by the ICT Health Law, and the localisation rule stays. The PDPL is still worth mapping for data that is not clinical, such as marketing lists and staff records. A

January 2025 law-firm summary reported that the PDPL's executive regulations had not yet been published; check their status before relying on any detail.

4 · Abu Dhabi: the Department of Health

The Department of Health – Abu Dhabi (DoH) regulates through standards that every licensed facility must meet. Two matter most for data and AI.

The Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS), version 2 (DOH/SD/ICSO/ADHICS/V2/2024), was published in May 2024 and took effect in August 2024. It applies to any entity in the emirate that generates, accesses, stores, uses, processes or transmits health information, including healthcare technology and service providers. DoH's own FAQ answers whether a small clinic with one doctor, two nurses and an administrator must comply: yes, at the level set for its facility type. Compliance is checked through audits and licence registration and renewal. On data location, ADHICS says:

- **Cloud, backups included (CS 1.2).** The cloud environment must be physically hosted in the UAE, with no environment, infrastructure or system outside the country, including backup and disaster recovery. Data in the cloud must not be open to access, use or support by a party that sends data or a copy abroad for analysis, or that gives remote support from outside the UAE. Data must be encrypted at rest and in transit, with keys the cloud provider does not supply or control.
- **Anonymised copies too (DP 1.4).** Health information and its copies in any form, whether encrypted, anonymised, de-identified or pseudonymised, must not be stored, processed or transferred outside the UAE. Only people physically in the UAE, or holding a DoH licence to practise, may access systems holding patient data. Exemptions go through the entity's management and then to DoH for approval.
- **Third parties (CO 9.2).** Identified or de-identified health information may not be shared with third parties or data processors unless DoH authorises it, and staff and third parties must support the service from within the UAE unless DoH has issued an exemption.

The Responsible AI Standard (DoH/ST/DDGO/RAI/V1/2025, published and effective October 2025) applies to the DoH and every licensed entity in Abu Dhabi that develops, buys or deploys AI, including AI from third-party vendors, for clinical, financial and administrative work alike. It succeeds DoH's 2018 Policy on Use of AI in the Healthcare Sector (version 0.9, 30 April 2018). Among its requirements:

- **In-country compute (3.1.4.5.1).** The compute and storage behind an AI system, for both the active and the disaster recovery site, must be in the UAE, and remote access for development and support teams should be only from within the UAE.
- **No training on production data (3.1.4.4.2).** Patient data used in AI must be encrypted, anonymised or pseudonymised as required, and production data shall not be used to train the model.
- **People stay in charge (3.1.1.2, 3.1.7.2.2).** AI systems must work under human oversight with clear escalation, and clinicians keep the final decision.
- **Patients are told (3.1.6.1).** Patients and clinicians must be told when AI contributes to a clinical or operational decision, and patients told of any right to opt out.

DoH officials have also said in public that using a cloud inside the UAE needs no Article 13 exemption, though the company should still apply to DoH to use it, and that exemptions for transfers abroad run for up to a year (U.S.–U.A.E. Business Council account of a DoH webinar, 12 May 2025). The Responsible AI Standard lists October 2026 as its revision date, so check for a newer version before you build to it.

5 · Dubai: the Dubai Health Authority

The Dubai Health Authority (DHA) sets the same line through several policies.

- **Cloud storage.** The Policy for Health Information Assets Management (DHA/HISHD/PP-12, issued 26 December 2022, effective 26 March 2023) says a cloud solution must not store health information with a cloud provider outside the UAE's legal jurisdiction or borders, including for the provider's backup or disaster recovery. Its contract must say the provider has no ownership rights in the data, returns it in a usable format if the clinic moves, and destroys it when no longer needed.
- **Sharing and transfer.** The Policy for Health Information Sharing (DHA/HISHD/PP-13, issued 10 August 2024, effective 10 November 2024) says protected health information should not be transferred outside the UAE except within the categories of Resolution No. 51 of 2021, and that DHA approval is needed under its classification policy.
- **Security standard.** The NABIDH Information Security Standards (version 1.0, September 2020) say facilities shall not use cloud services to store, process or share health information outside the UAE, backups and disaster recovery included.
- **AI.** The DHA Policy for Artificial Intelligence in the Healthcare (DHA/HISHD/PP-09, issued 1 July 2021, effective 1 October 2021) requires AI tools to comply with the ICT Health Law in full, with federal and Dubai rules on data protection and security, and asks that users be told what role the healthcare professional plays in the final decision. Its listed revision date, 1 July 2026, has passed; check for a newer version.

Dubai's documents are less explicit than Abu Dhabi's on anonymised data. The NABIDH standard notes that anonymised information is not necessarily subject to the same sharing restrictions. Treat that as a question for DHA, not as permission to send de-identified data abroad.

6 · DIFC and ADGM: where their laws reach, and where they do not

The DIFC and ADGM have their own data protection laws, both close to Europe's GDPR. Both treat health data as a special category. Neither replaces the federal health rules for a clinic.

- **DIFC.** The DIFC Data Protection Law, DIFC Law No. 5 of 2020, took effect on 1 July 2020 and was amended in July 2025. It applies to controllers and processors incorporated in the DIFC, wherever they process, and to others processing personal data in the DIFC as part of stable arrangements. The DIFC also has a regulation on personal data processed through autonomous and semi-autonomous systems (Regulation 10 of its Data Protection Regulations).
- **ADGM.** The ADGM Data Protection Regulations 2021 apply to processing in the context of the activities of a controller or processor established in ADGM, whether or not the processing happens in ADGM.

What that means in practice:

- **A clinic licensed by DHA in mainland Dubai, or by DoH in Abu Dhabi,** is not brought under DIFC or ADGM law because its software or AI vendor is incorporated there. The vendor may be bound by that law for its own processing. The clinic's duties stay federal and emirate ones.
- **A clinic physically in a free zone** still has the ICT Health Law, which Article 2 applies to free zones, and its health regulator. A free-zone data protection law adds duties; it does not lift Article 13.
- **A vendor's free-zone address** says nothing about where the data sits. Ask where it is processed, not where the company is registered.

Dubai Healthcare City has its own Health Data Protection Regulation (No. 7 of 2013). A clinic licensed there should confirm with its regulator how that regulation sits alongside the federal law.

7 · What this means for hosted AI models

Most clinics will not run their own AI models. The graphics processors and the people to run them cost more than a clinic or a small group can carry, so in practice only large groups host models themselves. Everyone else uses a model from an AI provider, and the question becomes where that provider processes the data. The table sets out the four patterns.

Pattern	How the rules treat it	In practice
Model hosted outside the UAE, patient data sent to it	Health data processed abroad: an Article 13 problem unless one of the ten exceptions applies. ADHICS and the DHA cloud rules do not allow it.	Do not use it for anything that carries patient data.
De-identify first, then send abroad	Abu Dhabi: ADHICS covers anonymised, de-identified and pseudonymised copies, so no. Dubai: less explicit.	Ask DHA or DoH in writing before relying on it.
Provider's UAE region, all processing in the UAE	The pattern the regulators describe: in-country compute, storage, backups and support. Abu Dhabi still expects an application to DoH for cloud use.	Workable for most clinics, if the whole path is in the UAE (see the questions below).
Own model on own GPUs, in a UAE data centre	Meets the location rules directly, and leaves the clinic running the hardware and the model.	Realistic for large groups. Most clinics cannot fund or staff it.

A "UAE region" label is not enough by itself. The rules are about every copy and every person with access, so ask the AI provider, and the software vendor that sits in front of it:

- **Where does the model run?** Inference, not just storage, in the UAE.
- **Where are prompts, outputs and logs kept,** including any copies kept for abuse monitoring or debugging, and for how long?
- **Where do backups and disaster recovery go?** ADHICS, the DHA policy and the NABIDH standard all name backups and disaster recovery.
- **Who can reach the data, and from where?** Support staff and engineers outside the UAE are a problem under ADHICS and the Responsible AI Standard.

- **Is our data used to train or improve the model?** DoH's standard says production data shall not be.
- **Who holds the encryption keys?** ADHICS says keys should not be supplied or controlled by the cloud provider hosting the data.
- **Which subprocessors touch the data,** and are they in the UAE too?

Get the answers in the contract, not in a sales deck, and keep them on file with the date. Providers change regions and terms, and your regulator will ask what you checked, and when.

8 · A checklist for a clinic owner

Most of this is a review of what you already run. In order:

- **List every system that holds patient data.** The clinic system, the lab and imaging links, billing, the booking tool, the WhatsApp or chat tool, email, file storage, and any AI tool staff use, including the free ones on their phones.
- **For each, write down where the data is stored and processed,** where the backups go, and who supports it from where. Anything outside the UAE needs an exception, an approval, or a replacement.
- **Stop patient data going into public AI tools.** A chatbot account a receptionist opened is still the clinic sending health data to a provider, often abroad.
- **Check each AI tool against the questions in section 7,** and get the answers into the contract.
- **Know which regulator and which rules you are under:** DoH (ADHICS, Responsible AI Standard), DHA (cloud, sharing and AI policies, NABIDH), or MOHAP or your own emirate's health authority elsewhere, plus any free-zone law.
- **In Abu Dhabi, check your ADHICS level and your cloud application to DoH.** A small clinic is in scope.
- **Tell patients when AI is used,** what it does, and that a person makes the clinical decision.
- **Keep a person on every clinical decision.** DoH's standard says clinicians keep the final decision, and DHA's policy expects users to be told the professional's role in it.
- **Plan retention for 25 years.** Your contracts should say the data comes back to you in a usable format if you change provider.
- **Write it down.** A one-page data map with dates is what you will want when an auditor or a patient asks.

9 · Questions to confirm with your regulator

Some points are not settled by the published documents. Settle these with your regulator, or a lawyer, before you build a process around one reading:

- **Anonymised data in Dubai.** ADHICS is explicit that anonymised copies stay in the UAE. Does DHA take the same view for AI processing abroad?
- **The cloud application in Abu Dhabi.** What does DoH need from a clinic that uses a UAE-hosted cloud or AI service, and does a vendor's approval cover its clinic customers?

- **Consent as an exception.** Can exception 10 ever cover routine processing, or only a transfer the patient asks for?
- **Support from abroad.** Does an overseas engineer who sees only system logs, not patient records, need an exemption?
- **Versions.** Are the DHA AI policy and the DoH Responsible AI Standard, both past or at their listed revision dates, still the current versions?

This paper is Xamun's reading of the published law and policies, not legal advice. Confirm with DoH, DHA or MOHAP as relevant, with a lawyer, or with your insurer before you rely on it.

10 · Where Xamun fits

We build clinic software, including ClinicOS, and Xami Workers, the AI workers we call Sam, which say they are AI, hand anything clinical to a person, and assist before they act alone. For UAE rollouts we deploy on UAE-compliant hosting, with AI providers that process in the UAE; groups large enough to run their own GPUs can host the models themselves. It is bought as a licence or as Outcome-as-a-Service, and the data map in section 8 is where we start.

Questions a clinic should ask, answered plainly

Can a UAE clinic send patient data to an AI model hosted outside the UAE?

Not by default. Article 13 of Federal Law No. 2 of 2019 bars storing, processing, generating or transferring health data outside the UAE for health services provided in the UAE, except in the cases Ministerial Resolution No. 51 of 2021 lists. Abu Dhabi's ADHICS and Responsible AI Standard, and Dubai's DHA cloud policies, also require the hosting, backups and disaster recovery to be in the UAE.

Can a clinic in the UAE use cloud hosting?

Yes, if the cloud is in the UAE. ADHICS requires the cloud environment, including backup and disaster recovery, to be physically hosted in the UAE, and DHA's Policy for Health Information Assets Management says the same for Dubai. DoH officials have said cloud use inside the UAE needs no Article 13 exemption, but the company should still apply to DoH to use it.

Does anonymising patient data let it leave the UAE?

Not in Abu Dhabi. ADHICS says health information and its copies in any form, whether encrypted, anonymised, de-identified or pseudonymised, must not be stored, processed or transferred outside the UAE without DoH approval. Ministerial Resolution No. 51 of 2021 uses anonymisation as a condition of some exceptions, such as research. Dubai's documents are less explicit, so ask DHA in writing.

What are the ten exceptions to Article 13?

Ministerial Resolution No. 51 of 2021 allows health data abroad for treatment abroad, samples sent to overseas laboratories, approved research, insurance, organisations cooperating with government, personal vital-sign devices, pharmacovigilance, emirate health authority approval, remote health services, and a patient's own request. Most need written approval and encryption, and several need a copy kept in the UAE.

Does the PDPL apply to patient records?

Generally not. Federal Decree-Law No. 45 of 2021 excludes health personal data that has its own legislation, which for clinical records is Federal Law No. 2 of 2019, and free zones with their own data protection law. Where the PDPL does apply, health information is sensitive personal data.

Does DIFC or ADGM data protection law apply to my clinic?

Only if the clinic is established there. The DIFC law applies to entities incorporated in the DIFC or processing there as part of stable arrangements, and the ADGM regulations to establishments in ADGM. A vendor's DIFC or ADGM address does not change a mainland clinic's duties, and a free-zone clinic still has the federal health data law.

What is the penalty for storing health data outside the UAE?

Breaching Article 13 of Federal Law No. 2 of 2019 carries a fine of AED 500,000 to AED 700,000. The health authority can add warnings, fines of AED 1,000 to AED 1,000,000, and suspension or cancellation of access to the central health data system.

How long must a UAE clinic keep patient records?

At least 25 years from the patient's last health procedure, under Article 20 of Federal Law No. 2 of 2019.

About this paper

This paper is Xamun's own reading of published UAE law and regulator policy, as at 6 November 2026. It is not legal advice, and it is not issued, reviewed or endorsed by the Ministry of Health and Prevention, the Department of Health – Abu Dhabi, the Dubai Health Authority or any free-zone authority. Where a source is a law-firm summary rather than the official text, the list says so. Confirm with your regulator (DoH, DHA or MOHAP), a lawyer or your insurer before you rely on it.

Sources and references

1. Federal Law No. (2) of 2019 Concerning the Use of Information and Communications Technology in Health Fields, issued 6 February 2019, in force May 2019 — Articles 2, 4, 13, 16, 20, 25 and the Article 13 penalty. Official text: uaelegislation.gov.ae. Read here through Latham & Watkins, "New UAE Law Regulates Healthcare Data", Client Alert 2514, 19 June 2019 (law-firm summary).
2. Cabinet Resolution No. (32) of 2020 on the executive regulation of Federal Law No. 2 of 2019 — as summarised by BCLP, JD Supra, 10 June 2020 (law-firm summary).
3. Ministerial Resolution No. (51) of 2021 on the cases permitting storage or transfer of health data outside the UAE, issued 28 April 2021 — the ten exceptions and their conditions, as tabulated by Latham & Watkins, "UAE Decision on Health Data Law Provides Clarity", Client Alert 2891, 29 August 2021 (law-firm summary).
4. Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data, in force 2 January 2022 — scope exclusions: Clyde & Co, "UAE issues landmark personal data protection law", 30 November 2021, and Gowling WLG, 7 February 2022; sensitive personal data definition and executive-regulation status: DLA Piper, Data Protection Laws of the World, UAE, updated 27 January 2025 (law-firm summaries).
5. Department of Health – Abu Dhabi, Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS), DOH/SD/ICSO/ADHICS/V2/2024, published May 2024, effective August 2024 — controls CS 1.2, DP 1.4 and CO 9.2. doh.gov.ae, Aamen programme.
6. Department of Health – Abu Dhabi, ADHICS Frequently Asked Questions, version 1.3 (2022) — scope for small clinics, audit and licensing, cloud. doh.gov.ae.

7. Department of Health – Abu Dhabi, Responsible Artificial Intelligence (AI) Standard, DoH/ST/DDGO/RAI/V1/2025, published and effective October 2025 — sections 1.2, 3.1.1.2, 3.1.4.4, 3.1.4.5, 3.1.6.1 and 3.1.7.2. doh.gov.ae.
8. Department of Health – Abu Dhabi, Policy on Use of Artificial Intelligence (AI) in the Healthcare Sector of the Emirate of Abu Dhabi, Policy/AI/0.9, 30 April 2018. doh.gov.ae.
9. U.S.–U.A.E. Business Council, "Department of Health – Abu Dhabi Clarifies Cross-Border Health Data Laws", account of a DoH webinar held 12 May 2025 — cloud inside the UAE, exemption terms. usuaebusiness.org.
.0. Dubai Health Authority, Policy for Health Information Assets Management, DHA/HISHD/PP-12, issued 26 December 2022, effective 26 March 2023 — section 4.5, cloud-based solutions. dha.gov.ae.
.1. Dubai Health Authority, Policy for Health Information Sharing, DHA/HISHD/PP-13, issued 10 August 2024, effective 10 November 2024 — section 4.20, transfer outside the UAE. dha.gov.ae.
.2. Dubai Health Authority, NABIDH Policies and Standards, Section 8: Information Security Standards, v1.0, September 2020 — Domain 17, cloud computing. dha.gov.ae.
.3. Dubai Health Authority, Policy for Artificial Intelligence in the Healthcare, DHA/HISHD/PP-09, issued 1 July 2021, effective 1 October 2021 — section 4.6, minimum requirements for AI tools. dha.gov.ae.
.4. DIFC Data Protection Law, DIFC Law No. 5 of 2020, in force 1 July 2020 — scope as amended 8 July 2025: DLA Piper, 28 July 2025; special categories: Latham & Watkins, "New Data Protection Law in the DIFC", September 2020; Regulation 10: Clyde & Co, September 2023 (law-firm summaries).
.5. ADGM Office of Data Protection, "ADGM Data Protection Regulations 2021 Update", 4 August 2021 — territorial scope, Article 3(1). adgm.com.
.6. Dubai Healthcare City, Health Data Protection Regulation No. 7 of 2013. dhcc.ae.
.7. Xamun Position Papers No. 1 to No. 11 (August–November 2026), xamun.ai/whitepapers.

No. 12 in the Xamun position-paper series. © 2026 Xamun Technologies. Version 1.0, November 2026. xamun.ai/whitepapers