

OpenEMR Weekly Meeting Detailed Summary

August 25, 2026

Attendees: Stephen Nielson (chair), Stephen Waite, David Eschelbacher, Luis M. Santos, Eric Stern (OCE), Ian McDonald (new), Sherwin Gaddis, Michael Smith (OCE), Bobby Anchanattu, Mike. Brady Miller absent (family reunion).

Recording: Attendees were informed that the meeting is recorded to generate a transcript for AI-assisted summary notes, and confirmed they were comfortable with that. It was noted that anything off the record can be handled by pausing.

Introductions

Ian McDonald

- **Worked with Dr. Luis Santos at the NIH** in the clinical center's radiology and imaging sciences department, on custom pipeline projects for research data processing.
- **Left the NIH during the federal reduction in force** carried out under the Department of Government Efficiency.
- **Subsequently at Microsoft as an interface engineer on PowerShare**, implementing automated order generation — a subsystem producing automated ORM messages that interface with the EMR so that importing an external study creates a corresponding internal order, giving parity between PACS and the EMR. Roughly 110 hospitals implemented over about eight months; three to four years on that work overall.
- Now collaborating with Luis at MedicalMasses, the independent company Luis opened earlier this year.

Luis M. Santos

- **Has known of OpenEMR since roughly 2019–2020** but has not previously had the opportunity to be involved. Plans to begin visiting local clinics in the coming weeks to understand their needs.
- **CEO and founder** of MedicalMasses. <http://medicalmasses.com/>
- **Current focus is HL7 — specifically a V2 to FHIR conversion toolset (RUMTK).** The stated ambition: a simple set of tools for Linux and cloud that can move installations from V2 to FHIR, and eventually connect systems so that the patient record travels with the patient — authenticate with a token, and systems collect the patient's records across providers.
- **Also holds a technology transfer from the NIH covering DICOM work.** The intent is to combine these into a comprehensive package.
- **Team is small:** Luis and Ian on technology, with Kelsey (not present) on administrative work and styling.
- Noted that his availability comes in bursts between other commitments — acknowledged as a common pattern in open source contribution.

Internationalization Question

- **Asked whether the V2-to-FHIR work targets US variants of HL7**, given that every country introduces its own variations — Ireland was cited as an example.
- **Answer:** Unicode support is present, so names and text should be handled — everything is converted to UTF-8, with an additional package used to determine expected country and language. The current focus is the V2 side to ensure backwards compatibility.

Business Development and Collaboration

Contract Opportunity

- **Luis circulated an email about an EHR contract opportunity** in the mental health space — currently at the request-for-information stage rather than a live bid.
- **The ask:** whether the foundation and OpenCoreEMR would be interested in collaborating, since his team does not have the capacity to handle the full complexity of an EHR system alone.
- **OpenCoreEMR:** the email has been passed to their head of product and CEO; no response yet at the time of the call.
- **Sherwin Gaddis:** mental health is squarely in his wheelhouse — he has worked with a number of mental health clinics over the years and developed workflows for them. Happy to collaborate, though his availability is limited for another month or two.
- Details to be circulated separately by email rather than on the call.

Other Opportunities

- An earlier opportunity was mentioned as something Luis could revisit, now that he has a relationship with the project and access to people who can answer technical requirements.
- **Rural funding:** individual states are leveraging the rural development fund, and CMS has been releasing funds under rural transformation. Flagged as another area to work on together.
- **Introduction offered to James Shelby,** who is helping oversee ONC and ASTP guidelines around rural funding for the next four to five years across grant applications.
- **Proposal:** schedule a separate call for interested vendors rather than occupying the weekly slot — not this week, possibly next week outside the Tuesday call, or handle it by email.
- Luis also asked whether the group knows of opportunities that would let him mature the HL7 V2-to-FHIR pipeline work.

DICOM, PACS, and the Viewer Gap

OHIF Viewers: <https://github.com/OHIF/Viewers>

- **A genuine gap was identified in OpenEMR:** the DICOM viewer currently in use is not certified in the US for diagnostic purposes. It works comparably to other viewers in practice, but is not permitted for diagnosis.
- **There have been various open source PACS integrations,** but nothing turnkey for handling PACS and DICOM. Every vendor builds their own custom solution, and there is nothing in the open source community suitable to roll out and develop against.
- **OHIF was raised as the strong candidate.** Categorized as a research viewer because it is an open source project, and missing some pieces for a full radiology workflow — but for a PCP clinic it has more than enough features to confirm what a radiologist is looking at. FDA-type accreditation for diagnostics remains the sticking point.
- **Luis is already packaging OHIF with his DICOM automation platform,** which together forms a small research PACS.
- Noted that a company working on OHIF was acquired, in a pattern compared to OpenCoreEMR's relationship with OpenEMR.
- **Stephen Waite has contributed patches to OHIF** that are still awaiting review, and has had contact with the project at a conference.

External IDP and the Module-First Position

Bobby Anchanattu's PR: <https://github.com/openemr/openemr/pull/13023>

- **Bobby has an early-version PR for OpenID Connect external IDP authentication.** He noted in chat that it needs substantial cleanup, that he has further changes, and that he will only update it if there is future interest — otherwise he will close the PR.
- **Review response:** better as a separate external module than folded directly into core. Bobby had paused after that feedback, having found that some OpenEMR-side changes would be needed for loading and UI, and is trying to work out how much of that he can avoid.
- **His argument for the feature:** an external IDP enabling single sign-on would be a good addition, and a single IDP avoids token leakage issues.
- **Context given on why module-first:** maintainer time is heavily committed at present, as it is across most open source projects right now. With limited review capacity, new feature development is directed toward modules wherever the capability allows. Features can be brought into core later once they have been tested and proven in use.
- **Noted that there have been four or five prior attempts at IDP integration** — enough that reviewers could not immediately recall which PR was which.
- **Michael Smith's caveat:** sometimes it genuinely is impossible to do something as a module without a core change. If that happens, raise a separate PR stating exactly what core change is required for the rest to work as a module. That will probably unlock other things too.
- **Eric Stern:** often one or two event hooks is all that is needed to unlock building the whole thing as a module — far easier to review and far more likely to be accepted than a large rewrite into core.
- **Front controller connection:** authentication-facing work always needs to hook in very early in the request. It may be easier not to support IDP in the old architecture at all and support it only through the front controller. Position taken: that would be acceptable — no appetite for bending over backwards to support it in the old architecture.

Front Controller and Demo Farm

Demo farm repository: https://github.com/openemr/demo_farm_openemr

- **The agreed ordering was restated:** deprecate non-webroot installations, then turn on the front controller, then the module overhaul and its downstream implications follow. The demo servers need the webroot change because the front controller assumes it is running at the web root.
- **Vendor-side status:** OpenCoreEMR has the deployment configuration in place so the front controller can be switched on for internal dev servers, but it has not yet been enabled anywhere.
- **Eric's development experience:** he ran OpenEMR through the built-in PHP web server pointed at the front controller during initial development, and other than the usual PHP development server quirks it ran well.
- **Where the snags are expected:** modules with their own custom access rules. All bundled modules have been ported into the front controller, but Composer-installed modules with their own htaccess are invisible to the project — described as a chicken-and-egg problem.
- **Bandwidth:** both admins and the foundation side are consumed by security work. Realistic expectation set that nothing moves on the front controller for a couple of weeks unless someone stands up the demo. Eric was explicit that he is in no hurry.
- **The demo farm process turns out to be simpler than assumed:** it is a config-file PR to the demo farm repository, pointing at a GitHub branch, and Brady typically approves within a day. The process has been automated for at least a couple of years — once merged, the instance is added automatically and the demo resets on a schedule. Since it runs Docker, the Docker image changes for htaccess and web roots should carry through.
- **Eric's goal:** a public instance people can poke at to give feedback on the front controller. It is already integrated into the test suite, so his concern is not correctness — the lack of an outside-OCE public instance is one of the major hesitations about bundling it into the actual deployment.

Test Data for Development

openemr-cmd: <https://github.com/openemr/openemr-devops/tree/master/utilities/openemr-cmd>

- **Bobby asked for realistic test data** for his AI work; a previous attempt corrupted his database, which he suspected was his own setup.
- **Two avenues offered.** First, the limited demo database in the OpenEMR codebase, available through the Easy Development Environment and the OpenEMR command utility.
- **Useful commands:** openemr-cmd drid resets the database and installs demo data; openemr-cmd irp {number} renders and imports that number of Synthea patients.
- **Second, the Synthea data set**, which generates transfer summary of care documents (CCDAs) that get imported, producing patients with fairly comprehensive encounter history, procedures, medications, allergies, and immunizations.
- **Acknowledged weakness:** the CCDA import only populates seven or eight discrete functional database models beyond basic demographics. Synthea generates far more data than is currently imported, and contributions to improve the CCDA import are actively wanted.
- **A much more comprehensive data set exists for certification work** but cannot be shared publicly due to licensing restrictions under contract.

Proposed Security Modules

Stephen Nielson previewed two modules he has been building and intends to release to the community.

Module 1 — File Integrity and Advisory Surfacing

- **Generates a hash manifest of every release file** and scans the OpenEMR installation to identify anything that has changed.
- **Retrieves the published advisories applicable to the installed release** and surfaces them in a report presented to the administrators who install the module.
- **Handles local modifications through explicit whitelisting** — additional files listing your known changes, which have to be re-approved on each update. The purpose is to let operators see what they have changed so they can plan an upgrade.
- **Built to be backwards compatible potentially as far as version 6**, since it takes a release version and builds the manifest from that.
- **Distribution:** via Packagist and Composer, possibly also as a download from the OpenEMR site. Not to be bundled into core initially — the intent is to let it bake and be tested first. Eric noted that since most affected installs are on older versions, bringing it into core does not help them anyway; both agreed it makes sense in core going forward.
- **Eric's suggestion:** a GPG-signed PHAR would be a good distribution route, since affected users may be running XAMPP, non-Docker, or custom configurations and need something they can simply drop on their system. Well received.
- **Caveat noted:** a scanner installed independently of the product is harder to assure than one shipped with it, which is an argument for eventual inclusion in core.

Module 2 — Automated Backup and Upgrade

- **A means of performing an automated backup from a root-type user** — sites directory and database — and driving the upgrade schedule off the release manifest.
- **Aimed specifically at operators not running Docker**, where the existing automatic update path does not apply.
- **Scope boundary stated:** it will identify how an upgrade is going to break — here are the files you have modified — and leave resolution to the operator. No attempt to reapply customizations on top of an upgrade.

Existing Tools and Related Ideas

- **Comparable tools exist in other projects** — Gentoo's GLSA check was named, with Debian and Red Hat having equivalents. OpenEMR does not ship through Linux distributions so direct integration is not applicable, but their UX for listing vulnerabilities and prescribing remediations is a good model.
- **Research found nothing that fit well**, given that OpenEMR has to run both inside Docker and on a flat file system. Noted as surprising that this appears unsolved.
- **Adding a workaround section to published advisories was proposed**. Where an operator cannot upgrade immediately, a documented configuration-level mitigation gives them an interim option. Acknowledged as additional documentation work for the project, but valuable to operators.
- **Messaging insight**: people do not respond to being told their version is out of date, but they do respond to being told they have important updates outstanding. Related to the previously discussed freshness check, but with a stronger hook.
- **Second messaging angle**: telling an operator that a large number of their files have been modified and the project cannot vouch for their security.

SBOM and Syft

Syft: <https://github.com/anchore/syft>

- **Luis raised software bill of materials work** from his time with the radiology department, where they used Syft — a Go tool usable as a CLI utility and integrable into scripts and pipelines, which can generate a report of modules with outstanding or resolved issues.
- **Coverage**: Syft can scan Docker directly or a host system, and supports languages with package managers — Go, Rust, Python. Whether PHP is covered was uncertain and worth checking.
- **The distinction drawn**: SBOM tooling tracks dependencies, which is a different problem from comparing an installation against a known-good release manifest. If someone has modified core components directly, dependency tracking does not help; a published package at least shows up as a tracked dependency.

The Customization Problem

- **The recurring pattern**: operators install a version, then hack it or hire a vendor to customize it. They subsequently do not know what software they are actually running, cannot upgrade, and face further cost to find out.
- **Costs cited**: \$5,000 to \$20,000 paid for customizations, then a further \$10,000 to \$20,000 to diagnose why an upgrade fails. Cases were described of installations several versions behind where the operator has been maintaining their own patches on top of heavy customization.
- **The first requirement is awareness** — until an operator knows what they have modified, they do not know they have a problem. That is the primary value proposition of the integrity module.
- **Composer installation raised as a longer-term structural answer**: if OpenEMR itself lived under a vendor directory, most people have the sense not to edit code there. Would not help existing installations, but could be a way to discourage painting oneself into a corner — floated as a possibility for a future major version.
- Luis noted general value in anything that makes migrations easier, and offered to contribute time to a Docker migration tool if his business situation allows.

Module Discovery

- **Third-party modules are discoverable on Packagist** — anything including the OEmodule type is searchable, and searching for OpenEMR surfaces them.
- **Current counts checked live:** 28 packages tagged openemr and 19 more tagged openemr-module. Up from around eight the last time anyone had looked, one of which was the sample module and was the most installed by a good margin.
- **The unpublished majority:** Stephen estimated he alone has around 20 modules developed for clients that are not yet publicly released — they are open source but need client permission to publish. Overall estimate offered that only five to ten percent of modules written are publicly available, though that is still considered a good start.
- **Discoverability action:** point people to Packagist from the OpenEMR homepage and from the modules page inside the application, which already links out to the modules page on the website.
- **Distribution channel for the new modules:** mention them in the security update announcements — framed as something being experimented with, aimed at those who care about security, with a request for feedback. The intent is a report page plus an option to have scan results emailed.

Release

- **Release cadence needs reconciling.** The board meeting and the weekly calls reached materially different conclusions about how often to release. With Brady absent, this was punted to next week.
- **The next release is targeted at roughly two weeks out.**
- No release call held this week given Brady's absence.

Items Discussed and Proposed

Recorded as topics raised and directions favored, not as assigned work or commitments.

Area	Discussed / Proposed
Luis Santos	Recirculate the opportunity details by email to interested parties, including Sherwin Gaddis.
Vendors	A separate call proposed for interested vendors rather than using the weekly slot. Possibly next week, or handled by email.
Stephen Nielson	Introduce Luis Santos to James Shelby, who is helping oversee ONC/ASTP guidelines around rural funding grant applications for the next four to five years.
Bobby Anchanattu	Guidance given: pursue the external IDP as a module. If a core change is genuinely required, raise it as a separate small PR describing the hook needed.
Stephen Nielson	Two modules in progress — a file integrity monitor with advisory surfacing, and an automated backup/upgrade module for non-Docker installs. To be distributed via Packagist/Composer, possibly as a signed PHAR.
Documentation	Adding a workaround section to published advisories was proposed, so operators unable to upgrade immediately have a documented mitigation.
Eric Stern	Stand up a public front controller instance on the demo farm for outside feedback. Process is a config-file PR to the demo farm repo, now automated.
Front controller	Agreed ordering: deprecate non-webroot installations, then enable the front controller, then the module overhaul follows.
Release	Cadence needs reconciling — the board meeting and the weekly calls reached different conclusions. Deferred to next week. Next release targeted roughly two weeks out.
Discovery	Point users to Packagist for third-party modules from the OpenEMR homepage and the in-application modules page.

Notes

- A light meeting on project mechanics, weighted toward introductions and business development. Summer availability was noted repeatedly as the reason several threads have not moved; expectation is that things pick up in September.
- Recurring theme: module-first is now the consistent answer to new feature proposals. It appeared in the IDP discussion, the new modules, and the DICOM viewer gap alike — driven less by architectural preference than by the reality that maintainer review capacity is the binding constraint. Contributors willing to build and maintain modules have a clear route in.