EXAMPLE HEALTHTECH DPIA REPORT

HealthTech DPIA Evidence Report

Theom technical controls, example discovery scenarios, and residual-risk treatment plan

Report type	Example data protection impact assessment evidence pack
Industry profile	Dental healthtech platform and full-service lab handling patient cases, scan/design files, crown and bridge orders, logistics, billing, analytics, and AI-assisted workflows
Control model	Theom data discovery, access governance, activity monitoring, lineage, policy, and AI data-use monitoring
Status	Example report for stakeholder review; not a legal opinion or final DPIA determination

Important use note: This document is an example dental healthtech DPIA evidence report. Findings and metrics illustrate conditions Theom can identify or substantiate across data stores, identities, access paths, lineage, activity, and policy controls.

Prepared June 24, 2026 for privacy, security, data governance, infrastructure, and AI risk teams.

Executive Summary

This report models a data protection impact assessment for an example dental healthtech organization operating a full-service dental lab. The platform supports digital case intake and manufacturing workflows for services such as 5-day zirconia crowns, eMax crowns, PFM crowns, metal crowns, and dental bridges. The processing profile is high risk because it includes patient identifiers, prescriptions, intraoral scans, CAD/CAM design files, provider and billing data, cross-border access, service-account automation, third-party integrations, and AI retrieval or summarization paths.

Theom provides the technical evidence layer for the assessment. The control model focuses on continuous discovery, classification, entitlement mapping, actual-use monitoring, lineage, policy findings, and AI data-use evidence. The example scenarios are framed as review-ready findings that can be validated, refined, or replaced with organization-specific evidence during a formal DPIA.

42,870	312	91	17	8
Data assets in scope	PHI/case-data stores	Overprivileged identities	Countries / access regions	Priority findings

Item	Executive takeaway
Primary risk	Unbounded propagation of dental PHI, scan/design files, crown and bridge order details, logistics data, billing data, and support context into analytics, AI, and non-production environments.
Strongest control coverage	Inventory, classification, access path mapping, actual-use evidence, policy findings, and overprovisioning worklists.
Key gap	DPIA sign-off requires organization-specific Theom evidence, local legal transfer mapping, retention policy alignment, and data-owner review attestation.
Recommended next action	Run a 30-day Theom evidence sprint across dental case intake, scan/CAD design, crown and bridge production, shipping, billing, support, AI retrieval, and partner-share domains.

Processing Scope and Assumptions

The target organization is an illustrative cloud dental healthtech provider and full-service dental lab. The platform supports dentist onboarding, patient case intake, intraoral scan and design-file upload, prescription capture, case planning, lab production, quality review, shipping, billing, analytics, support workflows, data science notebooks, partner exports, and AI copilots. The report assumes cloud warehouse, application datastore, object storage, SaaS, API, and notebook environments are connected to Theom.

Scope element	Report assumption
Data subjects	Patients, dentists, practice staff, lab technicians, support users, administrators, contractors, logistics partners, suppliers, and integration/service identities.
Data categories	PHI, patient identifiers, provider/customer identifiers, crown and bridge prescriptions, intraoral scans, STL/PLY/CAD files, shade and margin notes, case status, material selection, remake reasons, shipping addresses, payment data, support tickets, access logs, and AI prompt/output metadata.
Processing purposes	Dental restoration manufacturing, case planning, lab operations, quality review, logistics, billing, analytics, customer support, security monitoring, data governance, and AI-assisted productivity.
Regulatory framing	GDPR Articles 5, 9, 25, 30, 32, 35, and 44-49; HIPAA/HITECH concepts where applicable; local health-record retention and cross-border transfer rules.
DPIA trigger	Large-scale special-category health data, systematic monitoring, cross-border processing, new AI data-use pathways, and broad non-human access.

Control Evidence Domains

Domain	Evidence target
Discovery and classification	Find PHI, identity, payment, prescription, scan/CAD, provider, material, shipping, and custom dental-case entities across structured and unstructured stores.
Residency and transfer	Map asset location, access location, replication paths, and transfer mechanism tiers.
Lineage and minimization	Trace copies, clones, views, extracts, notebook outputs, and production-to-non-production flows.
Access governance	Compare granted access with actual use, role paths, service accounts, admin grants, and dormant access.
Activity and AI monitoring	Monitor queries, exports, joins, prompt-driven retrieval, tool calls, output surfaces, and anomalous behavior.
Audit and accountability	Produce policy violations, data-owner review packs, remediation records, and DPIA evidence appendices.

Theom Technical Control Model

Theom's role in this example DPIA is to turn data-security telemetry into usable privacy evidence. Rather than relying on static inventories or point-in-time access reviews, Theom continuously correlates data sensitivity, asset location, identity paths, observed use, lineage, and policy outcomes.

Control area	Question answered	Theom evidence
Data security posture	Where is sensitive data, what is exposed, and which stores are stale, dark, copied, or misclassified?	Inventory, classification, criticality, location, ownership, dark-data state, and error coverage.
Access governance	Who and what can reach dental PHI and case data, and does that match actual purpose and use?	Effective access, overprovisioning, roles, groups, direct grants, service accounts, admin posture, MFA/network-policy signals.
Activity monitoring	What is happening now, from where, by whom, and against what class of data?	Queries, exports, joins, login country/IP, MFA use, failed attempts, unusual access patterns, and policy findings.
Lineage and minimization	Where did patient case data, scan files, and production metadata move after intake, and what downstream copies must be reviewed or erased?	Source-to-target lineage, clones, views, notebook outputs, ETL jobs, and production-to-non-production propagation.
AI data-use monitoring	Which AI tools, copilots, retrieval workflows, or notebooks touched restricted data?	Prompt/task context where available, source data, tool calls, retrieval sets, joins, output actions, and policy violations.

Evidence principle: For formal use, every DPIA assertion should cite a Theom export or screenshot pack: asset inventory, classifier results, access list, activity sample, lineage graph, policy rule, violation record, and remediation ticket.

Example Theom Findings

The following findings are example review-ready scenarios for a dental healthtech and lab environment. They show the kinds of control issues Theom can identify, evidence, prioritize, and route into remediation workflows.

ID	Severity	Finding	Example Theom evidence	DPIA implication
HT-01	High	Cross-border dental case replica without transfer tag	An EU production case schema replicated into a US BI workspace contains patient identifiers, dentist account IDs, crown/bridge prescription fields, scan metadata, material selection, and turnaround timestamps. No SCC/TIA or adequacy tag is attached.	Articles 44-49 transfer review required; pause new replication until policy tagging and legal basis are validated.
HT-02	High	Unmasked scan and order data in non-production	A staging bucket contains unmasked intraoral scan files, crown margin notes, shade selections, and patient/dentist identifiers copied from production 142 days ago. Access includes contractor and QA roles with no recent business use.	Minimization and security-of-processing risk; delete stale extracts or mask/tokenize before non-production use.
HT-03	High	AI copilot retrieval overreach	Support copilot retrieval pulled patient name, scan preview, crown prescription details, dentist account context, remake reason, and billing status into 116 ticket-assist prompts in seven days. The support policy allowed order status but not clinical or design-file details.	Restrict retrieval index, enforce purpose-bound prompt policy, and log prompt/source/output evidence for review.
HT-04	High	CAD/CAM export service account privilege drift	A service account used for nightly design and milling exports holds 218 grants but exercised only three in 90 days. It can read patient identity tables, scan-file metadata, and production queues, and can write into a raw data lake zone.	Shrink-wrap service permissions, require network policy, rotate credentials, and alert on out-of-profile writes.
HT-05	High	Toxic ad hoc join for growth analytics	A notebook joined patient demographics, dentist account tier, procedure type, crown material, turnaround time, remake reason, support sentiment, and payment status into a growth cohort. Each dataset was approved separately, but the joined profile is materially higher risk.	Create toxic-combination rules and require privacy approval before persistent cohorts are exported.
HT-06	Medium-High	Scan and CAD metadata retention drift	STL/CAD metadata containing scanner serial, practice location, capture timestamp, restoration design markers, material selection, and patient linkage remained in cold storage 18 months beyond the 90-day derived-data retention policy.	Retain only clinical records with a valid basis; purge or aggregate derived metadata outside the retention window.
HT-07	High	Dormant admin with no MFA on case warehouse	A dormant administrator with no MFA retained access to high-criticality patient case, scan, order, and billing tables and logged in from a new country after 120 days of inactivity.	Disable or step-up verify dormant admins; require MFA and network controls for all high-privilege roles.
HT-08	Medium-High	Partner share exceeds minimum necessary	A material supplier and logistics partner share includes patient ZIP, dentist account, restoration type, shade, order timestamp, and shipping status where the partner only needs aggregate material demand and delivery-band information.	Replace row-level share with aggregate or purpose-limited feed and document partner purpose, retention, and onward-transfer controls.

Risk Assessment and Treatment

The inherent risk remains high because the processing combines special-category health data, scan and design files, dental lab production data, broad operational use, cross-border movement, non-human access, and AI retrieval. The residual-risk target assumes Theom findings are triaged through owners, tickets, and evidence-retention controls.

Risk area	Inherent	Theom controls	Target residual	Treatment
Cross-border transfer and residency	High	Location, lineage, access geography, and custom transfer rules.	Medium	Block untagged replicas; map region-to-country and transfer mechanism; require legal review for SCC/TIA tiers.
Non-production dental PHI and design-file exposure	High	Dark data, classification, copy lineage, effective access, and masking checks.	Medium	Mask or delete staging extracts; restrict contractor roles; enforce expiry for test data.
Least-privilege drift	High	Overprovisioned identities, role-path analysis, service-account flags, and actual-use windows.	Medium	Revoke unused grants; replace broad roles with purpose-bound groups; review service accounts monthly.
AI retrieval and toxic joins	High	Prompt/source/tool-call correlation, query monitoring, toxic-combination policy, and output review where available.	Medium-High	Restrict retrieval corpora; block toxic joins involving dental case data; require AI workflow registration and DPIA review.
Retention and erasure scope for scan/CAD data	Medium-High	Lineage, derived stores, cold storage age, data-owner tags, and policy violations.	Medium	Apply retention labels to scan/CAD files and derived data; produce erasure-scope lineage packs for DSAR workflows.
Audit evidence incompleteness	Medium	Policy violations, activity records, evidence exports, and review worklists.	Low-Medium	Define evidence retention, export cadence, owner attestations, and sign-off records.

Escalation threshold: Any finding combining dental PHI, scan/CAD files, external transfer, AI retrieval, or admin/service-account overreach should be routed as a priority privacy-security issue until the data owner and privacy counsel agree on treatment.

DPIA Evidence Pack

A formal DPIA should convert Theom telemetry into repeatable evidence artifacts. The pack below is designed as a practical checklist for privacy, security, and data governance teams.

Evidence artifact	What it should contain	Cadence
Inventory baseline	Asset export by environment, owner, criticality, sensitivity, region, dark/error state.	Weekly during assessment; monthly thereafter.
Classifier validation	Precision/recall sample for PHI, prescriptions, scan metadata, STL/CAD markers, crown and bridge order metadata, provider/customer identifiers, material/logistics fields, payment data, and custom dental entities.	At onboarding and after taxonomy changes.
Access review worklist	Users, roles, groups, service accounts, admins, overprovisioned grants, unused access, MFA/network posture.	Monthly for high-criticality dental PHI and case-data stores.
Activity and anomaly sample	Query events, exports, joins, login country/IP, failed attempts, anomalous queries, and privileged activity.	Continuous monitoring with weekly sample pack.
Lineage and minimization	Copies, clones, views, notebook outputs, production-to-non-production movement, derived datasets, and DSAR erasure scope.	Quarterly or after major pipeline changes.
AI data-use evidence	Registered AI apps, retrieval sources, prompts/tasks where available, tool calls, source data, outputs/actions, and policy violations.	Before launch and continuously for high-risk workflows.
Remediation ledger	Finding owner, ticket, severity, due date, status, validation evidence, and residual-risk acceptance.	Updated at least weekly during remediation.

90-Day Remediation Roadmap

Window	Actions	Theom evidence expected
Days 0-30	Connect priority environments; confirm dental PHI taxonomy; classify case intake, scan/CAD, production, billing, logistics, support, and partner stores; encode residency policy; remediate admins without MFA; freeze untagged cross-border case replication.	Inventory baseline, classifier validation, high-risk asset list, admin/MFA worklist, transfer-policy violations.
Days 31-60	Shrink-wrap CAD/CAM, ETL, and partner-export service accounts; delete or mask non-production dental PHI and design files; define toxic-combination policies; register AI workflows; route Theom findings into ticketing and incident response.	Overprovisioning reduction, service-account review, masking/retention exceptions, AI retrieval findings, remediation tickets.
Days 61-90	Produce DPIA evidence pack; run data-owner attestations; validate case, scan/CAD, production, billing, and partner lineage; test cross-border and AI incident playbooks; document residual-risk acceptance.	Signed owner reviews, lineage export, audit sample, incident tabletop notes, final residual-risk register.

Operating Cadence

Cadence	Review activity
Daily	Review critical policy violations for AI retrieval, external sharing, failed privileged access, and unapproved cross-region movement.
Weekly	Triage new high-criticality case, scan/CAD, billing, logistics, and support stores, new service-account grants, and anomalous query/export patterns.
Monthly	Run access shrink-wrap, admin/MFA review, service-account review, and data-owner attestation for dental PHI and case-data stores.
Quarterly	Refresh DPIA evidence pack, revalidate classifiers, assess transfer mechanisms, and review AI workflow purpose limits.

Appendix - Source Notes

Input	How it was used
Example operating model	Dental healthtech and full-service lab profile covering patient case intake, scan/design files, crown and bridge services, production workflows, logistics, billing, support, analytics, and AI-assisted operations.
Theom capability model	Frames technical evidence around data security posture, discovery and classification, access governance, activity monitoring, lineage, policy findings, and AI-aware data-use monitoring.
Evidence sources	Represents evidence categories that can be supplied by Theom, including inventory, identity and access paths, overprovisioning worklists, activity records, policy violations, and lineage exports.

Example boundary: No real patient, provider, practice, or lab-production data is represented in the example findings. Names, metrics, counts, timelines, and scenarios are illustrative and should be replaced with organization-specific Theom evidence before formal review.