

PRE-ENABLER

Introduction to the Interagency Architecture Paper

From a personal evidence-preservation tool to a sustainable, authorised national routing layer for safeguarding, investigation and post-death activation.

Core proposition

PRE-ENABLER should not become another isolated government database. It should become the persistent citizen-centred reference and authorised routing layer through which relevant evidence held across existing systems can be discovered, linked, preserved and acted upon when a lawful trigger occurs.

Introduction

PRE-ENABLER began as a simple accountability question: what happens when a person has credible evidence that serious harm may occur, but later dies or becomes unable to explain where that evidence is? The original answer was a structured form capable of preserving the person's frame, context, chronology, supporting material, alternative explanations, predicted risks and routes to independent verification.

That concept developed further once a second problem became clear. The evidence needed after a serious incident is rarely held in one place. A hospital may hold the clinical record; a police force may hold an incident log; a local authority may hold safeguarding material; a regulator may hold a complaint; a business may hold CCTV; a solicitor may hold an authenticated copy of the evidence package; and an independent witness may hold the missing factual link. The person at risk may be the only individual who understands how those records connect.

If that person is no longer available, investigators can lose not only a witness but also the map showing where the evidence is. PRE-ENABLER therefore evolved from an evidence-preservation form into a broader interagency architecture: a persistent reference capable of connecting distributed records without requiring every agency to surrender those records to a single central database.

1. From personal form to interagency infrastructure

The central architectural shift is from storing every item of evidence in one repository to preserving a trusted index of what exists, where it is held, how it can be verified, who may lawfully access it, and what event should cause it to be reconsidered.

A PRE-ENABLER record can therefore operate as a common evidential envelope across otherwise separate systems. A single PRE-ENABLER identifier could connect a person, organisations, events,

evidence items, external references and trigger conditions while allowing the authoritative source material to remain with the body that created or holds it.

Illustrative common reference language

Code	Meaning	Example use
P	Person	P-03 clinician / witness
O	Organisation	O-02 NHS trust / police force
EVT	Event	EVT-019 treatment, incident or decision
E	Evidence	E-027 video, document or record
REF	External reference	REF-008 policy, law or guidance
TRG	Trigger	TRG-004 defined future activation event

This does not require agencies to replace their own identifiers. It gives them a shared cross-reference. A police occurrence number, NHS record, safeguarding case and regulatory complaint can remain separate authoritative records while also being linked to the same PRE-ENABLER case.

2. A distributed network, not a universal data warehouse

The sustainable model is a distributed network. PRE-ENABLER should know that evidence exists and how an authorised body can obtain it; it should not automatically copy every medical, police, financial and safeguarding record into one uncontrolled repository.

That design follows existing UK information-governance principles. The Caldicott Principles require the minimum necessary confidential information to be used and access to be restricted on a strict need-to-know basis. Current College of Policing information-sharing guidance likewise recognises shared-platform models while requiring lawful, proportionate and purpose-specific disclosure.^{1 2}

The proposed division of responsibility

- Source agencies retain responsibility for their authoritative records.
- The PRE-ENABLER custodian maintains the persistent case identity, evidence index, trigger logic, provenance and access history.
- Authorised agencies receive only the evidence routes or material necessary for their lawful function.
- Every access, disclosure, update and activation is auditable.
- Contradictory or exculpatory material is preserved alongside incriminating material rather than filtered out.

This is better described as statutory custodianship than ownership. The custodian would hold the durable registry and governance responsibility, while the underlying records remain with the NHS body, police force, local authority, regulator, solicitor, company, witness or other lawful holder.

3. The death link changes the system from storage to activation

The decisive development is that PRE-ENABLER does not need to remain a passive archive. The UK already operates official death-registration data infrastructure capable of supporting a lawful activation mechanism. The General Register Office administers the Disclosure of Death Registration Information (DDRI) scheme, under which licensed organisations can receive a weekly electronic file of newly registered UK deaths for qualifying purposes connected with preventing, detecting, investigating or prosecuting offences. Most records are available in the weekly data within seven days of registration.^{3 4}

That existing mechanism demonstrates that a national PRE-ENABLER registry could, subject to an appropriate statutory basis and eligibility, be linked to an official death signal rather than relying solely on relatives, friends or individual professionals to remember that a PRE-ENABLER exists.

Conceptual activation sequence

Step	Function	Purpose
1	PRE-ENABLER registered	Identity, PE number, evidence index, trigger summary and custodian are recorded.
2	Official death signal received	A lawful death-data feed or equivalent service identifies a possible match.
3	Human verification	Identity and active status are checked; no allegation is automatically generated.
4	Trigger review	Relevant death/incapacity triggers and evidence routes are examined.
5	Authorised routing	The appropriate medical examiner, coroner, police, safeguarding body or regulator receives the necessary case key or evidence route.
6	Existing law takes over	The receiving body verifies evidence and exercises its own statutory powers and duties.
7	Audit returned	Receipt, access and action are logged against the PRE-ENABLER record.

4. Existing statutory systems already provide activation points

PRE-ENABLER would not need to invent an entirely new public-safety ecosystem. Existing UK systems already perform many of its component functions, but they do so separately.

The 2024 Medical Certificate of Cause of Death Regulations require attending practitioners to review relevant health records and other relevant information. Medical examiners must make whatever enquiries they consider necessary, take relevant information into account, keep records

of conclusions, and refer a death to the senior coroner where the applicable notification threshold is met.⁵ A PRE-ENABLER activation notice can therefore be designed to feed relevant pre-existing information into a process that already has legal duties to scrutinise death and escalate appropriate cases.

Adult safeguarding provides another existing pathway. Care Act statutory guidance states that local authorities must make enquiries, or cause others to do so, where they reasonably suspect that an adult meeting the safeguarding criteria is or is at risk of abuse or neglect. The guidance expressly contemplates formal multi-agency action.⁶

Multi-agency safeguarding and policing systems also demonstrate the operational value of shared information. College of Policing guidance notes that partnership working makes it possible to see the whole picture through earlier risk identification, improved information sharing, joint decision-making and coordinated action. More recent MASH automation work has focused specifically on speeding information exchange, reducing repetitive processing and increasing staff capacity for risk assessment.^{7 8}

5. Authorised access: the case key rather than universal visibility

The PRE-ENABLER architecture should not give every participating institution unrestricted access to every case. Instead, authorised institutions should receive an institutional credential or case-specific access key that reveals only the information required for their lawful role.

At policy level the implementation can remain technology-neutral. A “key” may eventually be implemented as a secure case token, role-based credential, API permission, cryptographic capability or another controlled mechanism. The principle is more important than the implementation: access must be authenticated, purpose-specific, minimal and logged.

Example

Agency	Likely access	Not automatically exposed
Medical examiner / coroner	Death trigger, relevant medical/care history, evidence routes, prior warnings	Unrelated financial or private material
Police	Events, witnesses, criminal evidence routes, preservation priorities, relevant prior reports	Unrelated clinical detail without lawful need
Safeguarding authority	Risk history, care context, relevant agencies, prior safeguarding evidence	Material unrelated to safeguarding function

This approach is consistent with existing police information-sharing guidance, which requires a clear purpose, proportionality, verification of the requester, and need-to-know controls, and which recognises that several organisations may make information available through a shared platform.²

6. A common communication layer can reduce duplication and missed risk

The potential efficiency gain is substantial. A person may currently have to reconstruct substantially the same story for a GP, hospital, police force, adult social care team, regulator, complaints body and solicitor. Each organisation creates another narrative. Dates may diverge, names may be recorded differently, case references become disconnected and later agencies may not know that earlier agencies already hold relevant information.

PRE-ENABLER provides a way to connect those records without pretending that one organisation owns the whole case. A discrepancy itself becomes visible evidence: if one agency records an event on one date, another records a different date, and the original video metadata supports one version, the shared evidential frame allows that inconsistency to be identified and resolved rather than perpetuated.

The benefit is not limited to building cases against suspected wrongdoing. The same network can expose evidence that clears a person or organisation. Because PRE-ENABLER explicitly preserves contradictory and exculpatory evidence, the interagency layer can prevent an outdated allegation from becoming more credible simply because the original witness is no longer available to explain that they later changed their view.

7. The proposed institutional role

The long-term proposal is therefore not that the death-registration authority itself should own every PRE-ENABLER record. The cleaner model is a dedicated statutory custodian or formally designated public body that receives or registers PRE-ENABLER records, maintains the persistent identifier, protects integrity, manages access, monitors activation signals and routes the case to the competent authority.

Its function would be deliberately narrow. It would not decide whether a crime occurred, whether medical treatment was negligent, whether an organisation was liable or whether somebody should be arrested. It would make sure that the right authority can discover the right evidential pathway at the right time.

Core functions of the custodian

- Register and authenticate PRE-ENABLER records and subsequent versions.
- Maintain a durable evidence index and pointers to distributed source records.
- Maintain trigger conditions and activation metadata.
- Receive lawful life-event signals, including death-registration matches where authorised.
- Verify identity before activation.
- Issue or validate authorised agency access.
- Route the minimum necessary information to competent bodies.
- Maintain a permanent audit of access, disclosure and activation.
- Preserve corrections and exculpatory evidence rather than silently overwriting history.

8. Why the architecture is sustainable

A sustainable PRE-ENABLER does not need to rebuild the NHS record, police database, adult-social-care system, coronial system or regulatory infrastructure. Those institutions already possess specialist records, powers and retention frameworks. PRE-ENABLER supplies the missing connective layer.

This keeps the system comparatively small. The registry needs to know enough to identify the person, identify the evidence, locate the evidence, identify lawful access routes, recognise defined triggers and prove what existed at a particular time. The source systems continue to do what they already do.

That architecture also makes future expansion possible. New agencies can join through a governed access model without redesigning the citizen's original evidence package. The PRE-ENABLER identifier remains constant while the network around it can evolve.

9. What this paper proposes

The accompanying interagency architecture paper should therefore treat PRE-ENABLER as three connected components rather than a single form or database:

- The Personal Evidence Framework - the citizen-facing record of frame, context, evidence, verification routes, alternative explanations, risks and triggers.
- The PRE-ENABLER Exchange Standard - the common reference structure through which participating bodies can identify and lawfully exchange relevant case information.
- The PRE-ENABLER Activation Service - the governed mechanism that detects a qualifying life event, verifies the match, determines which authority needs to know, and activates controlled access to the evidential route-map.

Together, these components turn PRE-ENABLER into more than a post-death safeguard. It becomes a citizen-originated interoperability framework capable of supporting prevention while the person is alive, continuity if they lose capacity, independent investigation if serious harm occurs, accountability where evidence establishes responsibility, and exoneration where the evidence points elsewhere.

The architectural principle

PRE-ENABLER should not replace the agencies that already hold evidence and exercise statutory powers. It should provide the persistent, authorised and auditable key that allows those agencies to discover how their separate pieces of information connect when prevention, safeguarding, investigation or death makes that connection necessary.

Selected official sources

1. National Data Guardian, The Caldicott Principles. [Official source](#)
2. College of Policing, Information sharing (Authorised Professional Practice; updated July 2026). [Official source](#)
3. HM Passport Office / General Register Office, Disclosure of death registration information. [Official source](#)
4. HM Passport Office / General Register Office, DDRI advice for applicants. [Official source](#)
5. The Medical Certificate of Cause of Death Regulations 2024. [Official source](#)
6. Department of Health and Social Care, Care and support statutory guidance - safeguarding. [Official source](#)
7. College of Policing, Partnership working and multi-agency responses/mechanisms. [Official source](#)
8. College of Policing, Robotic process automation in multi-agency safeguarding hubs (MASH). [Official source](#)

Status note: This introduction is a policy and architecture proposal. It identifies existing UK mechanisms that could support a PRE-ENABLER network, but it does not claim that a national PRE-ENABLER registry or statutory activation duty currently exists.