DrDoctor

DCB0129 — Clinical Safety Case Report

The DrDoctor Digital Health Platform

Published: 8 May 2026

Document owner: Joe Horne, Clinical Safety Officer

Executive Sponsor: Brigitte West

Version history

Version	Date approved	Changes	Approver
1.0	8 May 2026	Initial unified Clinical Safety Case Report for the DrDoctor digital health platform. Consolidates seven previous product-specific safety case reports (listed under Related Documents) into a single platform-level safety argument aligned to the Assuric hazard log and the current product set.	Brigitte West

Related documents

The documents listed below are legacy product-specific clinical safety reports retained for reference and audit purposes, available on request. The current clinical safety position is defined by this CSCR and the Hazard Logs maintained in Assuric, a clinical risk management platform purpose-built for DCB0129 and DCB0160 governance.

Title	Version
DrDoctor_DCB0129_CSCR_Auto Scheduling, Rescheduling, PIFU (Accessing Care)	1.1
DrDoctor_DCB0129_CSCR_CareHub	1
DrDoctor_DCB0129_CSCR_Co-ordinating Care	1
DrDoctor_DCB0129_CSCR_Data Led Care	1
DrDoctor_DCB0129_CSCR_LI	1

TE	
DrDoctor_DCB0129_CSCR_NHS App Integration	4.4
DrDoctor_DCB0129_CSCR_PEPCore	1.2

Contents

1. Introduction

2. The Assuric platform

3. System scope and product definition

4. Functional scope of the platform

5. Intended use and clinical boundaries

6. Clinical Risk Management System (CRMS)

7. Governance, roles, and oversight

8. Platform-wide safety controls

9. Clinical risk management process

10. Hazard Logs and safety case structure

11. Safety incidents, service issues, and learning

12. Third-party products, integrations, and data safety

13. Planned review and proactive assurance

14. Clinical risk control measures

15. Technical assurance

16. Configuration control and documentation management

17. Test issues and defect management

18. CSO safety statement (summary assurance)

Appendix 1 — Suggested considerations for provider deployment (DCB0160 support)

Appendix 2 — Clinical risk matrix

1. Introduction

DrDoctor is a modular digital health platform used by NHS and private healthcare providers to support patient engagement, appointment management, and administrative coordination across outpatient, elective, and hybrid care pathways. Functional capabilities are interoperable and may be deployed individually or in combination depending on local configuration, clinical context, and operational need. Further information is available at https://www.drdoctor.co.uk.

This Clinical Safety Case Report (CSCR) presents the safety argument for the platform and provides assurance that clinical risks associated with its design, development, deployment, and live operation have been systematically managed and reduced to As Low As Reasonably Practicable (ALARP) within the platform's intended use and stated clinical boundaries. It applies to the live production platform and reflects the current operational state of the system.

1.1 Definition of “provider”

Within this report, “provider” refers to NHS organisations (including Trusts and Foundation Trusts) and private healthcare organisations that deploy and operate the DrDoctor platform within their care pathways. The clinical safety responsibilities described under DCB0160 apply to all such providers and are managed locally as part of the provider’s own clinical risk management arrangements. Statements specific to NHS Trusts (for example deployment scale figures) are stated explicitly.

1.2 Scope and level of detail

This CSCR is a platform-level safety argument describing the Clinical Risk Management System (CRMS), governance, processes, and overall risk posture of the platform in accordance with DCB0129. It does not duplicate function-specific hazard detail.

Detailed, functionality-level hazards (for example those relating to Direct Messaging, Forms, or Scheduling) are maintained in the Hazard Log set in Assuric. The Hazard Logs are the authoritative and current record of identified hazards, controls, ownership, and residual risk, segmented by functional capability so that providers can review the hazards relevant to their configuration and apply appropriate local controls under DCB0160.

The absence of function-level hazard detail in this report is therefore not a lack of risk identification. It is a deliberate separation between the manufacturer’s safety argument and the detailed hazard records that underpin it, supporting robust version control, traceability, and proportionate assurance.

For support and access to the DrDoctor CSO, contact **support@drdoctor.co.uk**.

1.3 Purpose of this CSCR

This CSCR is intended to:

1. define the scope and intended use of the DrDoctor platform;
2. describe the clinical risk management arrangements applied throughout the system lifecycle;
3. summarise the hazard identification, evaluation, and control approach, and provide assurance that residual risks are acceptable (ALARP); and
4. support deploying providers in meeting their local responsibilities under DCB0160.

This document is not a user manual, configuration guide, or full technical specification. Operational guidance and onboarding support are provided separately by DrDoctor's Transformation Team.

2. The Assuric platform

2.1 What Assuric is

Deploying providers are provided with read-only Assuric access to DrDoctor's provider-facing clinical safety documentation. Assuric is the authoritative, version-controlled repository for:

1. this CSCR;
2. the Clinical Risk Management Plan (CRMP);
3. the Clinical Risk Management Policy and Procedure;
4. the Hazard Log set, segmented by functional capability; and
5. associated supporting evidence.

Providers use Assuric to review the platform-level safety argument and to self-serve from the full set of Hazard Logs, selecting those relevant to their deployed functionality. This approach avoids the need for DrDoctor to push or restrict logs as a provider's enabled functionality changes over time, and supports proportionate local assurance under DCB0160. Where a hazard relies on provider-owned controls (for example reconciliation processes, monitoring, or response SLAs), the dependency and ownership is stated in the Hazard Log to support local DCB0160 activity.

2.2 How to request access to Assuric

Users can request Assuric access through either:

1. the DrDoctor support desk at **support@drdoctor.co.uk**; or
2. the provider's nominated DrDoctor Transformation Team representative.

Either route arranges read-only access for nominated personnel, typically including the provider's Clinical Safety Officer, clinical safety leads, and project leads responsible for deployment.

2.3 Migration of safety artefacts to Assuric

Migration of clinical safety artefacts to Assuric was undertaken alongside a structured review of the hazard set as a whole. Hazard wording was refined for clarity and consistency, evidence was re-checked, and risk scoring was reviewed under the same matrix. As a result of this review, some risk scores changed, but no hazard moved into an unacceptable risk category requiring further controls or actions; the platform's residual risk profile remains acceptable and ALARP. The migration represents an improvement in documentation management, clarity, and traceability rather than a re-baseline of the safety case.

2.4 Where DrDoctor’s clinical safety documentation lives

Figure 1 shows the artefacts that underpin this CSCR, the systems they are held in, and how learning from incidents flows back into the safety case.

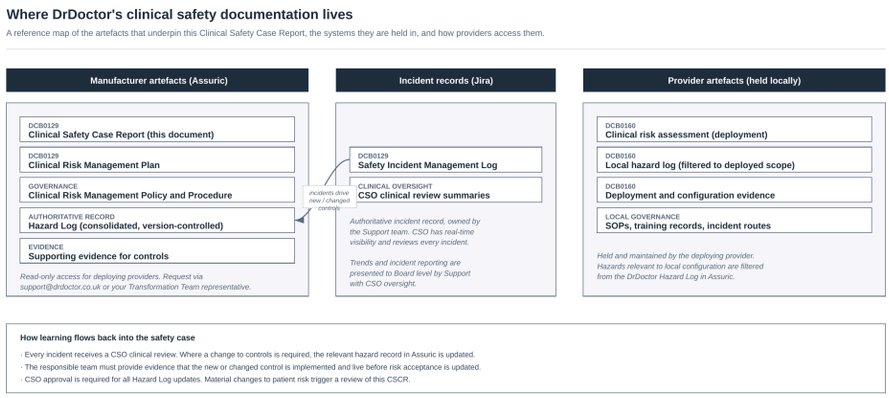

Figure 1 — Where DrDoctor’s clinical safety documentation lives. Manufacturer artefacts are held in Assuric; the Safety Incident Management Log is held in Jira and owned by the Support team; provider DCB0160 artefacts are held locally.

3. System scope and product definition

3.1 Platform definition (functionality-led)

For clinical safety compliance, DrDoctor is treated as a single Health IT platform comprising interoperable, configurable products that enable functional capabilities. This:

1. provides clear traceability of clinical risk to functional behaviour rather than commercial packaging;
2. supports consistent governance across a connected platform; and
3. avoids maintaining multiple overlapping safety cases as deployments and configurations change.

3.2 System identification and versioning approach

The platform is a live production system where individual functional capabilities are developed and released independently rather than as a single monolithic version. Each functional area follows a controlled release process, with Clinical Safety Officer (CSO) review applied where changes may affect clinical risk. This CSCR is therefore not tied to a single software build or platform version. The authoritative point-in-time snapshot of clinical risk is provided by the

Hazard Logs and evidence in Assuric, with version history and approvals captured under configuration control.

3.3 Deployment scale and clinical environment

DrDoctor is deployed across 70+ NHS Trusts, supporting 152 million appointments, with approximately 300,000 daily logins, serving 47+ million patients (May, 2026). Deployments vary by provider depending on enabled functionality, local configuration, and governance arrangements.

3.4 Scope statement

This CSCR covers all live DrDoctor platform functionality that falls within the scope of DCB0129, as represented in the Assuric platform. Agentic Voice, DrDoctor's AI-driven voice agent, is excluded and is governed by its own dedicated DCB0129 Clinical Safety Case Report due to the AI-specific nature of its hazards, controls, and evaluation requirements. Analytics-only digital tools are excluded where they do not meet DCB0129 applicability.

4. Functional scope of the platform

Each product associated with the functional areas described below has been assessed under the CRMS and is represented in the Hazard Logs. Figure 2 shows the products as they sit across a typical patient care pathway, together with the cross-cutting orchestration capabilities and the patient and staff access surfaces through which the platform is used.

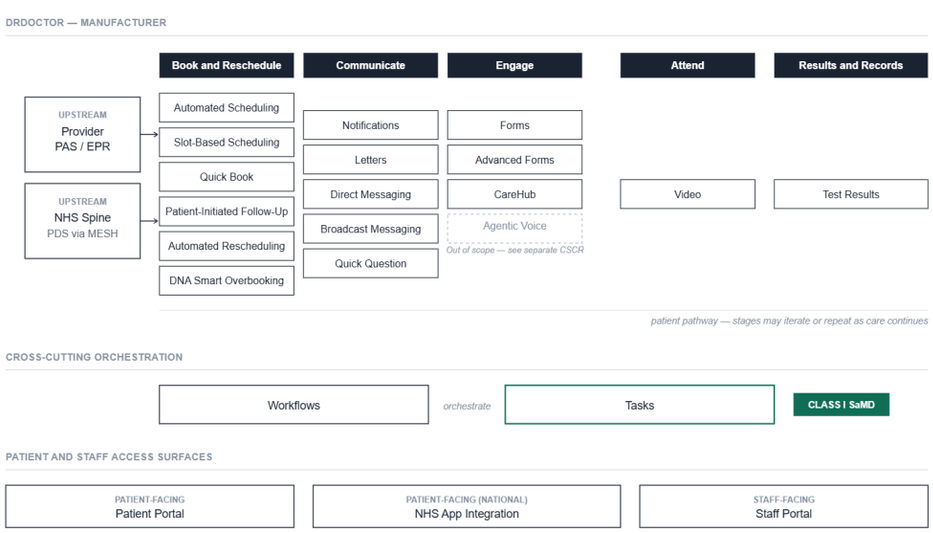

Figure 2 — The DrDoctor platform: patient care pathway and product ecosystem. Tasks is identified as a Class I Software as a Medical Device (see Section 5.3). Agentic Voice is shown for context with a dashed outline; it is out of scope of this CSCR and is governed by a separate

4.1 Functional areas and product descriptions

Functional area	Product	Description
Scheduling and capacity management	Automated Scheduling	Enables patients to book appointments from available clinic capacity in accordance with eligibility, timing, and pathway rules configured by the provider. Behaviour reflects local operational models and relies on upstream PAS / EPR data.
	Slot-Based Scheduling	Structures appointment availability into predefined time slots with associated capacity limits, eligibility criteria, and constraints. Behaviour is determined by local configuration and supports patient-facing and staff-mediated booking workflows.
	Quick Book	Enables healthcare teams to create clinic schedules and invite patients to self-book appointments directly, without requiring integration with PAS, EPR, or other source systems. Quick Book is typically used for pop-up clinics, walk-in services, or edge-case pathways outside the provider’s integrated booking environment. Patient-initiated cancellation, rescheduling, and pre-appointment reminders are not provided by default; these rely on local administrative processes or additional DrDoctor products where required.

	Patient-Initiated Follow-Up (PIFU)	Allows eligible patients to request or book follow-up appointments within defined criteria when clinically appropriate, rather than being routinely scheduled. PIFU workflows rely on local governance to define eligibility, review expectations, and response times.
	Automated Rescheduling	Allows patients to cancel or change existing appointments and select alternative slots within rules defined by the provider. Designed to reduce administrative burden while maintaining visibility of cancelled and rebooked activity.
	DNA Smart Overbooking	Supports controlled overbooking of appointment slots by combining DrDoctor's DNA prediction model with a statistics-led overbooking algorithm. The system recommends a number of overbooking slots and their placement within a clinic day; recommendations are presented to staff for review and applied within local governance and confidence thresholds. Predictive outputs are intended for administrative decision support only and do not trigger automated clinical actions.
Patient communications	Notifications	Sends appointment-related messages such as confirmations, reminders, and changes via SMS, email,

		and the NHS App (where enabled). Timing, content, and delivery channels are configurable by the provider.
	Letters	Delivers digital patient letters based on locally approved templates and administrative workflows. Letter generation and delivery rely on configuration and upstream data sources.
	Direct Messaging	Supports secure one-to-one messaging between healthcare teams and patients for administrative and pathway-related communication. Messages are asynchronous and subject to local governance, response expectations, and monitoring.
	Broadcast Messaging	Sends one-to-many, non-urgent messages to predefined patient cohorts for service updates, information sharing, or operational communication. Not intended for urgent or emergency use.
	Quick Question	Sends structured single-question messages to patient cohorts and captures responses without deploying a full digital form. Responses are presented for review and action according to locally defined workflows.
Digital forms and documents	Forms	Supports the assignment, completion, and management of patient questionnaires linked to appointments, pathways, or administrative processes. Responses may be reviewed

		by clinical or administrative staff as part of established workflows.
	Advanced Forms	Enables creation of configurable digital questionnaires with conditional logic, validation rules, and structured data capture. Form behaviour and content are defined locally and require appropriate governance and testing prior to use.
Virtual consultations	Video	Enables secure video consultations between patients and healthcare professionals to support scheduled virtual appointments.
Portals and interfaces	Patient Portal	Provides patients with secure access to appointments, messages, forms, letters, and related service information. Portal content and functionality depend on local configuration and enabled features.
	Staff Portal	Provides healthcare staff with access to configuration tools, operational workflows, patient interactions, and monitoring views. Access is controlled through role-based permissions.
	NHS App Integration	Surfaces selected DrDoctor appointments, messages, notifications, and documents within the NHS App where deployed. Availability and presentation are subject to national constraints and local configuration.
	NHS Spine Integration	Integrates the platform with

		the NHS Spine Personal Demographics Service (PDS) to support accurate patient identification and demographic data exchange via daily MESH transmission. The integration consumes PDS data to support patient matching, NHS number verification, and demographic accuracy across products that rely on identity and contact information. DrDoctor holds the supplier-level Technical Conformance Certificate for Spine connectivity; each deploying provider remains responsible for its own DCB0160 obligations and for the accuracy of source data transmitted to the integration.
Automation and coordination	Workflows	Enables configuration of rule-based automation linking events such as bookings, messages, forms, and tasks. Behaviour reflects locally defined logic and supports administrative coordination rather than clinical decision-making.
	Tasks	Enables creation, assignment, tracking, and completion of operational actions for staff, triggered manually or by defined system events. Tasks presents information and workflow context but does not interpret patient data or automate clinical decisions. Tasks is registered as a Class I Software as a Medical Device; see Section 5.3.

Patient health record	CareHub	Provides a patient-facing space for accessing service information, resources, and activity relevant to a patient's care pathway. Content and functionality are defined and governed by the provider.
	Test Results	Surfaces selected pathology results to patients within the Patient Portal once a release delay defined by the provider has elapsed, with SMS notification and an explanatory link to support patient understanding. A supporting view in the Staff Portal allows staff to see which results have been released and when, in support of local quality assurance and accreditation processes (e.g. ISO/UKAS). Test Results does not interpret clinical content; clinical assurance of upstream pathology data and configuration of release rules remain the responsibility of the provider.

5. Intended use and clinical boundaries

DrDoctor supports patient engagement, administrative efficiency, and pathway coordination across outpatient and elective care settings in NHS and private healthcare environments. The platform:

1. does not provide diagnosis or treatment recommendations;
2. does not automate clinical decision-making; and
3. does not remove clinical responsibility from healthcare professionals.

Where functionality surfaces patient-submitted information (for example Forms, Quick Question, messaging content), DrDoctor acts as a presentation and coordination layer. Interpretation, decision-making, and action remain the responsibility of appropriately trained professionals operating under local governance.

5.1 Non-urgent limitation

The platform is not intended for emergency care use. This limitation is enforced through a combination of system design choices (for example, asynchronous-only patient communications, no clinical triage in patient-facing forms, and explicit non-urgent positioning in product copy and onboarding), training and guidance to providers and patients, and contractual provisions establishing the non-urgent intended use. Detailed controls are described in Section 14.

5.2 Predictive functionality within DNA Smart Overbooking

DNA Smart Overbooking combines a DNA prediction model with a statistics-led overbooking algorithm to recommend a number of overbooking slots and their placement within a clinic day. The prediction component supports administrative prioritisation and overbooking decision support only. Outputs do not trigger automated clinical actions and remain subject to staff review.

The confidence threshold that controls the balance between utilisation gain and overrun risk is configured by the provider, reflecting the provider’s local risk appetite for clinic overrun. DrDoctor does not set or override this threshold; staff confirm each overbooking recommendation before any action is taken in the provider’s PAS.

The predictive component is designed to fail safely. If the underlying data feed is lost or interrupted, the system reverts to standard reminder behaviour rather than producing inaccurate predictions, and the overbooking recommendation is suppressed. Where predictive functionality is demonstrably low risk and non-clinical, formal AI safety frameworks are not applied disproportionately; the risk is addressed through the hazard and control model in the Hazard Logs.

5.3 Tasks — intended use and regulatory position

Tasks supports operational coordination by enabling authorised staff to create, assign, track, and complete tasks relating to administrative and pathway activity (for example, follow-up actions triggered by patient-submitted information or service events). Tasks presents relevant information and workflow context to support timely action, but it:

1. does not interpret patient data;
2. does not generate clinical conclusions;
3. does not classify clinical urgency; and
4. does not automate clinical decisions or actions.

Where Tasks is used within pathways that involve clinical review, all clinical judgement and decision-making remain the responsibility of appropriately trained professionals operating under local governance.

Regulatory position

Tasks is registered with the Medicines and Healthcare products Regulatory Agency (MHRA) as a Class I Software as a Medical Device (SaMD) under UK Medical Devices Regulations 2002 (as amended), classified in accordance with UK MDR Rule 11. DrDoctor is the legal manufacturer and is established in the United Kingdom; no UK Responsible Person is required, and no notified body involvement is required for Class I conformity assessment. The associated technical file and Declaration of Conformity are owned by the CSO and maintained as controlled regulatory records.

Tasks is the only product within the scope of this CSCR that is classified as a medical device. Product governance and change control processes maintain the defined intended purpose and prevent scope expansion into higher-risk clinical decision support functionality, which would trigger reclassification under UK MDR Rule 11.

6. Clinical Risk Management System (CRMS)

DrDoctor maintains a single Clinical Risk Management System (CRMS) that governs the identification, assessment, control, and ongoing management of clinical risk across the platform, in line with DCB0129. The CRMS is defined through:

1. a Clinical Risk Management Plan (CRMP);
2. a Clinical Risk Management Policy and Procedure; and
3. associated safety records and repositories, including the Hazard Logs, this CSCR, and the Safety Incident Management Log (maintained by the Support team in Jira).

These artefacts support both manufacturer obligations (DCB0129) and local provider obligations (DCB0160).

The CRMP describes the methodology by which the safety argument set out in this CSCR is constructed, maintained, and verified. It defines the scope of the CRMS, the roles and responsibilities of the CSO, Executive Sponsor, and supporting teams, the documentation set under configuration control, the activities applied across the product lifecycle (from discovery through to decommissioning), and the criteria by which residual risk is evaluated and accepted. Where the CSCR is the safety argument, the CRMP is the method behind it. The CRMP is held in Assuric and available on request, and is reviewed at material changes to the platform, the CRMS, or DCB0129 itself.

7. Governance, roles, and oversight

7.1 Clinical Safety Officer (CSO)

Overall responsibility for the operation of the CRMS sits with DrDoctor’s Clinical Safety Officer (CSO), Joe Horne. The CSO is a Registered Mental Health Nurse (NMC PIN 09E1340E, registered since 2010) and is a trained Clinical Safety Officer, having completed NHS Digital Clinical Risk Management training in May 2022. The CSO has held CSO-accountable roles since 2022 (previously at Health Call Solutions, currently at DrDoctor), maintains active continuous professional development in clinical safety — including annual attendance at the Clinical Safety in Practice Conference — and holds an MSc in Applied Health Research alongside qualifications in change management. The CSO has also completed the University of York Safe Adoption of AI into Healthcare programme. The CSO is responsible for:

1. ensuring clinical risks are identified, assessed, and controlled in line with DCB0129;
2. maintaining clinical safety documentation, including review and approval of Hazard Log updates;
3. providing clinical safety input across design, change, configuration, deployment, and live operation; and
4. confirming residual risks are acceptable prior to release.

7.2 Top management oversight

All Clinical Safety Case documentation, including this CSCR, is reviewed and approved by an Executive Sponsor, providing evidence of top-management oversight as required by DCB0129.

7.3 Competence and training

DrDoctor ensures personnel contributing to the safe design, deployment, and support of the platform are appropriately competent. New starters receive clinical safety awareness training, and ongoing role-specific safety training is provided for relevant teams (Product, Engineering, Support, Transformation, Delivery).

In addition to the CSO, DrDoctor employs other clinically-registered staff embedded across product, transformation, and delivery teams, several of whom have also completed full NHS Digital Clinical Risk Management training. This embedded clinical capability supports day-to-day safety judgement within product design, configuration decisions, and provider deployment, without dependence on a single CSO escalation route.

8. Platform-wide safety controls

Each DrDoctor product has its own defined hazards, risk assessments, and mitigations in the Hazard Logs. In addition, the foundational safety controls below apply consistently across the platform. They operate independently of any single feature and provide the baseline governance framework within which all products are deployed, ensuring systems are used appropriately, activity is traceable, access is proportionate, and vulnerable or dependent users are safeguarded.

8.1 Training and competency

Safe use of the platform relies on users understanding intended use, workflow boundaries, and local operational processes. A structured train-the-trainer model is used during onboarding and ongoing operation:

1. designated organisational “superusers” receive implementation training from DrDoctor;
2. knowledge is cascaded locally to operational and clinical teams;
3. scheduled onboarding sessions and product demonstrations are provided;
4. self-service guidance, help centre articles, and product playbooks are available; and
5. user access and training are coordinated through nominated provider leads.

Safety implication: promotes correct and consistent use of the system and reduces the likelihood of operational or configuration error.

8.2 Audit and traceability

Platform activity is auditable to support accountability, investigation, and assurance. Providers can directly view operational information within the Staff Portal, including patient communications history and delivery status, appointment and pathway activity, and system and integration status information.

DrDoctor also maintains secure backend audit logs that record:

1. staff authentication and access activity;
2. user actions and workflow events;
3. configuration and clinic changes (with user attribution and timestamps); and
4. technical execution and processing logs.

Detailed audit evidence can be provided on request to support incident investigation, governance review, or information governance enquiries.

Safety implication: enables traceability of actions, supports root cause analysis, and allows timely detection of abnormal behaviour or system failures.

8.3 Proxy and delegate access

DrDoctor does not provide a native shared or proxy portal account model. Each account represents a single patient identity and login; shared credentials and delegated record access are not supported. Where patients require support from carers or family members, this is managed through the provider’s existing consent and governance processes.

The platform supports configuration of alternative or secondary contact details (for example an additional mobile number or email address) so that communications such as reminders or booking links may be received by a carer on the patient’s behalf. This functions solely as a notification routing mechanism and does not provide authentication or access to patient information. Formal proxy or linked profile access provided through national services (such as the NHS App) operates outside DrDoctor and is governed through national identity and GP practice processes.

Safety implication: avoids risks associated with shared accounts or inappropriate disclosure while still enabling supported patients to receive communications.

8.4 Children and young people

Age, consent, and safeguarding arrangements for children and young people are managed locally by the deploying provider in line with national policy and safeguarding requirements. DrDoctor uses demographic and contact details supplied by the provider's source systems, sends communications according to locally recorded parent / guardian or young person contact information, and does not independently determine consent status or impose age-based access rules.

Where the NHS App or other national services are used, their nationally defined identity, proxy, and competency rules apply (including GP practice-managed proxy access and safeguarding considerations during adolescence). These arrangements sit outside the DrDoctor platform.

Safety implication: aligns system behaviour with established organisational and national safeguarding processes, avoiding conflicting or duplicate consent models.

9. Clinical risk management process

DrDoctor applies a consistent and repeatable clinical risk management process across all platform functionality, aligned to DCB0129.

9.1 Risk identification

Clinical hazards are identified through:

1. structured hazard workshops and "what-if" interrogation at discovery and build phases;
2. scheduled product reviews;
3. real-time oversight and follow-up learning from incidents and near-misses; and
4. service monitoring signals and customer feedback.

9.2 Risk evaluation

Each hazard is assessed for:

1. likelihood, considering technical reliability, human-factor dependencies, configuration complexity, and monitoring or fallback controls; and
2. severity, using a worst-case patient harm scenario relevant to typical outpatient and administrative care contexts.

Risk scoring follows DrDoctor's clinical risk matrix, derived from the NHS clinical risk model and reproduced in Appendix 2. Scoring is led by the CSO with appropriate subject-matter expert input.

9.3 Risk control (layered controls)

Controls are applied using a layered approach:

1. Health IT design controls (validation, RBAC, monitoring, audit, fallbacks);
2. training and guidance controls (onboarding, safe-use guidance, communications governance); and
3. operational and business process controls (including provider-owned controls where appropriate).

Only controls that are implemented and evidenced at release are relied upon for risk acceptance. Planned controls are tracked but not treated as active mitigations until evidenced.

9.4 Ongoing monitoring and continuous improvement

Clinical risks are reviewed and updated in response to product or configuration changes, incidents and near-misses, customer feedback, and emerging safety concerns identified through monitoring or audit. Additional hazard workshops are conducted for new or materially changed functionality where necessary.

9.5 Risk acceptance criteria

DrDoctor applies the following acceptance criteria to residual clinical risk, using the clinical risk matrix reproduced in Appendix 2:

1. hazards with a residual risk classification of 1 (Acceptable, no further action required) or 2 (Acceptable where cost of further reduction outweighs benefits gained or where further risk reduction is impractical) are accepted by the CSO without further escalation, where supporting evidence of implemented controls has been reviewed and approved;
2. hazards with a residual risk classification of 3 (Undesirable level of risk) require documented justification and explicit CSO sign-off prior to acceptance, including consideration of whether further controls can reasonably be applied to reduce the residual risk to an acceptable level;
3. hazards with a residual risk classification of 4 or 5 (Unacceptable level of risk) are not accepted. Either further controls must be applied to reduce the residual risk to an acceptable level, or the affected functionality is not released.

At the time of issue of this CSCR, no hazard in the Hazard Log set has a residual risk classification above 2. Where a future hazard is identified with a residual classification of 3 that cannot reasonably be reduced further, this will be explicitly called out in the next issue of this CSCR to ensure deploying providers are aware of any hazard not controlled to a level routinely accepted by DrDoctor.

Acceptance is recorded against each hazard in the Hazard Logs in Assuric, with the rationale captured under configuration control. Residual risk acceptance is reviewed when controls change, when incidents indicate that the residual risk profile may have shifted, or as part of the planned annual functional hazard completeness review described in Section 13.1.

10. Hazard Logs and safety case structure

10.1 Hazard Logs (authoritative record)

DrDoctor maintains the Hazard Logs under version control in Assuric, segmented by functional capability so that providers can self-serve the logs relevant to their deployment. The Hazard Logs are the authoritative record of:

1. hazards (Cause → Hazard → Effect → Harm);
2. controls (design, training, operational);
3. risk scoring and justification;
4. ownership (DrDoctor or provider); and
5. residual risk acceptance justifications.

This segmentation supports proportionate local assurance where a provider deploys only a subset of the platform. Each Hazard Log also provides DCB0160 considerations and transferred controls for each hazard.

10.2 Why the CSCR does not reproduce the hazard list

This CSCR presents the platform safety argument and governance approach at a defined point in time. The detailed hazard set is maintained in Assuric to ensure clear configuration control, an authoritative hazard record per functional capability, up-to-date control evidence, and the ability for providers to filter hazards to their deployed scope. This avoids maintaining multiple overlapping hazard lists across documents and supports robust version control.

Hazard Logs are developed collaboratively by the responsible product team and the CSO. Logs are only approved and published in Assuric once the CSO is satisfied that hazards, controls, evidence, and residual risk have been properly captured and reviewed; logs in development are not visible to providers.

11. Safety incidents, service issues, and learning

11.1 Safety Incident Management Log (authoritative record)

In line with DCB0129, DrDoctor maintains a Safety Incident Management Log to record the reporting, management, and resolution of safety incidents associated with the Health IT system. The authoritative incident record is maintained in Jira and owned by the Support team. Incidents are typically raised in Slack, logged and monitored via Jira, and post-mortems are documented in Jira. Trends and incident reporting are presented to the executive team via the Support function with CSO oversight.

11.2 Clinical safety involvement during incidents

The CSO has visibility and input into all incidents in real time and provides a clinical review summary following every incident. The CSO also produces a monthly company-wide brief providing organisational visibility of incidents, impact, learning, and the clinical safety work delivered.

11.3 Provider communication during incidents

Affected providers are informed via support channels during incident management, with follow-up communication once root cause and mitigations are understood and confirmed.

11.4 Incident learning and linkage to controls and hazards

DrDoctor does not maintain a running list of incidents in this CSCR. This supports robust version control of the safety argument while ensuring the time-sensitive incident record remains authoritative in Jira. Where an incident results in a requirement to create or change a control:

1. design controls are prioritised through the Product roadmap, with urgency in line with agreed SLAs; and / or
2. operational and process controls are prioritised through the Transformation roadmap.

The relevant hazard record in Assuric is updated to reflect the new or amended control, and the responsible team must provide evidence that the control has been implemented and is live. Hazard Log updates are reviewed and approved by the CSO. If a change materially affects patient risk, the safety case is reviewed and the Hazard Logs updated. In the unlikely event that a hazard is identified that presents an unacceptable risk that cannot be controlled, this will be documented in this report.

12. Third-party products, integrations, and data safety

The DrDoctor platform integrates with a range of third-party products and services. Some are clinically safety-relevant dependencies (where failure could contribute to delayed or missing patient communication); others are infrastructure-only dependencies. Third-party risks are assessed proportionately as part of clinical risk management, including consideration of foreseeable failure modes, detection mechanisms, fallbacks, and operational response.

Third-party dependencies with potential clinical safety relevance fall into the following categories:

1. SMS gateway providers, where failure could contribute to delayed or missing patient notifications;

2. email delivery providers, where failure could contribute to delayed or missing patient communication;
3. letter print and physical mail providers, where failure could contribute to delayed or undelivered patient correspondence;
4. cloud hosting and infrastructure providers, where failure could affect the availability of the platform as a whole;
5. identity and authentication providers, where failure could affect access to the Staff Portal or Patient Portal; and
6. other clinically-adjacent integrations (such as third-party patient health record platforms) where DrDoctor exchanges or surfaces data on behalf of the provider.

DrDoctor maintains contractual arrangements, supplier assurance documentation, and Data Processing Agreements (DPAs) with these suppliers as appropriate. Supplier-specific assurance detail can be provided on request via the support desk or the provider's Transformation Team representative.

DrDoctor integrates with provider PAS and EPR systems using standard interfaces where available and supports bespoke provider-specific integrations where required. PAS and EPR systems are upstream services that feed DrDoctor; DrDoctor does not control PAS / EPR configuration or source data quality, and responsibility for assessing upstream systems sits with the deploying provider under DCB0160. Data received from external systems is validated and monitored for completeness and timeliness where feasible.

13. Planned review and proactive assurance

13.1 Annual functional hazard completeness review

DrDoctor operates a planned annual review cycle for functional hazard coverage — the work that produced this issue of the CSCR (consolidating prior product-specific reports and refining the Hazard Log set) is itself an example of this cycle in action. To ensure the identified hazard set remains complete as the platform evolves, for each functional capability the responsible Product Manager and the CSO perform a structured review of:

1. intended use and live usage patterns;
2. functional changes over the preceding period; and
3. hazard completeness and relevance, including additional DrDoctor controls and provider-owned controls and assumptions.

The CSO reviews and approves any resulting updates under configuration control in Assuric. This planned review cycle supports a proactive clinical safety posture and aligns with the DCB0129 expectation for regular review of the clinical risk management process.

13.2 CSCR re-issue criteria

A new version of this CSCR is issued when:

1. substantial functionality is introduced to the platform that changes the risk profile;
2. a change materially affects patient risk beyond an acceptable level; or
3. DCB0129 (or associated national guidance) is updated requiring further information or assurance content.

Routine product changes, UX changes, and minor workflow adjustments are communicated via the product release note process. Where relevant, release notes include a CSO comment and guidance to receiving provider CSOs. Updating this CSCR for all changes is not proportionate; the decision to re-issue this report rests with the DrDoctor CSO.

14. Clinical risk control measures

Clinical risks are controlled through a layered control framework applied consistently across platform functionality, at three levels: Health IT design, training and guidance, and operational and business processes.

14.1 Health IT design controls

Design-level controls prevent, detect, and mitigate foreseeable safety risks, including:

1. Role-Based Access Control (RBAC) restricting configuration and operational actions to authorised users;
2. configuration validation and guardrails to reduce misconfiguration likelihood;
3. audit logging of user actions and system events to support traceability;
4. monitoring and alerting for integration failures and abnormal behaviour;
5. retry and fallback mechanisms to reduce the risk of silent failure;
6. multi-channel communication support (portal, SMS, email, NHS App where enabled) to avoid reliance on a single delivery method; and
7. in-product guidance and warnings where appropriate to reinforce safe use and boundaries.

The platform does not independently initiate diagnosis, treatment, or clinical escalation. Actions that may influence patient care require human initiation, review, or confirmation, within local governance arrangements.

14.2 Training and guidance controls

Training and guidance mitigate risks arising from human factors, local configuration, and operational interpretation, including:

1. structured onboarding delivered by the Transformation Team;
2. role-specific training and safe-use guidance aligned to deployed functionality;

3. governance of patient-facing content (templates, wording, and usage boundaries); and
4. explicit non-urgent positioning for relevant functionality.

14.3 Operational and business process controls (including provider-owned controls)

Certain risks are inherently dependent on local pathways and deployment configuration, and are controlled through shared or provider-owned measures, including:

1. local SOPs for configuration, reconciliation, monitoring, and escalation;
2. processes to maintain accurate demographics and contact details in source systems;
3. defined responsibilities for review and actioning of patient-submitted information within agreed timeframes; and
4. local business continuity arrangements for platform or supplier outages.

Where a hazard relies on local controls, this dependency is explicitly recorded in the Hazard Logs and ownership is assigned accordingly to support DCB0160 responsibilities.

15. Technical assurance

DrDoctor applies an organisation-wide engineering and assurance approach to ensure the platform operates reliably, securely, and safely within healthcare environments.

15.1 Development and testing

Platform functionality is subject to layered verification and validation activities, proportionate to risk and intended use, including:

1. peer-reviewed code changes with enforced branch protection;
2. automated testing covering unit, integration, and regression scenarios;
3. manual and scenario-based testing for functional changes and configuration variants;
4. end-to-end testing of integrations where applicable; and
5. pre-release validation in non-production environments.

Only changes that meet defined quality gates are promoted to live environments.

15.2 Deployment and change control

Platform changes are released using controlled deployment practices, including staged rollout and feature controls where appropriate. Changes that may have clinical safety implications are assessed under the CRMS with CSO involvement where relevant. Where changes introduce new or modified risks, the Hazard Logs are updated and supporting evidence reviewed prior to release.

15.3 Monitoring and incident response

Live services are monitored using logging, alerting, and health checks to provide visibility of system behaviour, integration health, and failure conditions. DrDoctor operates an incident management process with triage, investigation, root cause analysis, clinical safety review where relevant, and communication with affected providers. The authoritative Safety Incident Management Log is maintained by the Support team in Jira; learning that results in new or changed controls is reflected in the Hazard Logs with evidence required to demonstrate implementation and live operation.

15.4 Assurance scope

This technical assurance applies to the DrDoctor platform. Local configuration, deployment choices, and operational use remain the responsibility of deploying providers and must be assured under DCB0160.

15.5 Decommissioning and offboarding

DrDoctor manages decommissioning under the CRMS in two scenarios: provider offboarding (where a provider terminates or does not renew its contract) and functionality retirement (where a specific product or capability is withdrawn from the platform).

Provider offboarding follows a documented process owned by the Transformation and Client Offboarding Teams. Contractual obligations apply in every case:

1. all services cease within 48 hours of contract termination;
2. personal data is retained only until termination of the Call-Off Contract, unless retention is required by law;
3. where no legal retention obligation applies, personal data is anonymised within 30 days of the end of the contractual relationship.

Where DrDoctor retires functionality from the platform, the change is managed under the configuration and change control arrangements described in Sections 15.2 and 16, with appropriate provider notice and Hazard Log update where the change introduces a new or modified clinical risk.

16. Configuration control and documentation management

DrDoctor maintains formal configuration and change-control arrangements to ensure the ongoing safety and integrity of the platform and its clinical safety documentation:

1. system configuration is controlled through RBAC and supported by defined governance processes;
2. product and configuration changes follow structured change control, with CSO involvement

where changes may affect clinical risk;

3. clinical safety artefacts (CSCR, CRMP, Policy and Procedure, Hazard Logs, evidence) are maintained under version control within Assuric; and
4. evidence supporting controls is captured in Assuric where appropriate. Controls are not relied upon for risk acceptance until evidence has been reviewed and approved by the CSO.

17. Test issues and defect management

At the time of issue, there are no known outstanding test issues with a potential clinical safety impact.

Test issues are managed through DrDoctor's engineering quality processes. Defects identified during automated testing, manual testing, or pre-release validation are triaged for severity and prioritised in line with internal SLAs. Defects with potential clinical safety implications are escalated for clinical review.

Where engineering identifies testing issues that require clinical consideration, these are escalated via the incident reporting process and tagged for clinical review. This ensures potential safety concerns are assessed consistently under the CRMS with appropriate CSO oversight, and that any resulting hazard or control updates are reflected in Assuric.

18. CSO safety statement (summary assurance)

Based on the clinical risk management activities described in this CSCR, and the Hazard Logs maintained in the Assuric platform, I confirm that clinical hazards associated with the DrDoctor platform have been identified, assessed, and controlled in accordance with DCB0129. Residual risks are considered acceptable and ALARP within the platform's intended use and stated clinical boundaries. All manufacturer-owned hazards have been assessed at residual risk classifications of 1 or 2 (acceptable with no further action required, or acceptable where the cost of further reduction outweighs the benefit and further risk reduction is impractical).

The Hazard Logs maintained in Assuric are the authoritative record of hazards, controls, ownership, and residual risk. Safety incidents are managed through an established process, are clinically reviewed by the CSO for every incident, and are used to drive control improvements with evidence required to demonstrate implementation.

Joe Horne

Clinical Safety Officer, DrDoctor

Registered Mental Health Nurse (NMC PIN 09E1340E)

Appendix 1 — Suggested considerations for provider deployment (DCB0160 support)

Note: This is not an exhaustive list. It provides high-level recommendations to support

deploying providers in meeting their local responsibilities under DCB0160. Function- and hazard-specific considerations are documented within the Hazard Logs and should be reviewed in the Assuric platform.

Access to Assuric: providers can request read-only access to Assuric through either the DrDoctor support desk at **support@drdoctor.co.uk** or their nominated Transformation Team representative. The DrDoctor Transformation Team and Clinical Safety Officer can provide further guidance where required.

A1. Scheduling, capacity management, and follow-up

(Automated Scheduling, Slot-Based Scheduling, Quick Book, Automated Rescheduling, PIFU, DNA Smart Overbooking)

Governance and configuration

- Define SOPs governing booking rules, eligibility criteria, rescheduling windows, overbooking thresholds, and operational ownership.
- Ensure local clinical and operational sign-off of scheduling logic prior to go-live.
- For Quick Book deployments without integration, define local administrative processes for cancellation, rescheduling, and reminders, since these are not provided by default.

Data quality and PAS / EPR integration

- Maintain accurate demographics and appointment data in source systems.
- Nominate a named owner for integration oversight and incident response.

Manual oversight and fallback

- Maintain SOPs for worklist monitoring and responding to failed or incomplete bookings.
- Perform regular reconciliation to confirm that appointments, cancellations, and follow-up actions processed in DrDoctor are accurately reflected in PAS / EPR records.

PIFU-specific

1. Define eligibility, expiry, and review expectations in local SOPs.
2. Ensure staff are trained to action requests appropriately, including how completion states align to PAS / EPR updates.
3. Clearly communicate urgent-contact routes and monitor for misuse.

Predictive and overbooking outputs

1. Treat outputs as administrative decision support only.
2. Set the overbooking confidence threshold to reflect local risk appetite, with experienced staff review and outcome monitoring.

A2. Patient communications

(Notifications, Letters, Direct Messaging, Broadcast Messaging, Quick Question, Video)

1. Establish approval and review processes for all patient-facing templates.
2. Align messaging with provider policy and accessibility requirements.
3. Do not use messaging tools for urgent or emergency care pathways.

4. Monitor delivery failures and define follow-up ownership.
5. Maintain fallback communication routes and business continuity plans.
6. For Video consultations, clinicians retain discretion to convert to in-person consultation where clinically indicated, with local clinical governance defining when remote consultation is and is not appropriate.

A3. Digital forms, questionnaires, and documents

(Forms, Advanced Forms)

I. Define SOPs for designing, approving, testing, and deploying forms and questionnaires.
II. Ensure clinical review and smoke testing of logic prior to live use.
III. Define handling processes for responses where EPR write-back is not in place.
IV. Ensure staff responsibilities and timeframes for reviewing submissions are clear.

A4. Portals, interfaces, and NHS App integration

(Patient Portal, Staff Portal, NHS App Integration, NHS Spine Integration)

- Define support processes for access issues and identity verification.
- Maintain RBAC aligned to information governance requirements and local governance.
- Validate appointment naming and presentation to avoid patient confusion.
- Monitor feedback and delivery reports and escalate concerns through local governance.
- Maintain alternative communication channels (SMS, email, telephone, letter) to ensure continuity of patient communication during periods of Patient Portal unavailability, aligned with local business continuity arrangements.

NHS Spine Integration

i. Maintain accurate NHS numbers and patient demographics in source systems (PAS / EPR), and align local update processes with DrDoctor's daily MESH transmission.
ii. Resolve data quality discrepancies identified by DrDoctor through Spine reconciliation.
iii. Maintain non-digital fallback routes (e.g. postal correspondence, telephone contact) for patients affected by Spine integration failures, NHS number issues, or missing PDS responses.

A5. Automation, workflows, and tasks

(Workflows, Tasks)

- Map workflows and task logic to agreed pathways and define ownership.
- Require documented specification and sign-off prior to build and go-live.
- Restrict configuration access to trained and authorised users.
- Tasks is registered as a Class I Software as a Medical Device (see Section 5.3); local deployment under DCB0160 should reflect that Tasks supports operational coordination only and does not interpret patient data.
- For Tasks, implement local triage and prioritisation processes to ensure time-sensitive tasks are identified and actioned promptly, with task ownership and completion practices supervised through local audit.

- Maintain manual workarounds and alternative routes for time-sensitive activity during periods of Tasks unavailability.

A6. Patient health record and results

(CareHub, Test Results)

CareHub

A. Communicate how patient-reported data will be reviewed and used.

B. Ensure disclaimers and guidance are visible and aligned with provider policy.

C. Define review expectations, escalation routes, and SOPs for concerning content.

D. Govern publication and maintenance of patient-facing resources.

Test Results

- Define and approve the release delay for results made visible to patients, in line with local clinical and information governance policy.
- Ensure upstream pathology systems are clinically reviewed and released in line with local quality assurance and accreditation processes (e.g. ISO/UKAS) before results are available for patient release.
- Communicate clearly to patients what results will and will not be visible, and the routes available to patients with questions about a result.
- Monitor the Staff Portal audit view periodically to confirm release behaviour is operating as expected.

A7. Cross-cutting governance and assurance

a. Ensure local CSO review and sign-off of deployment.

b. Maintain incident reporting and escalation routes.

c. Review training regularly and ensure staff remain competent.

Appendix 2 — Clinical risk matrix

Clinical risk is defined as the combination of the severity of harm to a patient and the likelihood of occurrence of that harm. Under DCB0129, the following definitions and two-dimensional clinical risk matrix are used to combine hazard likelihood and severity to yield a measure of risk. The matrix and its associated definitions are held in Assuric and are applied consistently across all hazards in the Hazard Log set.

A2.1 Severity classification

Severity classification	Interpretation	Number of patients affected
Catastrophic	Death	Multiple
	Permanent life-changing incapacity and any condition for which the prognosis is death; permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Multiple
Major	Death	Single
	Permanent life-changing incapacity and any condition for which the prognosis is death; permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Single
	Severe injury or severe incapacity from which recovery is expected in the short term	Multiple
	Severe psychological trauma	Multiple

Considerable	Severe injury or severe incapacity from which recovery is expected in the short term	Single
	Severe psychological trauma	Single
	Minor injury or injuries from which recovery is not expected in the short term	Multiple
	Significant psychological trauma	Multiple
Significant	Minor injury or injuries from which recovery is not expected in the short term	Single
	Significant psychological trauma	Single
	Minor injury from which recovery is expected in the short term	Multiple
	Minor psychological upset; inconvenience	Multiple
Minor	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible consequence	Single

A2.2 Likelihood classification

Likelihood category	Interpretation
Very High	Certain or almost certain; highly likely to occur
High	Not certain but very possible; reasonably expected to occur in the majority of cases
Medium	Possible
Low	Could occur but in the great majority of occasions will not
Very Low	Negligible or nearly negligible possibility of occurring

A2.3 Risk matrix

Severity (across) and likelihood (down) combine to produce a risk classification on a 1–5 scale.

Likelihood \ Severity	Minor	Significant	Considerable	Major	Catastro
Very High	3	4	4	5	5
High	2	3	3	4	5
Medium	2	2	3	3	4
Low	1	2	2	3	4
Very Low	1	1	2	2	3

A2.4 Risk acceptability definitions

Classification	Definition
5	Unacceptable level of risk. Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level.
4	Unacceptable level of risk. Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level.
3	Undesirable level of risk. Attempts should be made to eliminate the hazard or implement control measures to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical.
2	Acceptable where cost of further reduction outweighs benefits gained or where further risk reduction is impractical.
1	Acceptable, no further action required.