UK Care Sector Cyber Risk Report

Insure24 domiciliary care insurance downloadable PDF

Downloadable PR asset linking ICO breach reporting, digital care records, rota systems and cyber insurance for domiciliary care providers.

Canonical URL

https://www.insure24.co.uk/domiciliary-care-insurance/resources/cyber-risk-report/

UK Care Sector Cyber Risk Report

Downloadable PR summary

This cyber risk report explains why cyber insurance is becoming a core domiciliary care cover. Home care providers now rely on rota platforms, digital care records, mobile devices, email, cloud storage and sometimes remote monitoring or family portals.

Cyber incidents in care are not only technical events. They can create missed visits, inaccessible care plans, exposed medical information, keysafe or access concerns, regulator notification, contract pressure and loss of family trust.

Care sector cyber risk scenarios

The scenarios below are designed for PR, board discussion and insurer evidence preparation.

Cyber scenario | Operational impact | Insurance evidence to prepare

- Rota system outage | Missed visits, manual scheduling, family complaints and continuity pressure. | Business continuity plan, offline rota process, backups and incident response records.
- Wrong-recipient email | Sensitive care notes, addresses, access information or medication prompts disclosed. | Email controls, breach log, staff training, notification process and cyber/data cover.
- Lost mobile device | Care records or login access exposed outside the office environment. | Device encryption, remote wipe, MFA, access controls and mobile-device policy.
- Ransomware or cloud-platform lockout | Care plans, medication records and visit logs unavailable. | Backups, recovery testing, supplier due diligence and cyber incident response plan.

PR findings

- Cyber risk in home care should be framed around service continuity as much as data protection.
- ICO breach-reporting rules make response speed and evidence critical after a data incident.
- Care providers should prepare cyber evidence before renewal: MFA, backups, device controls, staff training, supplier checks and incident response.

Suggested media angles

- Why a rota outage can become a care-delivery and insurance problem.
- The hidden data risk in home care: addresses, access notes and medication prompts.
- Why cyber insurance belongs in a domiciliary care insurance programme.

Sources used

- ICO data security incident trends: https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/
- Domiciliary care cyber insurance guide: /domiciliary-care-insurance/cyber-insurance/
- Domiciliary care data breach claim example: /domiciliary-care-insurance/claims/data-breach/
- UK Domiciliary Care Insurance Report 2026: /domiciliary-care-insurance/report/

Help Build The 2026 Domiciliary Care Insurance Survey

Take the survey

Insure24 is collecting anonymised input from UK domiciliary care providers on insurance costs paid, renewal pressure, claim concerns, staff numbers, cyber readiness, service mix and CQC status. The results will help turn this report into an original-source annual benchmark for care providers, journalists and AI search systems.

Take the domiciliary care insurance survey

- Share approximate premium bands rather than exact commercially sensitive figures.
- Tell us which claims or incidents concern your care business most.
- Help benchmark cyber readiness, workforce pressure and renewal evidence across the home care sector.

UK Care Sector Cyber Risk Report: Detailed Insurance Guide

Why uk care sector cyber risk report matters

UK Care Sector Cyber Risk Report needs its own page because domiciliary care insurance is rarely solved by a generic commercial policy. The provider is working in clients' homes, often with vulnerable people, mobile staff, sensitive records, medication routines, family expectations and regulator scrutiny. A useful insurance page therefore has to explain how this risk area changes the risk, what underwriters will ask and which evidence helps the provider obtain suitable terms.

The important point is to match the insurance conversation to the real operating model. A provider researching uk care sector cyber risk report may be a startup agency, a self-employed carer, a live-in care business, a multi-branch provider or a specialist service working with clients who have complex needs. The right answer depends on services delivered, staff arrangements, contracts, CQC status, claims history, training standards and whether the work includes personal care, medication support, manual handling, lone working or delegated healthcare tasks.

How the exposure usually arises

The exposure behind uk care sector cyber risk report usually starts with everyday care delivery. A carer may be entering a client's home, using a keysafe, checking medication prompts, helping with mobility, supporting washing or dressing, recording observations, travelling to another visit or escalating a change in the client's condition. Any weakness in care planning, supervision, communication or records can become important if a complaint or claim follows.

Domiciliary care is also sensitive because incidents are often judged with hindsight. A family may ask why a deterioration was not escalated. A commissioner may ask whether the provider followed the care plan. CQC may ask how the provider learned from the incident. An insurer may ask whether the relevant policy section has been notified in time and whether the evidence supports the provider's version of events.

- Client vulnerability, including age, dementia, disability, frailty, medication dependency, mobility limitations or complex health needs.
- The number of visits, carers, coordinators, branches, vehicles, contracts and subcontracted or agency arrangements involved.
- Whether the service includes personal care, medication support, manual handling, live-in care, overnight care, palliative support or complex care.
- The quality of records, including care plans, visit logs, medication administration records, risk assessments, training files and incident reports.
- The provider's ability to show timely escalation, family communication, complaints handling, safeguarding reporting and improvement action.

Which insurance covers may be relevant

UK Care Sector Cyber Risk Report may involve several policy sections rather than one obvious cover. Public liability can be relevant where a client, family member, visitor or third party alleges injury or property damage. Professional indemnity can be relevant where the allegation is about advice, care planning, judgement, supervision or failure to follow professional duties. Medical malpractice can be relevant where medication support, delegated healthcare tasks or care-related clinical decisions are

involved.
Employers' liability should be reviewed where staff may be injured through manual handling, slips and trips, lone working, stress, aggression, infection exposure or travel. Cyber insurance matters where records, rota systems, mobile devices, email or cloud care platforms are involved. Motor insurance matters where carers travel between visits, use personal cars for work or operate pool vehicles. Legal expenses and directors' and officers' insurance may help with disputes, investigations and management decisions, subject to policy wording.
- Check whether the policy wording includes the actual care activities being delivered.
- Confirm whether medication, clinical tasks, safeguarding allegations, abuse allegations and professional negligence are treated clearly.
- Review limits of indemnity against contracts, commissioner requirements and the severity of potential claims.
- Make sure business-use motor exposure is not assumed away because carers use their own vehicles.
- Consider cyber and legal expenses where the provider relies on digital systems and faces employment or regulatory pressure.

What insurers will usually ask

Underwriters assessing uk care sector cyber risk report will usually want more than turnover and staff numbers. They want to understand what care is being delivered, who receives it, how staff are recruited and trained, how managers supervise remote workers and how the provider proves that policies are followed in practice. The stronger the operational evidence, the easier it is to explain why the risk is controlled.
A provider should be ready to describe CQC registration status, regulated activities, inspection history, claims experience, safeguarding notifications, complaints, medication incidents, manual-handling incidents, staff turnover, use of agency staff, training matrix, DBS process, induction, supervision, spot checks, care-plan reviews and incident learning. If there has been a claim or adverse inspection finding, the renewal submission should explain what changed afterwards.
- Services delivered and excluded, including whether high-dependency or complex care is undertaken.
- Client groups supported and any concentration in dementia, palliative, children's, learning disability or mental health care.
- Medication, manual-handling, lone-worker, safeguarding, infection-control and missed-visit procedures.
- Training evidence, competency sign-off, refresher frequency, supervision notes and quality audits.
- Claims history, complaints trends, CQC actions, improvement plans and lessons learned.

Cost implications

The cost of insurance linked to uk care sector cyber risk report depends on the provider's scale and severity profile. A small provider with low-intensity support, clean claims history and strong documentation may be easier to place than a larger provider delivering complex care with rapid growth, high staff turnover or open regulatory concerns. Pricing also depends on limits, excesses, policy wording, retroactive dates and whether the market sees the service as specialist or high acuity.
Providers can often improve the pricing conversation by presenting evidence rather than relying on broad assurances. Training records, medication audits, electronic visit monitoring, safeguarding reviews, completed CQC actions, driver checks, cyber controls and incident learning all help explain why the provider deserves better terms. The aim is not to hide risk; it is to show that the risk is understood and controlled.

Claims examples and evidence

A claim involving uk care sector cyber risk report may start with a single incident but quickly involve several lines of evidence. The provider may need care notes, rota data, visit times, medication records, family correspondence, training evidence, risk assessments, supervision records, photographs, witness details, complaints notes and regulator communications. Missing records can be as damaging as the original event because they make the provider harder to defend.

Early notification is important. Providers should tell their broker or insurer when there is injury, an allegation of negligence, safeguarding concern, data incident, possible employment claim, motor accident, property damage or regulator involvement. Good claims handling is calm, evidenced and prompt. It protects the client first, then preserves the information needed to decide liability and coverage.

- What happened, when it happened and who was present.
- Which care plan, risk assessment, medication record or visit instruction applied.
- What immediate steps were taken for client safety, escalation and family communication.
- Which policy section may respond and whether the claim has been notified correctly.
- What changed afterwards to reduce the chance of a repeat incident.

Practical next steps for providers

Before arranging or renewing cover for uk care sector cyber risk report, providers should map the real service model against the insurance programme. That means checking not only whether a policy exists, but whether it matches the actual activities, contracts, client needs, staff structure, vehicle use, data systems and regulator position. The most expensive insurance gap is often the one nobody noticed because the business had changed gradually.

A useful review should end with a cleaner underwriting story: what the provider does, what it does not do, which covers are required, which limits are needed, what claims have occurred, what lessons were learned and which controls support safe delivery. That is the difference between a page that describes insurance and a page that helps a care provider make a better decision.

- Confirm service activities, client groups, staff numbers, turnover, payroll, contracts and CQC position.
- Review public liability, employers’ liability, professional indemnity, medical malpractice, cyber, legal expenses, business interruption and motor cover.
- Gather claims history, complaints, incident logs, safeguarding notifications and evidence of completed actions.
- Prepare training, DBS, supervision, medication, manual-handling, lone-worker and cyber-control evidence.
- Use the related domiciliary care pages to check adjacent exposures before requesting quotes.