SELF-ASSESSMENT

The Cybersecurity and Data Protection Self-Assessment

What this is	A fifty-item maturity self-assessment across ten domains, scored on a five-level scale that measures evidence rather than intention — with a harm classification that decides the remediation order, a board reporting page, and the reassessment cadence.
It assumes	You hold confidential records about people. You do not need an IT department, a security officer, or a budget to complete it.
Change before use	The retention periods, the notification obligations, and any domain that does not apply to how you operate. Those depend on what you hold and where — confirm them with your own counsel.

The problem this fixes

Organizations in this sector hold some of the most sensitive records that exist about private people: children, families, allegations, medical and behavioral histories, immigration status, the addresses of people who are hiding from someone. They hold them because a public agency requires them to. And they are, almost always, protecting those records with an arrangement nobody has ever written down, owned by whoever happened to set up the email.

The reason is not carelessness. It is that the question "are we secure?" has no answer. It is unanswerable in the same way "are we healthy?" is unanswerable — there is no threshold, no score, and no honest yes. So it gets asked at a board meeting, receives a reassuring answer from the person least able to give one, and is not asked again until something has already happened.

This document replaces that question with a different one that does have an answer: **for each of fifty specific things, can you produce the evidence, for a date somebody else picks?** That question is answerable today, by you, without hiring anyone. What it produces is not a security rating. It is a map of where your protection depends on a person remembering, ranked by what is lost if that person forgets.

> **WHAT THIS IS NOT — READ THIS BEFORE YOU SCORE ANYTHING**
>
> This is not an audit, and completing it does not make you audited. An audit is performed by an independent party who tests your evidence and can be held responsible for the opinion. This is you, scoring yourself, on your own honor. The two are not substitutes and should never be described to a board, a funder, an insurer, or a licensing authority as though they were.
>
> This is not a certification and it is not an accreditation. Nothing in this document confers any status on any organization. There is no passing score, no badge, and no level at which you may describe yourself as certified. The top of this scale means "you can prove it and someone checked" — not "you are approved."
>
> This is not a compliance determination. Scoring well here does not establish that you comply with any statute, regulation, contract, licensing standard, or funder requirement — including any that govern health, education, or child-welfare records. Which obligations apply to you depends on what data you

hold, who you hold it for, and where you operate. Confirm them with your own counsel.

This is not a penetration test, a vulnerability scan, or a technical review. It does not examine your systems. It examines whether your organization has decided who is responsible for what, written it down, and kept the record.

It is also not a purchasing list. Nothing in the ten domains requires you to buy a product. A meaningful number of the fifty items are satisfied by a document, a calendar entry, and a named person.

The five levels

One scale, applied to all fifty items. The levels are deliberately about **evidence and independence**, not about sophistication — a small organization with a written procedure, a named owner, and a folder of dated records scores higher than a large one with expensive software nobody administers.

Level	Name	What it means	The test
0	Absent	It is not happening, and nobody in the organization would claim otherwise.	You cannot name anyone who does it.
1	Ad hoc	It happens when a particular person thinks of it. It is not written down, has no stated frequency, and would stop if that person left.	You can name the person but not the procedure.
2	Defined	It is written down, a named individual owns it, and a frequency is stated. Whether it is actually being done on that frequency is a separate question.	You can produce the document that says who and how often.
3	Operating	It is being done on the stated frequency, and each occurrence leaves a dated record.	You can produce the last three records without preparing them first.
4	Evidenced and checked	Everything at level 3, plus: someone who does not perform the work verifies it at least annually and records what they found — including when they found nothing wrong.	Someone else picks a date; you produce that date's record within a few minutes; and you can show the last independent check.

Level 4 is the top of this scale and it is not a certification. It says one thing: that the control leaves evidence, and that a second pair of eyes looks at the evidence on a cadence. That is the highest claim any organization can make about itself without an independent auditor, and it is a strong one. It is not the same as being certified against a standard, and it must never be presented as though it were.

Five rules for scoring, which matter more than the questions

1. **Score the evidence, not the intention.** "We do that" is a level 1 answer unless it is followed by a document. The most common failure of every self-assessment ever written is that people score what they meant to build.
2. **Two people score, and one of them must not operate the control.** The person who runs the backups cannot be the only person who scores the backups. If your organization is small enough that this is impossible for a domain, use a board member, and write down that you did.

3. **Score the organization as it is on the day.** Not as it will be when the project finishes, the contract is signed, or the new person starts. If it is not true this morning, it is not the score.
4. **Do not average a zero away.** A domain with four 4s and one 0 is not a domain at 3.2. It is a domain with a hole in it. The workbook reports the lowest item in each domain alongside the average, on purpose, and the lowest score is the one that goes to the board.
5. **Write the evidence reference next to every score above 1.** The folder, the file name, the calendar series, the ticket queue. An assessment with no evidence column is an opinion survey, and it will not survive its first contact with a real incident.

The harm classification — and why there are no weightings

Maturity models usually weight their domains, which requires asserting that one domain is worth 1.4 times another. That number is always invented, and once it is in a spreadsheet it stops being questioned. This assessment does not weight anything. Instead, every one of the fifty items carries a **harm class**, which describes what is actually lost when that item fails. The harm class does not change the score. It decides the order in which you fix things.

Class	What a failure here does	What it means for sequencing
A — Confidentiality of the people you serve	Records about children, families, or clients are exposed, altered, or lost. The harm lands on people who did not choose to be in your files and cannot undo it.	Fix first, always, regardless of score, cost, or how recently anything went wrong. A class A item at level 0 or 1 outranks every other finding in the assessment.
B — Continuity of service	You cannot operate. Staff cannot reach records, placements cannot be supported, payroll cannot run, the on-call phone does not work.	Fix second. These are the items that turn a bad week into a closure.
C — Money, contracts, and standing	Funds are diverted, a contract obligation is missed, a monitoring visit produces a finding, an insurer asks a question you cannot answer.	Fix third — genuinely important, and still behind A and B.

The sequencing rule is deliberately blunt because the alternative is worse. Left to itself, remediation gravitates toward whatever is cheapest, most visible, or most interesting to the person doing it. Harm class puts the records of the people you serve at the front and keeps them there.

The ten domains and the fifty items

Each domain lists its items, the harm class, and — where the distinction is easily got wrong — what specifically separates a 3 from a 4. Score every item on the 0–4 scale. Items that genuinely do not apply are marked N/A with a written reason; an item is not N/A because it is hard.

Domain 1 — What you hold, and where it is

This domain is first because every other domain depends on it. You cannot protect, retain, restore, or report on records you have not listed. In this sector the list is unusually hard to make, because sensitive records escape the case management system constantly and legitimately: a home visit becomes photographs on a personal phone, a court report becomes an email attachment, a reference check becomes a note in someone's drafts folder.

#	Item	Class	What separates 3 from 4
1.1	A written inventory of every system, application, and repository that holds confidential information about people you serve, staff, or applicants — including spreadsheets, shared drives, and mailboxes.	A	Someone who does not maintain it reviews it annually and looks for what is missing, not just whether what is listed is still true.
1.2	Each record type is classified by sensitivity, with a written definition of each class that a new employee could apply without asking.	A	The classifications are visible where the records are, not only in the policy.
1.3	It is written down which records may leave the primary system, in what form, and to whom — covering email attachments, printed copies, and mobile devices.	A	Exceptions are logged and reviewed, rather than tolerated silently.
1.4	Photographs, recordings, and images of the people you serve are governed by the same rules as written records, including where they live on personal devices.	A	There is a check that finds them, not only a rule that forbids them.
1.5	The inventory records who the data belongs to, which contract or license requires you to hold it, and the retention clock that starts when service ends.	C	The retention clock is linked to the destruction schedule in domain 9 rather than sitting on its own.

Domain 2 — Who can reach it

Access is where the largest gap between belief and reality usually sits, and it is almost never the result of a decision. It is the accumulated residue of people changing roles, covering for each other, and being given "temporary" access during a crisis that nobody remembered to remove.

#	Item	Class	What separates 3 from 4
2.1	Every person has their own named account. No shared logins for any system holding confidential records, including the ones vendors set up for you.	A	A periodic search actively looks for shared accounts rather than relying on the policy.
2.2	Multi-factor authentication is required on email, remote access, and every system holding confidential records.	A	Coverage is verified against the staff roster, not assumed from the setting being switched on.
2.3	Access is granted by role, and the roles are written down. Nobody has administrative rights because it was easier at the time.	A	Administrative accounts are listed by name and re-justified in writing each year.
2.4	A documented joiner–mover–leaver procedure, with access removed the same day someone separates.	A	The removal is evidenced per departure and reconciled against the payroll leaver list, so a departure that skipped the process is visible.
2.5	Access is reviewed on a stated cadence by the manager who owns the records, not by whoever administers the system.	A	The reviewer signs the list, including the entries they removed.

THE ITEM MOST OFTEN SCORED TOO GENEROUSLY

Item 2.4 is the one to be hardest on. Almost every organization has a separation checklist; considerably fewer can produce, for the last five people who left, dated evidence that each system was actually closed. The Open Shelf separation and access-termination checklist exists for exactly this item, and it is deliberately built to leave a record rather than to be ticked.

Domain 3 — The devices the work happens on

Human-services work is mobile by nature. Records travel to homes, courts, hospitals, and schools, on laptops and phones that are frequently personal property. This domain is not about banning that — it is about knowing which devices carry confidential records and what happens when one of them is left on a train.

#	Item	Class	What separates 3 from 4
3.1	A list of every device used for work that can reach confidential records, including personally-owned phones and home computers.	A	The list is reconciled against the staff roster rather than being self-declared once at hire.
3.2	Whole-disk encryption on every laptop and mobile device on that list, with the enabled state verified rather than assumed.	A	Verification produces a dated report per device, not a policy statement.
3.3	A written rule for personally-owned devices covering what may be stored on them, and a means of removing organizational data when someone leaves.	A	The removal has been performed and evidenced at least once, so it is known to work.
3.4	Screen lock and automatic timeout enforced on every device that leaves the office.	B	Enforced by configuration rather than requested by policy.
3.5	A stated procedure for a lost or stolen device, including who is told, within what time, and what is done remotely.	A	The procedure has been exercised, at least as a walkthrough, and the walkthrough is recorded.

Domain 4 — Everyone else who touches your data

Most organizations in this sector hold far less of their own data than they think. The case management system is a vendor. The email is a vendor. The payroll, the background checks, the training platform, the file storage, the accountant's portal — all vendors, most of them with subcontractors of their own. Your obligations do not transfer with the data.

#	Item	Class	What separates 3 from 4
4.1	A vendor list that records, for each one, what confidential data they hold or can reach.	A	Reconciled annually against accounts payable, which is where the vendors nobody registered are found.
4.2	A written agreement with every vendor holding confidential records, addressing permitted use, security obligations, breach notification to you, and return or destruction at termination.	A	The agreements are held centrally with their expiry dates, rather than being locatable in principle.

#	Item	Class	What separates 3 from 4
4.3	You know, for each significant vendor, whether they use subcontractors who can reach your data, and where the data is stored.	C	Recorded rather than believed; refreshed when the vendor changes terms.
4.4	Some form of assurance is obtained from significant vendors on a cadence — an independent report, a completed questionnaire, or a documented conversation with a dated record.	C	Findings are read and acted on, with a record of what was decided, rather than filed on receipt.
4.5	A stated exit position for each significant vendor: how you would get your records out, in what format, and how long it would take.	B	It has been tested with an actual export at least once.

Domain 5 — Whether you could get it back

The single most consequential distinction in this entire document is between a backup and a restore. A backup is a job that reports success. A restore is a file, opened, containing what it should. Organizations discover the difference on the worst day of their operating year, and the discovery is not recoverable.

#	Item	Class	What separates 3 from 4
5.1	Every system in the domain 1 inventory has a stated backup arrangement, including the ones the vendor operates on your behalf.	B	The vendor's actual commitment is on paper, not inferred from a marketing page.
5.2	A written recovery time objective and recovery point objective per system — how long you could be without it, and how much recent work you could afford to lose.	B	The objectives were set by the people who run the service, not by whoever configured the backup.
5.3	Backups are held so that a single compromised administrator account cannot destroy both the live data and the backups.	B	The separation is verified rather than assumed from the product description.
5.4	**A restore is actually performed on a stated cadence, and the restored data is opened and checked by someone who knows what it should contain.**	B	The test names the file restored, the date it came from, who checked it, and how long the whole thing took.
5.5	The restore procedure is written down well enough that someone other than its usual owner could follow it under pressure.	B	It has been followed by that other person at least once.

> **IF YOU FIX ONE THING AFTER THIS ASSESSMENT**
>
> Make item 5.4 real. Not a policy that says restores are tested — an actual restore, of an actual file, from an actual backup, opened by an actual person who can tell whether the contents are right, with the date and the elapsed time written down. It is the cheapest item in this document and it is the one that most often turns out to have been imaginary.

Domain 6 — The way you will actually be attacked

The realistic threat to an organization of this size is not a sophisticated intrusion. It is a convincing message. Someone impersonates the executive director and asks the bookkeeper to move money. Someone impersonates a vendor and sends new bank details. Someone sends a staff member a login page that looks exactly right. These are not technology failures — they are process failures, and the defense is a rule that survives being told the matter is urgent.

#	Item	Class	What separates 3 from 4
6.1	A written rule requiring out-of-band verification before any change to payment details or any unusual payment, by a call to a number already on file — never a number in the message.	C	It has held at least once against real pressure, and that is recorded.
6.2	The rule explicitly cannot be waived by seniority or urgency, and staff have been told, in those words, that they will not be criticized for applying it to the chief executive.	C	Leadership has restated it since the last staffing change.
6.3	Staff receive practical training on recognizing and reporting suspicious messages, at induction and on a stated cadence afterwards.	A	Completion is tracked against the roster and the content is refreshed rather than repeated.
6.4	A named, easy way to report a suspected message, and a stated expectation that reporting a false alarm is a good outcome.	A	Reports are logged, and the log shows people reporting things that turned out to be harmless.
6.5	Technical controls on email — such as filtering and external-sender marking — are configured and someone knows who owns them.	C	The configuration is reviewed rather than left as the vendor default.

Domain 7 — Whether you would notice

Detection is where small organizations most reasonably score low, and where the honest answer is often "we would find out when a person told us." That is a legitimate position, but it should be a decision rather than an accident, and it should be stated to the board in those words.

#	Item	Class	What separates 3 from 4
7.1	Logging is switched on for the systems in the domain 1 inventory, and you know how long logs are kept.	B	The retention period is deliberate and long enough to investigate something discovered weeks later.
7.2	Someone is responsible for noticing security alerts from your systems and vendors, and it is written down who.	B	The responsibility has a named alternate for absence.
7.3	Administrative actions in systems holding confidential records are logged and reviewable.	A	Reviewed on a cadence by someone who is not the administrator.
7.4	Failed and unusual sign-in activity is visible to someone, on some cadence, even if only monthly.	B	The review leaves a record, including the months where nothing was found.
7.5	If you have decided not to monitor something, that decision is written down, with the reason and who accepted the risk.	C	The acceptance is at board or executive level, dated, and revisited annually.

Domain 8 — What happens in the first four hours

This domain assesses readiness, not response quality — you cannot score how well you handle an incident you have not had. What you can score is whether the first four hours would be spent acting or improvising. The Open Shelf incident response plan and tabletop is the companion to this domain.

#	Item	Class	What separates 3 from 4
8.1	A written incident response plan naming who is called, in what order, and who decides.	B	It names people and alternates with contact details that were checked this year.
8.2	The plan states what must be preserved and what must not be switched off, so evidence survives the first hour.	B	The instruction is specific enough for a non-technical person to follow at 6am.
8.3	Your notification obligations are written down — who must be told, on what clock, under which contract, license, or statute — as confirmed by counsel rather than assembled from the internet.	A	They are reviewed when you take on a new contract or a new category of record.
8.4	A tabletop exercise has been run, with a record of what it revealed and what changed as a result.	B	Run at least annually, and each one starts by checking what the last one changed.
8.5	It is written down how you would operate without your primary systems for a stated period — the manual fallback.	B	The fallback has been walked through with the staff who would use it.

> **ON NOTIFICATION OBLIGATIONS SPECIFICALLY**
>
> Item 8.3 is the one place in this assessment where a wrong answer is expensive and a plausible-looking answer is dangerous. Notification duties vary by the category of record, the funder, the contract, the license, and the jurisdiction, and several may apply at once with different clocks. Do not populate this item from a template — including this one, which deliberately states no deadlines. Have your counsel write down the obligations that apply to your organization, and put that document behind this item.

Domain 9 — Keeping it only as long as you should

Retention is a security control, and it is the one most often missed, because holding records feels cautious. It is not. Every record you hold past its retention period is a record that can still be exposed and no longer serves any purpose. In this sector the periods are long and are set by other people — which is exactly why they have to be written down rather than remembered.

#	Item	Class	What separates 3 from 4
9.1	A written retention schedule covering each record type in the domain 1 inventory, with the source of each period cited.	C	Reviewed when contracts or licensing standards change, not only on a calendar.

#	Item	Class	What separates 3 from 4
9.2	Destruction actually happens when the period expires, and it is recorded — what, when, by whom, by what method.	A	The record would satisfy someone asking you to prove a specific file no longer exists.
9.3	A legal hold procedure that suspends destruction when litigation, an investigation, or a request is anticipated.	C	Holds are logged, tracked, and released deliberately rather than expiring by neglect.
9.4	The schedule covers backups, archives, and email — not only the primary system.	A	Verified against the actual backup retention rather than assumed to match policy.
9.5	Paper records are covered by the same schedule, including files held off site and in staff vehicles.	A	A physical check occurs on a cadence and is recorded.

Domain 10 — Who owns this at all

The final domain is governance, and it is the one that determines whether the other nine survive a staff change. Every organization has a point of failure here: the person who knows how everything is set up. This domain asks whether the organization would still know what it decided if that person left on Friday.

#	Item	Class	What separates 3 from 4
10.1	A named individual — not a department — is accountable for information protection, and their name appears in a document the board has seen.	A	The role has a written scope and a named deputy.
10.2	A written information security and data protection policy, approved at board level, with a review date that has not passed.	C	The review is substantive and recorded, not a re-adoption of the same text.
10.3	Every staff member and contractor has signed a confidentiality undertaking that covers the records of the people you serve, and the signatures can be produced.	A	Reconciled against the roster, so the people who never signed are visible.
10.4	The board receives a written report on information protection at a stated frequency, including this assessment's results and the open remediation queue.	C	The report names what has not been fixed and why, rather than only what has.
10.5	This assessment is repeated on a stated cadence, and the previous result is compared against the current one.	C	Movement is explained — including scores that went down because the last assessment was too generous.

Reading the result

The workbook produces four figures per domain and one for the organization: the average, the **lowest single item**, the count of items at 0 or 1, and the count of class A items at 0 or 1. Of these, the average is the least useful and the last is the most. Report all four; act on the last two.

Worked illustration — **invented figures, for shape only:**

Domain	Average	Lowest item	Items at 0–1	Class A items at 0–1
1 · What you hold	2.4	1	2	2
2 · Who can reach it	3.0	1	1	1
3 · Devices	1.8	0	3	3
4 · Vendors	2.2	1	2	1
5 · Recoverability	2.6	0	1	0
Organization	**2.4**	**0**	**9**	**7**

An organization reading only the left-hand column concludes it is at 2.4 and improving steadily. The column that matters is the right-hand one: seven items where a failure exposes the records of the people served are at level 0 or 1, and three of them sit in a single domain. That is the finding. "We scored 2.4" is not.

The four patterns worth recognizing

- **The flat middle.** Everything at 2, nothing at 0, nothing at 4. This means the organization has written policies and is not operating them. It is the most common pattern and the most misleading, because the documents make it look finished. The remedy is not more policy — it is picking the class A items and making each one leave a record.
- **The spike.** One domain at 4 and the rest at 1, almost always because one capable person owns that domain personally. This is a key-person risk wearing a security costume. The Open Shelf executive transition and key-person risk plan is the companion document, and the single-point-of-knowledge audit in it applies directly.
- **The technology floor.** High scores in domains 2, 3, and 7, low scores in 1, 9, and 10. The organization bought good tools and never decided who is responsible for what. Nothing further should be purchased until domain 10 is above 2.
- **The honest low.** Everything at 0 or 1, scored candidly. This is a better starting position than the flat middle, because nothing is being mistaken for finished. Take the class A items in order and expect the first reassessment to move very little — the early work builds the records that later scores depend on.

The remediation queue

The sequencing rule is mechanical, so that it survives the meeting where somebody argues for their own domain:

1. Every class A item at level 0 or 1, ordered by the cost of fixing it — cheapest first, so the queue starts moving.
2. Every class B item at level 0 or 1, same ordering.
3. Every class A or B item at level 2, which is where a written procedure needs to start producing evidence.
4. Every class C item at level 0 or 1.
5. Everything else, which is optimization and may be deferred without apology.

Two rules keep the queue honest. **First: no more than five items are in progress at once.** An organization that opens twenty simultaneous remediation items completes none of them and reassesses next year at the same level, with a longer list. **Second: each item has a named owner and a date, and the date is reported to**

the board whether or not it was met. An item without a date is not a plan; it is a wish with a number next to it.

Field	What goes in it
Item	The number from the assessment — 5.4, not "backups".
Current level and target level	Both. A target of 4 on every item is not a plan; most items should target 3.
Harm class	Carried across from the item. It is the reason this row is where it is in the queue.
What "done" looks like	The specific artifact that will exist. "A dated restore log with the last three tests in it" — not "improve backup process".
Owner	A person. Not a department, not a vendor, not "IT".
Target date	A date. Reported whether met or missed.
Cost and who approved it	Including zero, which is the correct entry for a meaningful share of the fifty items.

Cadence, and what to tell the board

Reassess annually, and additionally after any of: a change in the person accountable under item 10.1, a new system holding confidential records, a new contract carrying data obligations, or an actual incident. Reassessing more often than annually without one of those triggers produces movement that reflects who scored it rather than what changed.

The board report is one page and contains five things. It should not contain the fifty-item detail — that is the working paper, not the report.

1. The date, who scored it, and the name of the person who was not the operator of the controls they scored.
2. The count of class A items at level 0 or 1, this year and last year. This is the headline figure.
3. The three items currently in the remediation queue with owners and dates, and which dates were missed.
4. Anything the organization has consciously decided not to do, with the reason and the person who accepted that risk — item 7.5 in practice.
5. One sentence, in these words or their equivalent: **this is a self-assessment, not an audit, and it does not establish compliance with any legal or contractual obligation.**

The purpose of scoring yourself is not to find out how you are doing. It is to make a small number of specific things impossible to keep forgetting.

How to run it the first time

1. **Pick the two scorers before you look at the questions.** One who knows how things actually work, one who does not operate the controls. Agree in advance that a low score is a successful outcome of the exercise.
2. **Gather evidence before scoring, not during.** Half a day collecting the documents, logs, and lists first. Scoring while hunting produces generous scores, because the hunt is exhausting and 3 is easier than looking again.

3. **Score domain 1 completely before anything else.** If the inventory is at 0 or 1, expect the rest of the assessment to be less reliable than it looks, and say so in the board report.
4. **Score in one sitting per domain.** Splitting a domain across two sessions changes the standard between items.
5. **Write the evidence reference as you go.** If you leave it until the end, it will not be done, and the assessment loses most of its value the moment anyone asks a follow-up question.
6. **Do not fix anything while scoring.** Note it and move on. The queue is built afterwards, in harm-class order, or the fixing will follow interest rather than harm.
7. **Keep the completed workbook as a dated record.** Next year's value comes almost entirely from the comparison.

A first pass, done properly, takes most organizations a day of two people's time plus the half day of evidence gathering. That is the whole cost. If it is taking materially longer, the usual cause is that scoring turned into fixing.

Companion resources on the Open Shelf

- **Systems and vendor inventory** — the instrument behind domains 1 and 4. Build it first if item 1.1 scores below 2.
- **Separation and access-termination checklist** — item 2.4, in operable form.
- **Incident response plan and tabletop** — domain 8, including the exercise script for item 8.4.
- **The continuity of operations plan and tabletop** — items 5.2 and 8.5, and the wider question of operating without systems.
- **The executive transition and key-person risk plan** — the remedy for the spike pattern, and for domain 10 generally.
- **The enterprise risk register and board risk appetite statement** — where the risks you consciously accept under item 7.5 are recorded and reported.

All of them are free, require no registration, and are yours to adapt. None of them, individually or together, constitutes compliance with anything — they are working structures, and the obligations that bind your organization are confirmed by your own counsel, auditor, and licensing authority.

Published by The CARES Collaborative, a program of Knotts Family Services, Inc., for adaptation and use by charitable and community-serving organizations. No registration, no fee, no attribution required. This document is a working template, not legal, tax, or accounting advice — the requirements that apply to your organization are confirmed by your own counsel, auditor, and licensing authority. Version 1.0 · August 2026 · carescollaborative.org/open-shelf