Breach Notification Runbook (Public-Disclosable)

This runbook is the customer-facing and regulator-facing description of how Mabble Helix responds to a suspected or confirmed personal-data or PHI breach. It is the document referenced from the BAA (§4) and the DPA (§8). The internal operational runbook with hostnames, paging contacts, and forensic queries is at `mabble-runbooks/ir/ir-001-data-breach.md` and is not public.

This runbook does not replace the underlying contracts: where a BAA or DPA imposes a shorter timing or a stricter substantive obligation than the regulatory default, the contract prevails.

---

1. Definitions

Breach (HIPAA, 45 CFR §164.402) - the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

Personal data breach (GDPR Art. 4(12)) - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Discovery (HIPAA §164.404(a)(2)) - the first day on which the breach is known, or by exercising reasonable diligence would have been known, to Mabble (including any employee, officer, or agent of Mabble other than the person committing the breach).

Awareness (GDPR Art. 33(1)) - reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. The 72-hour clock starts when this threshold is met.

Notifiable incident - an incident that is reasonably likely, after the risk assessment in §3 below, to result in:

1. A use or disclosure of PHI compromising its security or privacy (HIPAA); or
2. A risk to the rights and freedoms of natural persons (GDPR); or
3. Triggering thresholds in any applicable US state notification statute.

Not every security incident is a notifiable breach. The §3 assessment governs.

---

2. Detection and triage

Step	Owner	Target time	Description

2.1	On-call engineer	T = 0	Incident detected via alerting (audit-log anomaly, R-P1.20 SLO breach, GuardDuty finding, customer report). On-call opens an incident in the incident-ticketing system and pages the Compliance Office.
2.2	On-call engineer	T + 15 min	Initial scoping: which tenants, which data categories, what timeframe. Audit log and Merkle-anchored evidence is preserved as forensic artefact (`internal/service/audit/...`).
2.3	Compliance Office	T + 1 h	Convene the Incident Response team: Mabble engineering, engineering lead, Compliance Office, legal. Internal classification preliminary (security incident / personal data event / notifiable breach).
2.4	Engineering lead	T + 2 h	Containment. Compromised credentials revoked via CAEP propagation (<=5 s). Affected tenant access frozen if required. Sub-processor notified if involved.
2.5	Compliance Office	T + 4 h	Forensic preservation. Audit-log range fixed via `audit_chain_snapshot` (R-P0.07). Sigstore Rekor anchor recorded for the snapshot. Backups frozen.
2.6	Compliance Office	T + 24 h	Risk assessment per §3 below. Notifiability determination.

The internal operational runbook at `mabble-runbooks/ir/ir-001-data-breach.md` contains the specific commands, dashboards, and contact rosters. The public-disclosable runbook reflects only the timing and the substantive obligations.

---

3. Risk assessment - is the incident notifiable?

The Compliance Office assesses notifiability against each applicable framework. The decision matrix is below; the assessment is documented and retained for at least 6 years (HIPAA §164.530(j)) and at

least the audit-log retention period (7 years).

3.1 HIPAA - the four-factor risk assessment (§164.402(2))

A use or disclosure of PHI is presumed a breach unless Mabble demonstrates a low probability of compromise based on:

Factor	Question
1	The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
2	The unauthorised person who used the PHI or to whom the disclosure was made.
3	Whether the PHI was actually acquired or viewed.
4	The extent to which the risk to the PHI has been mitigated.

If the four-factor analysis demonstrates a **low** probability of compromise, the incident is not a HIPAA breach. Otherwise the notifications in §4 are triggered.

3.2 GDPR - the Art. 33 / 34 thresholds

Threshold	Trigger
Art. 33(1) - supervisory authority notification	Any personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons.
Art. 34(1) - data subject communication	A personal data breach likely to result in a **high risk** to the rights and freedoms of natural persons.
Art. 34(3) - exceptions to data subject communication	Encryption such that the data is unintelligible to unauthorised persons (Art. 34(3)(a)); subsequent mitigation rendering the high risk no longer likely (b); disproportionate effort (c, public communication permitted instead).

For a Mabble breach where personal data was protected by AES-256-GCM with per-tenant DEKs and the DEKs were not compromised, Art. 34(3)(a) generally applies and direct data-subject communication may be substituted by a public communication. The Compliance Office documents the encryption status at the time of the incident.

3.3 US state law - common triggers

Mabble assesses state notification laws by reference to the data subjects' state of residence. The strictest applicable law is followed. Typical triggers include:

Element	Common state-law definition
Triggering data	Name plus SSN, driver-licence number, financial-account number with credentials, health information, biometric data - state-specific.

Encrypted-data safe harbour	Most states exempt encrypted data where the key is not also compromised - analogous to GDPR Art. 34(3)(a).
Timing	Typically "without unreasonable delay" or 30 / 45 / 60 / 90 days depending on state.
AG copy	California, New York, Massachusetts, Texas, and others require a copy of the consumer notice to the state AG above certain thresholds.

---

4. Notification obligations

4.1 Notification to customers (Mabble's Covered Entity or Controller counterparties)

HIPAA path (BAA) - Mabble commits in the BAA §4 to notify the Covered Entity without unreasonable delay and in no event later than **30 calendar days** from discovery. This is shorter than the HIPAA default of 60 days, which applies to a Covered Entity's notice to individuals (not Business Associate to Covered Entity). The 30-day window allows the Covered Entity to meet the §164.404 individual-notification deadline of 60 days from discovery.

GDPR path (DPA) - Mabble commits in the DPA §8 to notify the Controller without undue delay and in any event within **48 hours** of becoming aware. The 48-hour processor commitment is shorter than the 72-hour controller commitment to the supervisor under Art. 33(1) and is calibrated to leave the Controller time to assemble its own Art. 33 notification.

State-law path - where Mabble is the data holder for a state-law purpose, the relevant state's timing prevails.

The notification to the customer contains the elements required by §164.410(c) (HIPAA) and Art. 33(3) (GDPR), to the extent known at the time:

1. Identification of each individual whose unsecured PHI / personal data has been, or is reasonably believed by Mabble to have been, accessed, acquired, used, or disclosed.
2. A description of the nature of the breach, including the date of the breach and the date of discovery, if known.
3. The categories and approximate number of data subjects and records affected.
4. The likely consequences of the breach.
5. The measures taken or proposed to address the breach and mitigate its possible adverse effects.
6. Mabble's contact details (sales@mabble.ai).

Where information is not available at the time of initial notice, a phased notification is provided (Art. 33(4)) and supplemented as the investigation progresses.

4.2 Notification to supervisory authorities (where Mabble is acting as Controller)

In the limited cases where Mabble is the Controller (e.g., processing of Mabble employee data or Mabble's own marketing analytics), Mabble notifies the competent supervisory authority within **72 hours** of awareness under Art. 33(1). The lead supervisory authority is identified per Art. 56 and the EDPB Guidelines on Lead Supervisory Authority.

For HIPAA-covered breaches of 500 or more individuals where Mabble is itself the Covered Entity, Mabble notifies HHS Secretary contemporaneously with the individual notice under §164.408(b); for breaches affecting fewer than 500 individuals, Mabble logs the breach and submits an annual summary to HHS within 60 days after the end of the calendar year (§164.408(c)).

4.3 Notification to data subjects (Mabble acting as Processor)

Direct communication to data subjects is the **Controller's** responsibility under Art. 34. Mabble assists the Controller with content, timing, and channel as required by the DPA §7 / §8. Where Mabble has a direct relationship with the data subject (e.g., a Mabble employee), Mabble issues the communication directly per Art. 34, using the templates in §6 below.

4.4 Notification to media and HHS - HIPAA Covered Entity scenario

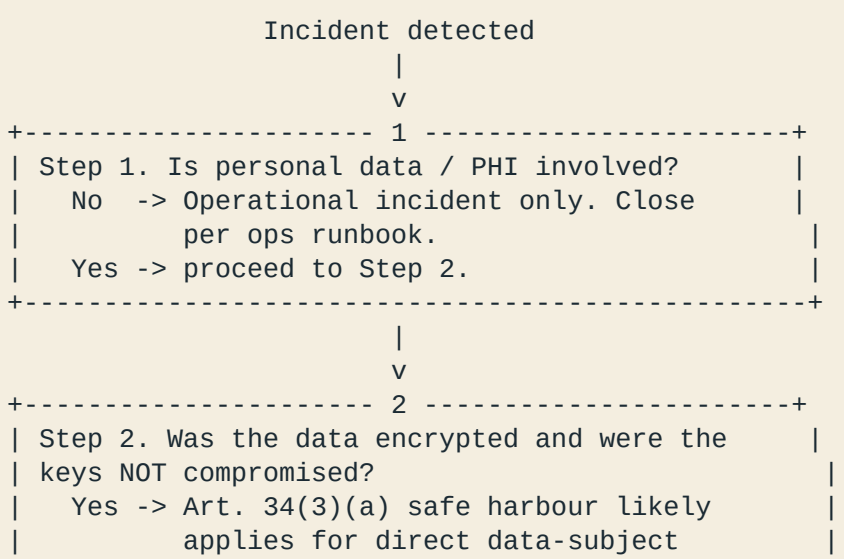
Where the underlying Covered Entity is a Mabble customer and the breach affects 500+ residents of a single State or jurisdiction, the Covered Entity (not Mabble) issues:

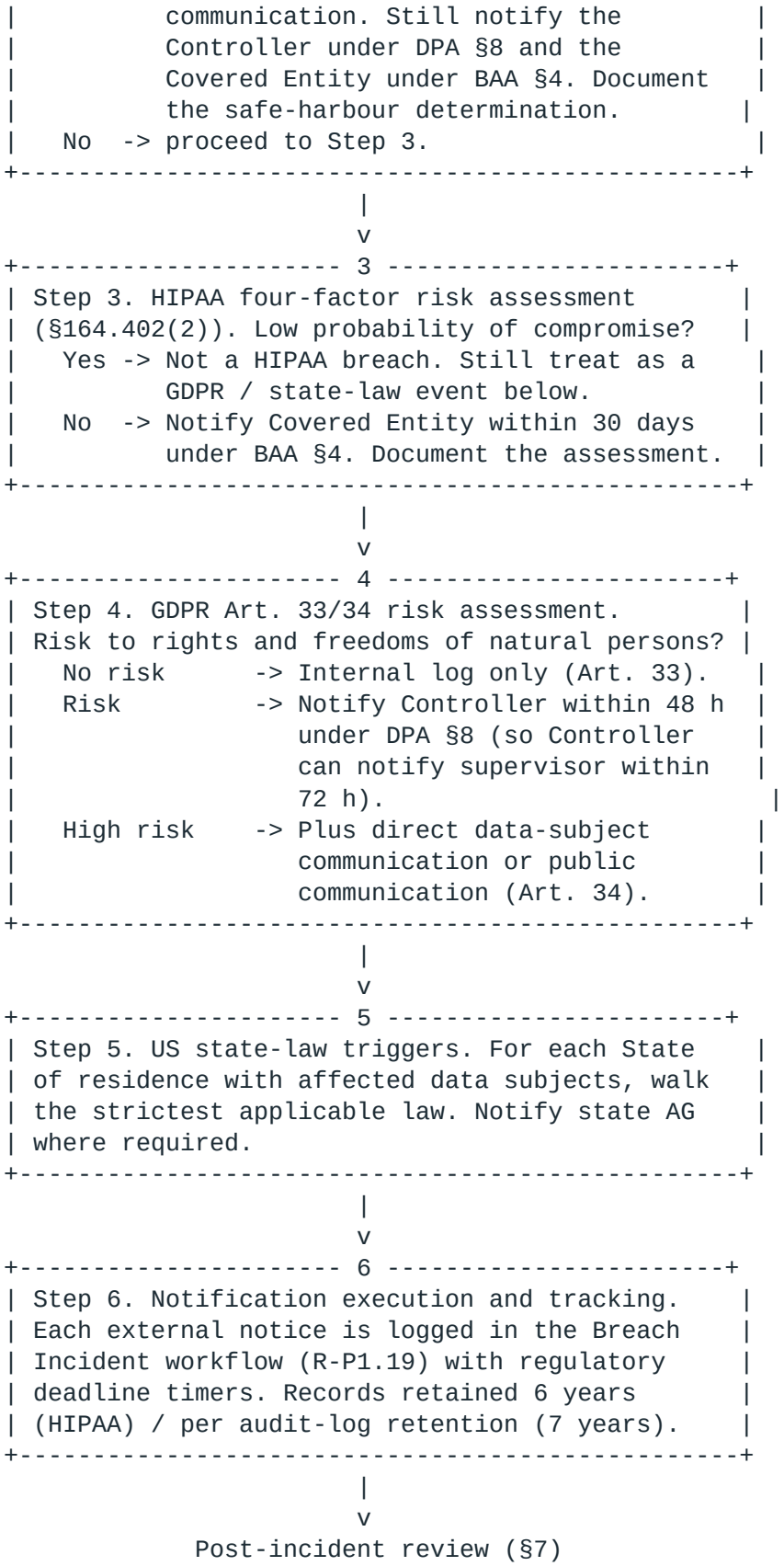
1. A notice to prominent media outlets serving that State or jurisdiction (§164.406);
2. A notice to the HHS Secretary contemporaneously with the individual notice (§164.408(b)).

Mabble supports the Covered Entity with the required information.

---

5. Internal decision tree




communication. Still notify the Controller under DPA §8 and the Covered Entity under BAA §4. Document the safe-harbour determination.
No -> proceed to Step 3.
3
Step 3. HIPAA four-factor risk assessment (§164.402(2)). Low probability of compromise?
Yes -> Not a HIPAA breach. Still treat as a GDPR / state-law event below.
No -> Notify Covered Entity within 30 days under BAA §4. Document the assessment.
4
Step 4. GDPR Art. 33/34 risk assessment. Risk to rights and freedoms of natural persons?
No risk -> Internal log only (Art. 33).
Risk -> Notify Controller within 48 h under DPA §8 (so Controller can notify supervisor within 72 h).
High risk -> Plus direct data-subject communication or public communication (Art. 34).
5
Step 5. US state-law triggers. For each State of residence with affected data subjects, walk the strictest applicable law. Notify state AG where required.
6
Step 6. Notification execution and tracking. Each external notice is logged in the Breach Incident workflow (R-P1.19) with regulatory deadline timers. Records retained 6 years (HIPAA) / per audit-log retention (7 years).
Post-incident review (§7)

6. Communication templates

The templates below are starting points. The Compliance Office tailors each one to the incident; legal review is mandatory before sending.

6.1 Initial customer notification - subject line and body

```
Subject:
  [Mabble Helix] Notice of a personal data security incident affecting
  your account - Mabble incident reference INC-YYYY-NNNN

Dear <Customer contact>,

This letter is to notify <Customer legal name> of a personal data
security incident affecting personal data processed by Mabble on
your behalf, identified by Mabble incident reference INC-YYYY-NNNN.

1. What happened
   <Brief factual description; do not speculate. Identify the
   timeframe, the categories of data potentially affected, and
   whether the data was encrypted at the time.>

2. When we learned of it
   Discovery: <ISO date / time UTC>
   Awareness (GDPR Art. 33 sense): <ISO date / time UTC>

3. Categories and approximate number of data subjects and records
   <Counts and categories, to the extent known. Phased
   notification per Art. 33(4) where information is still being
   gathered.>

4. Likely consequences for data subjects
   <Plain-language assessment of the risk to data subjects,
   referencing the four-factor HIPAA analysis where relevant and
   the GDPR risk threshold where relevant.>

5. What we are doing
   <Containment, eradication, recovery steps taken. Reference
   sub-processor coordination if any sub-processor was involved.>

6. What we recommend you do
   <Whether the customer must notify its data subjects, supervisors,
   AGs. Offer support per the BAA / DPA.>

7. Mabble contact for this incident
   sales@mabble.ai  (subject line: INC-YYYY-NNNN)
   <Named Compliance Office contact>

We will provide updates as the investigation progresses. This
notice is provided under the BAA Section 4 and DPA Section 8.

Sincerely,
```

<Mabble Compliance Office signatory>

6.2 Notification to a GDPR supervisory authority (where Mabble is Controller)

```
To:   <Lead supervisory authority - by online portal where one
       exists; otherwise by recorded mail and email>
From: Mabble, Inc. - Compliance Office, sales@mabble.ai
Date: <ISO date / time UTC>
Re:   Notification of a personal data breach pursuant to
      Regulation (EU) 2016/679 Article 33

1. Name and contact details of the data controller
   Mabble, Inc., d/b/a "Helix"
   [Registered address]
   Compliance Office contact: sales@mabble.ai
   DPO contact (interim): same address

2. Description of the personal data breach
   2.1 Nature of the breach
       <Confidentiality breach / integrity breach / availability
       breach - Art. 4(12)>
   2.2 Categories of data subjects
       <e.g., employees, customers>
   2.3 Approximate number of data subjects
       <number or "approximately N" or "currently undetermined">
   2.4 Categories of personal data records
       <e.g., identifiers, contact details, financial, special-
       category>
   2.5 Approximate number of personal data records
       <number or "currently undetermined">
   2.6 Date of breach (or range)
       <ISO range UTC>
   2.7 Date of awareness
       <ISO date / time UTC>

3. Likely consequences of the personal data breach
   <Plain-language assessment.>

4. Measures taken or proposed to address the breach
   <Containment, eradication, recovery, mitigation.>

5. Measures to mitigate possible adverse effects
   <Communication to data subjects per Art. 34 where applicable.
   Reference Art. 34(3) exceptions where invoked.>

6. Phased reporting per Art. 33(4)
   Where information was not available at the time of this
   notification, the Controller will provide additional information
   without further undue delay. The next planned update is on
   <ISO date>.

7. DPO / contact details
   sales@mabble.ai

Signature: <Mabble Compliance Office signatory>
Date:      <ISO date / time UTC>
```

6.3 Data-subject communication (Mabble as Controller)

```
Subject:
  Important notice about your personal data - Mabble incident
  reference INC-YYYY-NNNN

Dear <data subject>,

We are writing to inform you of a personal data security incident
that may have affected your personal data held by Mabble.

What happened
  <Plain-language description.>

When it happened
  <Approximate timeframe.>

What information was affected
  <Plain-language category list.>

What we are doing
  <Steps taken to investigate, contain, and mitigate.>

What you can do
  <Practical steps for the data subject - e.g., password reset,
  fraud monitoring, etc.>

How to contact us
  sales@mabble.ai  (subject line: INC-YYYY-NNNN)
  You may also lodge a complaint with your supervisory authority.

We are sorry that this incident has occurred and we are committed
to making sure it does not happen again.

Sincerely,
Mabble, Inc. - Compliance Office
```

6.4 Notification to a US State Attorney General (illustrative - exact form varies by state)

```
[State] Office of the Attorney General
[State AG mailing address]
[State AG breach-notification online portal where one exists]

Re: Notice of Data Security Incident - Mabble, Inc.
    State residents affected: approximately <N>

Dear Attorney General,

Pursuant to [cite state statute], Mabble, Inc. provides this notice
of a data security incident affecting approximately <N> residents
```

```
of <State>.

1. Date(s) of incident:   <ISO range UTC>
2. Date of discovery:     <ISO date UTC>
3. Description:           <Plain-language description.>
4. Types of information involved:
                          <Statutory categories.>
5. Mitigation steps:      <Description.>
6. Consumer notice:       Attached as Exhibit A. To be mailed /
                          emailed beginning <ISO date>.
7. Contact for inquiries: sales@mabble.ai

Sincerely,
<Mabble Compliance Office signatory>

Exhibit A - Copy of consumer notice
```

7. Post-incident review

Within 30 calendar days of incident closure, the Compliance Office leads a post-incident review covering:

1. **Root cause.** What allowed the incident to occur.
2. **Detection lag.** Time from event to detection; gap to close.
3. **Containment lag.** Time from detection to containment; gap to close.
4. **Notification timing.** Whether each external notice met its regulatory deadline.
5. **Lessons learned.** What controls (technical, organisational, contractual) need adjustment.
6. **Action items.** Logged in `internal/decisions/` and tracked to closure.

The post-incident review output is retained for at least 6 years (HIPAA §164.530(j)).

---

8. Record-keeping

Record	Retention	Location
Incident ticket (full timeline)	7 years	Incident-ticketing system, archived to S3 Object Lock COMPLIANCE
Audit-log range covering the incident	7 years	S3 Object Lock COMPLIANCE; Merkle anchor at Sigstore Rekor
Notifiability assessment	6 years	Compliance vault
External notices (customer, supervisor, AG, data subject)	6 years	Compliance vault
Post-incident review	6 years	Compliance vault, with summary in `internal/decisions/`

---

9. Cross-references

- BAA §4 - breach notification commitment: `docs/compliance/baa_template.md §4`
- DPA §8 - breach notification commitment: per the canonical DPA template
- Breach incident workflow (operational): R-P1.19, `internal/service/incident/...`
- Audit log Merkle chain: R-P0.07
- Outbox + NATS durable pipeline: R-P0.08 / R-P1.11
- Sigstore Rekor anchor: Mabble engineering decision D-005
- Internal operational runbook (not public): `mabble-runbooks/ir/ir-001-data-breach.md`
- SLO / SLI + alerts: R-P1.20, `docs/slo.md`
- DSAR workflow (for any data-subject right exercise arising from the incident): `internal/service/dsar/...`
- Vendor risk matrix (for sub-processor coordination): `internal/compliance/vendor_risk_matrix.md`

Change log

Version	Date	Change
0.1.0	2026-05-14	Initial Track C publication.