Investigation doc	<name + link to the investigation doc for this incident>
Title	<What happened? (a short sentence describing the outage)>
Author	<Full name of the person facilitating the post-mortem process>
Severity	**SEV1** / **SEV2** / **SEV3** (According to …)

Reviewers / List of stakeholders

Name	State (Not Reviewed/LGTM)	Date

Impact summary

High level of the impact, this is not for investigation sake but to give context for the severity of the incident

<Some text here…>

Timeline summary – All times are in <TTT (specify timezone)>

<This should be a compressed version of the investigation doc timeline, if it's a short incident than the **start** and **resolution** timeline would do.>

HH:MM XM	<Started at>
HH:MM XM	<Resolved at>

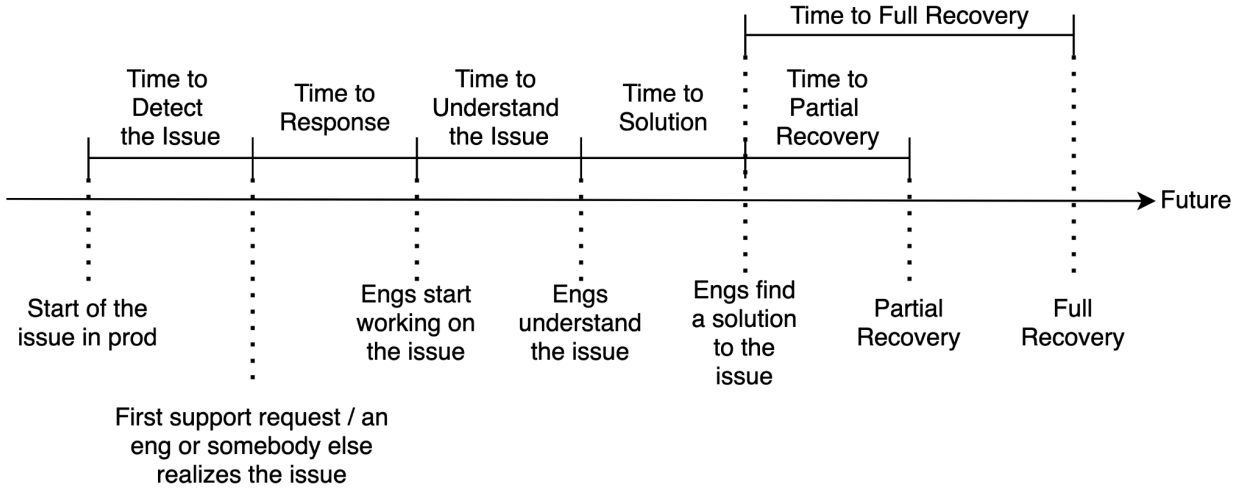
Incident Response Metrics

Blast Radius

Number of Clinics affected	< ## | Unknown >
Number of Providers affected	< ## | Unknown >
Number of Patients affected	< ## | Unknown >

Apps/APIs Affected	<Patient/Provider> <Web/iOS/Android/CWS APIs/All>

Timing of the response



Time to detect the issue (From when the issue started in production to when eng realized there was a problem)	<put time here>
Time to response (From when eng knew there was a problem to starting to work on it)	<put time here>
Time to understand the issue (Once eng started working on it, how long did it take to understand what the issue was)	<put time here>
Time to partial recovery (Sometimes we have a partial recovery. How long did it last from responding to the incident to partial recovery)	<put time here>
Time to solution (From understanding the issue to creating a solution)	<put time here>
Time to full recovery (From creating a solution to full recovery)	<put time here>

Participants

Number of TechOps engineers involved	<put # here>
Number of Software engineers involved	<put # here>
Number of Security engineers involved	<put # here>

Teams involved (list)	<put # here>

What went well?

Short version of what has happened well.

- E.g. Oncall identified the impact within 3 minutes

What didn't go well?

Short version of what did not go well.

- <E.g. it took us an hour to understand that the root cause of lack of disk space>

Where did we get lucky?

If things could have been much worse, detail them as well. We want to fix the "near miss" problems as well.

- <E.g. it happened on off hours and only 5% of our user base where impacted>

Why did it happen?

Summarize all the things that led to this problem in depth using the 5 whys mindset. Include both technical and organizational things like

- < e.g. What did we learn about our ability to handle outages like this? >
- < e.g. What went wrong with handling the outage in terms of organization/process? >
- …

Action Items

P0 Action Items (should be done within 48 hours)

- < AI1: e.g. immediately stop doing db migrations until we figure what's going on, owner: John, [ticket to Jira with a way to enforce migration stop] >
- < AI2: >

P1 Action Items (should be done within 14 days)

- < AI1: e.g. add documentation on how to do a safer db migration, owner: John [ticket to Jira to have someone do the documentation] >
- < AI2: >

P2 Action Items (should be done within 28 days)

- < AI1: e.g. create a staging environment and force migrations to run there first, owner: John, [ticket to Jira] >
- < AI2: >