



What can Cyber learn from Health in managing incidents?

Ian Pham, Head of Information Security
Victorian Managed Insurance Authority (VMIA)

ASTHMA FIRST AID

Blue/Grey Reliever

Airomir, Asmol, Ventolin or Zempreon and Bricanyl

Blue/grey reliever medication is unlikely to harm, even if the person does not have asthma

DIAL TRIPLE ZERO (000) FOR AN AMBULANCE IMMEDIATELY IF THE PERSON:

- is not breathing
- suddenly becomes worse or is not improving
- is having an asthma attack and a reliever is not available
- is unsure if it is asthma
- has a known allergy to food, insects or medication and has **SUDDEN BREATHING DIFFICULTY, GIVE ADRENALINE AUTOINJECTOR FIRST (if available)**

1 SIT THE PERSON UPRIGHT

- Be **calm** and reassuring
- Do not leave** them alone

2 GIVE 4 SEPARATE PUFFS OF RELIEVER PUFFER

- Shake puffer
- Put **1 puff** into spacer
- Take **4 breaths** from spacer
 - Repeat until **4 separate puffs** have been taken

If using **Bricanyl** (5 years or older)

- Do not shake.** Open, twist around and back, and take a deep breath in
- Repeat until **2 separate inhalations** have been taken

If you don't have a spacer handy in an emergency, take **1 puff** as you take **1 slow, deep breath** and hold breath for as long as comfortable. **Repeat** until all puffs are given

3 WAIT 4 MINUTES

- If breathing does not return to normal, give **4 more separate puffs** of reliever as above

Bricanyl: Give 1 more inhalation

IF BREATHING DOES NOT RETURN TO NORMAL

4 DIAL TRIPLE ZERO (000)

- Say **'ambulance'** and that someone is having an asthma attack
- Keep giving **4 separate puffs every 4 minutes** until emergency assistance arrives

Bricanyl: Give 1 more inhalation **every 4 minutes** until emergency assistance arrives

RESUSCITATION CHART

D

DANGER

Use all senses to check for dangers to yourself, others and the patient. Ensure the area is safe. Move the patient only if the danger cannot be eliminated.



R

RESPONSE

Check for a normal response by talking to the patient, asking them their name and squeezing their shoulders
DO NOT move the patient if the injury is the result of a fall



S

SEND FOR HELP

Send a bystander to call for help and an Ambulance as soon as possible
DIAL 000 and ask for Ambulance attendance.



A

AIRWAY

Open mouth and check for foreign objects. If objects are present place in recovery position and clear airway with fingers.
DO NOT move patient if the injury is the result of a fall.



B

BREATHING

Check breathing. **Look** for rise and fall of chest. **Listen** for breathing sounds. **Feel** for breaths on the cheek and for ribcage movement. If breathing is present keep the patient in the recovery position and monitor.



C

CPR

If no breathing is present commence CPR.
Give **30 Chest Compressions to every 2 Breaths**
@ 100 Compressions/minute.



D

DEFIBRILLATION

Apply defibrillator (if available) and follow the voice prompts or instruction on the device.
AED - Automated External Defibrillator



Continue CPR until responsiveness or normal breathing returns

Cyber incident response

Current standard

What's the bare minimum and what are we audited against?

Business Continuity Plan, Incident Response Plan, IT Disaster Recovery Plan...**all annually tested.**

- Is this enough?
- Do you have underpinning playbooks and are they tested?



Cyber Incident Response Plan	
Table of Contents	
1. Authority and Review	4
2. Purpose and Objectives	5
3. Standards and Frameworks	5
4. High Level Incident Response Process	6
5. Common Security Incidents and Responses	7
5.1. Common Threat Vectors	7
5.2. Common Cyber Incidents	8
6. Roles and Responsibilities	9
6.1. Points of Contact for Reporting Cyber Incidents	9
6.2. Cyber Incident Response Team (CIRT)	9
6.3. Senior Executive Management Team (SEMT)	10
6.4. Roles and Relationships	10
7. Communications	11
7.1. Internal Communications	11
7.2. External Communications	11
8. Supporting Procedures and Playbooks	12
8.1. Supporting Standard Operating Procedures (SOPs)	12
8.2. Supporting Playbooks	12
9. Sector, Jurisdiction and Nationality	12
9.1. Sector	12
9.2. Jurisdiction	12
9.3. Nationality	12
10. Incident Response	12
10.1. Legal	12
10.2. Insurance	12
11. Detection and Analysis	12
11.1. Incident Identification	12
11.2. Cyber Incident Analysis	12
11.3. Investigation	12
11.4. Escalation	12
12. Containment, Evidence Collection & Remediation	18
12.1. Containment	18
12.2. Documentation	18
12.3. Evidence Collection and Preservation	18
12.4. Remediation Action Plan	19
13. Recovery	20
13.1. Stand Down	20
14. Learn and Improve	21
14.1. Post Incident Review	21
14.2. Update and Test Cyber Incident Response Plan	22
14.3. Training	22
APPENDICES	23
Terminology and Definitions	24
Cyber Incident Response Readiness Checklist	25
ACSC Incident Triage Questions	28
Situation Report Template	29
Incident Log Template	30
Evidence Register Template	31
Remediation Action Plan Template	32
Post Incident Review Analysis Template	33
Action Register Template	39
Role Cards	40
ACSC Incident Categorisation Matrix 2022	41

Cyber incident risks

Insurance perspective



Risk insights:

- › Did not have a Cyber Incident Response Plan or no linkage with BCP
- › Did not have access to BCP (compromised system)
- › DR Plans didn't exist or outdated for critical and legacy systems
- › Time taken to restore systems longer than expected



What is Health
doing differently?



An example of Health Services' incident handover/escalation



Benefits/Value:

- Collaboration
- Understanding co-workers
- Concise and standard communication and information
- Agreed approach
- Ongoing practice and training for it to occur naturally.

ISBAR

Identify	Youself and your role, patient using 3 identifiers (refrain from using patient location).
Situation	What is going on? What is your reason? Use standardised status labels.
Background	What has been happening with the patient during your shift? What is their current diagnosis and plan of care?
Assessment and actions	Provide details of observations, procedures, treatment thus far, what do you feel needs to be done or changed?
Responsibility/ recommendations	How urgent do you require a response from this person? Set deadlines for actions.

SBAR report to clinician about a clinical obstetric situation

S	Situation	
	I am calling about (woman's name): _____ Ward: _____ Hosp No: _____	
	The problem I am calling about is: _____	
	I have just made an assessment:	
	The vital signs are: Blood pressure ____ / ____ Pulse ____ Respirations ____ SPO ₂ ____ % Temperature ____ °C	
	I am concerned about: Blood pressure because it is: systolic over 160 diastolic over 100 systolic less than 90 Pulse because it is: over 120 less than 40 Respirations because they are: less than 10 over 30 The woman is having oxygen at _____ l/min Maternal temperature because it is: ____ °C	Maternal serum lactate because it is: _____ mmol/l Urine output because it is: less than 100mls over the last 4 hours significantly proteinuric (+++) Haemorrhage: Antepartum Postpartum Fetal wellbeing: Pathological CTG FBS Result: pH _____ Time sample taken: _____ hrs Obstetric Early Warning Chart Score:
B	Background (tick relevant sections)	
	The woman is: Primiparous Multiparous Grand multiparous Gestation: _____ wks Singleton Multiple Previous Caesarean section or uterine surgery Fetal wellbeing Abdominal palpation: Fundal height: _____ cms Presentation: _____ Fifths palpable: _____ FH rate: _____ bpm CTG: Normal Suspicious Pathological Antenatal A/N problem (details): _____ Labour Spontaneous onset Induced IUGR Pre eclampsia Reduced Fetal movements Diabetes APH Syntocinon Most recent vaginal examination: Time _____ hrs Cervical dilatation: _____ cms Station of presenting part: _____ Position: _____ Membranes intact Meconium stained liquor Fresh red loss PV Third stage complete Retained placenta Postnatal Delivery date: _____ Delivery time: _____ hrs Type of delivery: _____ Perineal trauma: _____ Blood loss: _____ mls Syntocinon infusion Fundus: High Atonic Uterus tender Abdominal/perineal wound oozing Treatment given / in progress: _____	
A	Assessment	
	I think the problem is: _____ I am not sure what the problem is but the woman is deteriorating and we need to do something	
R	Recommendation	
	Request: Please come to see the woman immediately I think delivering needs to be expedited I think the woman needs to be transferred to delivery suite I would like advice please Reported to: _____ Response: _____	

Person completing form (name): _____ Date: _____ Time: _____

ISBAR escalation template

Example of Health Services' training



PROMPT

PRactical Obstetrics Multi-Professional Training

Training model:

- › Local unit – train where it happens
- › Regularly scheduled – recommended annually
- › Train 100% of staff – all at the same level
- › Evidence based – ensuring focus on risk priority
- › Practical – Lectures, hands-on skill stations, simulation scenarios in the clinical area
- › Multi-professional – improves comms, roles & leadership and situational awareness



Together we can make childbirth safer

50%

Reduced HIE (hypoxic brain injury)

Introduction of PROMPT training in North Bristol NHS Trust led to less birth hypoxia.

34%

Reduced maternal deaths

The introduction of PROMPT to Mpilo Hospital in Zimbabwe has improved maternal survival.

\$38m

Savings in litigation

After introducing PROMPT, Kansas University Hospital improved outcomes for individuals and families, resulting in reduced litigation costs.

PROMPT simulation



Figure 1. Managing a simulated postpartum haemorrhage on labour and birthing



Together we can make childbirth safer

50%

Reduced HIE (hypoxic brain injury)

Introduction of PROMPT training in North Bristol NHS Trust led to less birth hypoxia.

34%

Reduced maternal deaths

The introduction of PROMPT to Mpilo Hospital in Zimbabwe has improved maternal survival.

\$38m

Savings in litigation

After introducing PROMPT, Kansas University Hospital improved outcomes for individuals and families, resulting in reduced litigation costs.



What can
Cyber adopt?





- **Practical** simulations
- **Diversify** training methods
- **Regularly** schedule
- **Automate** and **optimise**
- Establish a **pulse checker** (helicopter view)
- **Tailored toolkits** for scenarios
- **Simple** classification (Visuals > Text)
- Continually **adopt** from other industries

Ransomware - Example Playbook

Identification

- Identify the following:
 - Impacted hosts
 - Impacted user accounts
 - Suspicious files and processes
 - Obtain file hashes
 - Command-and-control (C2) connections
- Determine the point of origin
- Run IoCs against Threat Intelligence
- If High or Critical risk, assemble Incident Management Team (IMT)

Containment & Eradicate

- Isolate impacted hosts in EDR
- Disable impacted user accounts in IdP and active sessions
- Disconnect backups for impacted hosts
- Reset passwords for impacted user accounts
- Block C2 connectivity on the Firewall
- Root cause analysis
- Conduct threat hunt to verify the threat is contained
- Invoke Data Breach playbook if required
- Notify cyber insurer (<72hrs of identification)
- Notify OVIC & CIRS

Recovery

- Confirm via threat hunt:
 - Verify the file is not present within the network
 - Ensure no other hosts have visited the URL
 - No suspicious activity or additional users/accounts impacted
- Rebuild host if required
- Re-enable user account if required

IF
REQUIRED

Incident Response

- VMIA engages Cyber Security Incident Response and Forensics partner
- Insurance Contact – X
- Policy # 999999999

VMIA Incident Response Contacts

Primary Contact:

VMIA Cyber Emergency Hotline | +61 X XXX XXXX

Secondary Contact(s):

Ian Pham | email address | +61 XXX XXX XXX

Tertiary Contact(s):

X person

Ransomware – Example Checklist

Identification		
Identify the following:	Details	
Impacted hosts		
Impacted user accounts		
Suspicious files and processes		
Obtain file hashes		
Command-and-control (C2) connections		
Determine the point of origin		
	Y	N
Run IoCs against MS Threat Intelligence		
If High or Critical risk, assemble Incident Management Team (IMT)		

Containment & Eradicate		
	Y	N
Isolate impacted hosts in MS Defender		
Disable impacted user accounts in Azure		
AD and active sessions		
Disconnect backups for impacted hosts		
Reset passwords for impacted user accounts		
Block C2 connectivity on the Palo Alto NGFW		
Root cause analysis		
Conduct threat hunt to verify the threat is contained		
Invoke Data Breach playbook if required		
Notify cyber insurer (<72hrs of identification)		
Notify OVIC & CIRS		


Recovery		
	Y	N
Rebuild impacted hosts		
Confirm root cause of the incident has been resolved		
Monitor closely to ensure incident is resolved		
De-escalation process - Notify IMT		

Hopefully, a Cyber version...

ASTHMA FIRST AID


Blue/Grey Reliever
Ailomir, Asmol, Ventolin or Zempren and Bricanyl

Blue/grey reliever medication is unlikely to harm, even if the person does not have asthma




DIAL TRIPLE ZERO (000) FOR AN AMBULANCE IMMEDIATELY IF THE PERSON:

- is not breathing
- suddenly becomes worse or is not improving
- is having an asthma attack and a reliever is not available
- is unsure if it is asthma
- has a known allergy to food, insects or medication and has **SUDDEN BREATHING DIFFICULTY**, GIVE ADRENALINE AUTOINJECTOR FIRST (if available)


- 

SIT THE PERSON UPRIGHT

 - Be calm and reassuring
 - Do not leave them alone
- 

GIVE 4 SEPARATE PUFFS OF RELIEVER PUFFER


 - Shake puffer
 - Put 1 puff into spacer
 - Take 4 breaths from spacer
 - Repeat until 4 separate puffs have been taken
 - If using Bricanyl (5 years or older)
 - Do not shake. Open, twist around and back, and take a deep breath in
 - Repeat until 2 separate inhalations have been taken

If you don't have a spacer handy in an emergency, take 1 puff as you take 1 slow, deep breath and hold breath for as long as comfortable. Repeat until all puffs are given
- 

WAIT 4 MINUTES





 - If breathing does not return to normal, give 4 more separate puffs of reliever as above
 - Bricanyl: Give 1 more inhalation

IF BREATHING DOES NOT RETURN TO NORMAL

- 








DIAL TRIPLE ZERO (000)

 - Say 'ambulance' and that someone is having an asthma attack
 - Keep giving 4 separate puffs every 4 minutes until emergency assistance arrives
 - Bricanyl: Give 1 more inhalation every 4 minutes until emergency assistance arrives

© Asthma Australia 2023

RESUSCITATION CHART

D	DANGER	 <p>Use all senses to check for dangers to yourself, others and the patient. Ensure the area is safe. Move the patient only if the danger cannot be eliminated.</p>
R	RESPONSE	 <p>Check for a normal response by talking to the patient, asking them their name and squeezing their shoulders. DO NOT move the patient if the injury is the result of a fall</p>
S	SEND FOR HELP	 <p>Send a bystander to call for help and an Ambulance as soon as possible. DIAL 000 and ask for Ambulance attendance.</p>
A	AIRWAY	 <p>Open mouth and check for foreign objects. If objects are present place in recovery position and clear airway with fingers. DO NOT move patient if the injury is the result of a fall.</p>
B	BREATHING	 <p>Check breathing. Look for rise and fall of chest. Listen for breathing sounds. Feel for breaths on the cheek and for ribcage movement. If breathing is present keep the patient in the recovery position and monitor.</p>
C	CPR	 <p>If no breathing is present commence CPR. Give 30 Chest Compressions to every 2 Breaths @ 100 Compressions/minute.</p>
D	DEFIBRILLATION	 <p>Apply defibrillator (if available) and follow the voice prompts or instruction on the device. AED - Automated External Defibrillator Continue CPR until responsiveness or normal breathing returns</p>



vmia.vic.gov.au