

eHealth 2016

Monitoring access to Personal Health Information using an Advanced Privacy Monitoring solution



Complying with legislations, legal directives and detecting unauthorized access to PHI

June 6, 2016

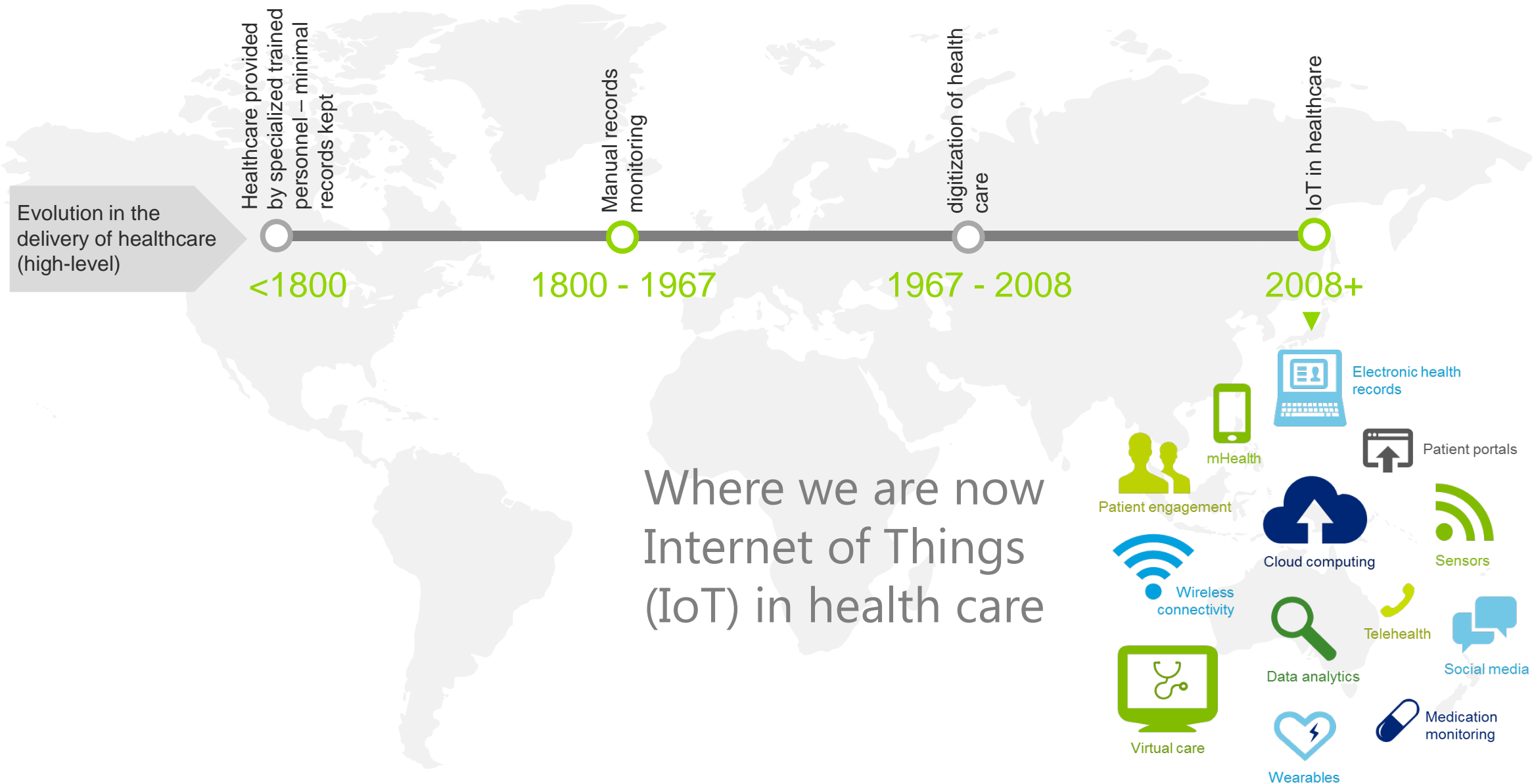
Agenda

1. Background
2. What is the solution?
3. Use case walkthrough
4. Is this solution for you?
5. Q & A



Background



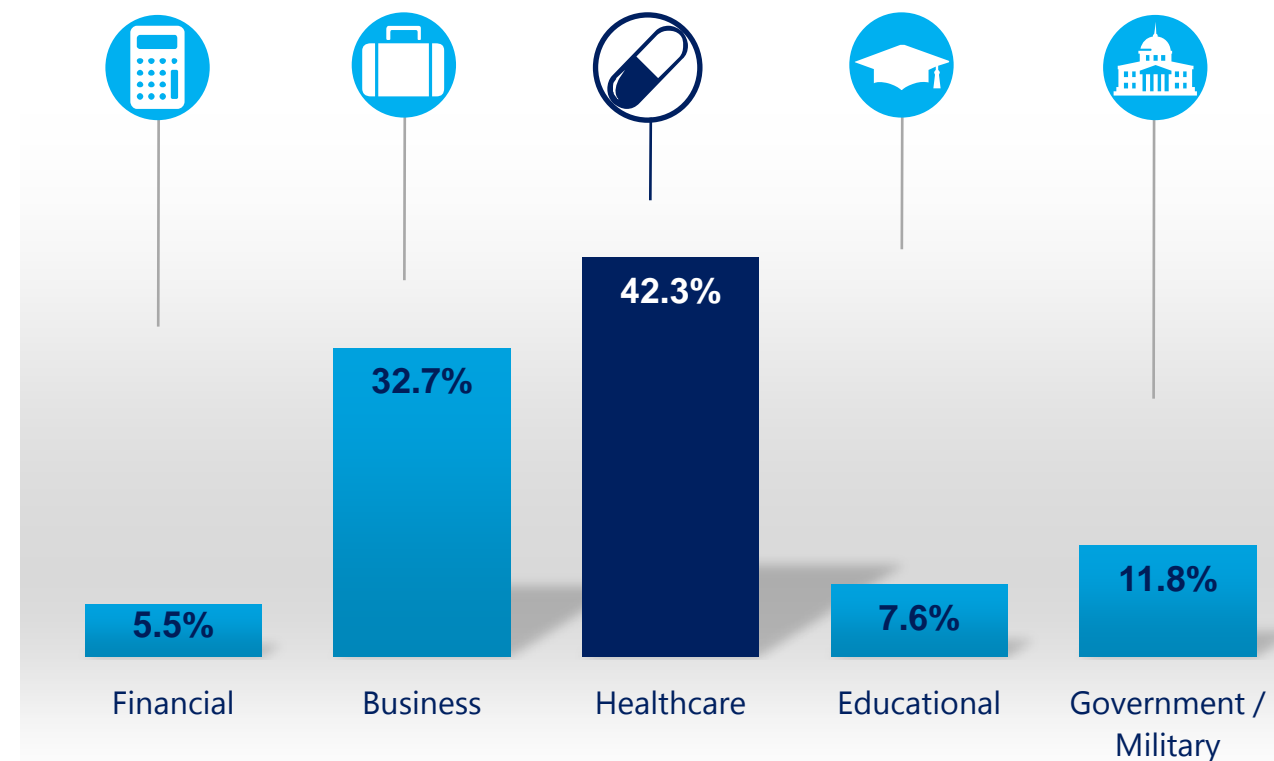


Common challenges

- Most patient privacy breaches occur due to **internal unmonitored processes** with little to no oversight
- Ongoing **privacy training and awareness** of employees, contracts, and third parties is often a “**myth**”
- Privacy/compliance offices **lack** the **visibility** and the **authority** to enforce policy
- **Manual privacy breach detection** processes are very **difficult** to scale and **sustain**
- Most organizations continue to use **various different Clinical Information Systems** (CIS) and **EHR applications** (e.g., off-the shelf systems, home grown systems, etc.) each with **different security capabilities** making it hard to manage
- Extracting, monitoring, and reviewing **audit log data** from applications
- Organizations **lack** an **enterprise strategy** and policy around privacy access violations

Healthcare organizations are increasingly targeted by cyber criminals as Personal Health Information (PHI) has become lucrative targets with a high market value in the underground cyber market.


In 2014, Identify Theft Resource Center (ITRC) reported that sensitive data breaches in Healthcare accounted for 42.3% of reported breaches, the highest amongst all compared industries.





What is the solution?



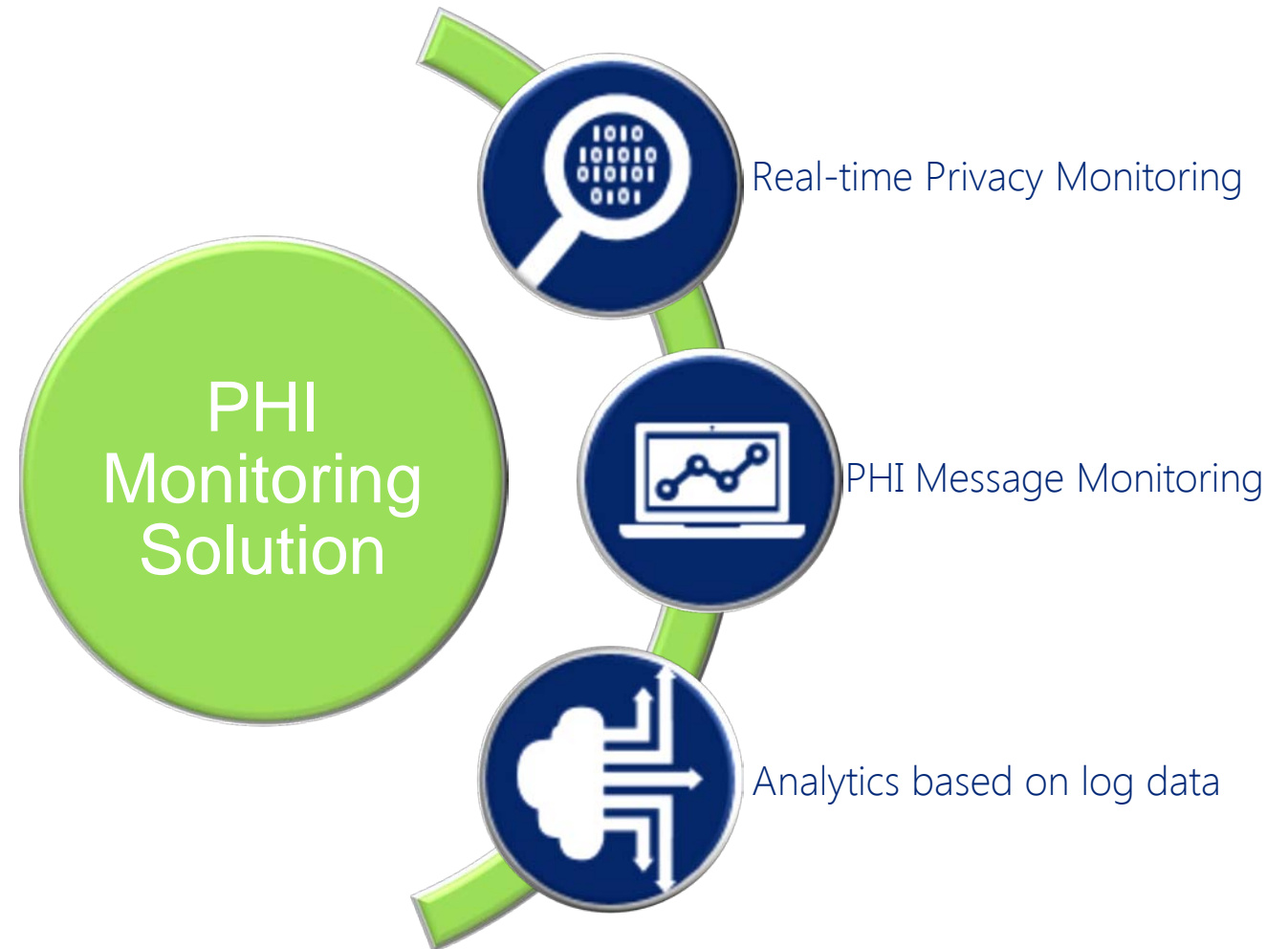
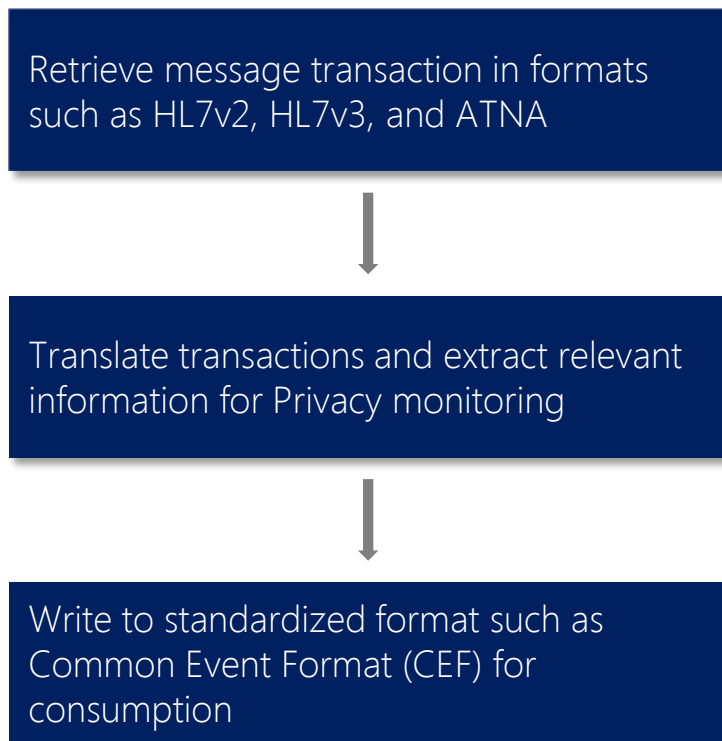


Operationalizing a monitoring service that provides **enhanced visibility** into transactions involving access to PHI using a combination of **audit collection, reporting and active PHI transaction monitoring capabilities.**

Uniqueness of the solution

We are not just **collecting** logs; we are **creating** logs by analyzing business transactions that are traversing an Integrated Health Environment (IHE) and generating standardized and normalized privacy audit event logs.

Solution logic flow



Uniqueness of the solution

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
3   <S:Body>
4     <hl7:PRPA_I101106CA ITSVersion="XML_1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:hl7=
5       "urn:hl7-org:v3" xmlns:empi="http://ehealthontario.on.ca/xmlns/pcr/emp/v01">
6       <hl7:realCode code="CA"/>
7       <hl7:id xsi:type="hl7:II" specializationType="II.TOKEN" root="4e303f75-d243-4cc1-bd44-58a9fbb1bd79"/>
8       <hl7:creationTime xsi:type="hl7:TS" specializationType="TS.FULLDATETIME" value="2013061122306-0400"/>
9       <hl7:responseModeCode code="I"/>
10      <hl7:versionCode code="V3-2008M"/>
11      <hl7:interactionId xsi:type="hl7:II" specializationType="II.PUBLIC" root="2.16.840.1.113883.1.6" extension=
12        "PRPA_I101106CA" displayable="true" use="BUS"/>
13      <hl7:profileId xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.2.20.2" extension=
14        "R02.04.03" use="BUS"/>
15      <hl7:profileId xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.3.239.7" extension="V03.00"
16        use="BUS"/>
17      <hl7:processingCode code="P"/>
18      <hl7:processingModeCode code="T"/>
19      <hl7:acceptAckCode code="NE"/>
20      <hl7:receiver typeCode="RCV">
21        <hl7:telecom xsi:type="hl7:TEL" specializationType="TEL.URI" value="http://120.120.120.120"/>
22        <hl7:device classCode="DEV" determinerCode="INSTANCE">
23          <hl7:id xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.3.239.4" use="BUS"/>
24          <hl7:name value="me"/>
25          <hl7:agent classCode="AGNT">
26            <hl7:agentOrganization classCode="ORG" determinerCode="INSTANCE">
27              <hl7:id xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.3.239" use="BUS"/>
28              <hl7:agentOrganization>
29                <hl7:agent>
30                  <hl7:device>
31                    <hl7:sender typeCode="SND">
32                      <hl7:telecom xsi:type="hl7:TEL" specializationType="TEL.URI" value="TBD"/>
33                      <hl7:device classCode="DEV" determinerCode="INSTANCE">
34                        <hl7:id xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.3.239.2" use="BUS"/>
35                        <hl7:name value="hl7:name"/>
36                        <hl7:agent classCode="AGNT">
```

```
34 <hl7:agentOrganization classCode="ORG" determinerCode="INSTANCE">
35   <hl7:id xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.3.239" use="BUS"/>
36   <hl7:agentOrganization>
37     <hl7:agent>
38       <hl7:device>
39     </hl7:device>
40   </hl7:agent>
41   <hl7:acknowledgement typeCode="AA">
42     <hl7:targetMessage>
43       <hl7:id xsi:type="hl7:II" specializationType="II.TOKEN" root="8a3ab3bf-8bb3-450d-81e5-ccc77e354e80"/>
44       <hl7:targetMessage>
45     </hl7:acknowledgement>
46   <hl7:controlActEvent classCode="CACT" moodCode="EVN">
47     <hl7:id xsi:type="hl7:II" specializationType="II.BUS" root="d28cf316-f2d4-4c59-b02a-0048f9dd8067" use="BUS"/>
48     <hl7:code code="PRPA_I101106CA" codeSystem="2.16.840.1.113883.1.18"/>
49     <hl7:statusCode code="completed"/>
50     <hl7:subject typeCode="SUBJ" contextControlCode="ON" contextConductionInd="false">
51       <hl7:registrationEvent classCode="REG" moodCode="EVN">
52         <hl7:statusCode code="active"/>
53         <hl7:subject typeCode="SBJ" contextControlCode="AN">
54           <hl7:identifiedEntity classCode="IDENT">
55             <hl7:id root="2.16.840.1.113883.3.239.20" extension="1752"/>
56             <hl7:id root="2.16.840.1.113883.3.239.19.64" extension="8865432"/>
57             <hl7:id root="2.16.840.1.113883.4.59" extension="677894"/>
58             <hl7:id root="2.16.840.1.113883.3.239.18.150" extension="MRN893452"/>
59             <hl7:statusCode nullFlavor="NI"/>
60             <hl7:effectiveTime>
61               <hl7:low value="20130228"/>
62             </hl7:effectiveTime>
63             <hl7:confidentialityCode codeSystem="2.16.840.1.113883.5.25" code="N"/>
64             <hl7:identifiedPerson classCode="PSN" determinerCode="INSTANCE"/>
65             <hl7:subjectOf typeCode="SBJ">
66               <hl7:observationEvent classCode="OBS" moodCode="EVN">
67                 <hl7:code codeSystem="2.16.840.1.113883.2.20.5.2" code="PTNM"/>
```

```
67 <hl7:value value="0"/>
68 </hl7:observationEvent>
69 </hl7:subjectOf>
70 </hl7:identifiedEntity>
71 </hl7:subject>
72 <hl7:custodian>
73   <hl7:assignedDevice classCode="ASSIGNED">
74     <hl7:id xsi:type="hl7:II" specializationType="II.BUS" root="2.16.840.1.113883.3.239.21.60" use=
75       "BUS"/>
76     <hl7:assignedDevice>
77       <hl7:name>
78         <hl7:assignedRepository classCode="DEV" determinerCode="INSTANCE" />
79         <hl7:assignedRepository>
80           <hl7:representedRepositoryJurisdiction classCode="STATE" determinerCode="INSTANCE">
81             <hl7:name>Ontario</hl7:name>
82           </hl7:representedRepositoryJurisdiction>
83           <hl7:assignedDevice>
84             <hl7:custodian>
85               <hl7:registrationEvent>
86                 <hl7:subject>
87                   <hl7:queryAck>
88                     <hl7:queryId xsi:type="hl7:II" specializationType="II.TOKEN"/>
89                     <hl7:queryResponseCode code="OK"/>
90                     <hl7:resultTotalQuantity value="1"/>
91                     <hl7:resultCurrentQuantity value="1"/>
92                     <hl7:resultRemainingQuantity value="0"/>
93                   </hl7:queryAck>
94                   <hl7:queryByParameter>
95                     <hl7:queryId xsi:type="hl7:II" specializationType="II.TOKEN" root="96242364-8405-4fdb-962a-021bbc98b274"/>
96                     <hl7:parameterList>
97                       <hl7:clientIDPub>
98                         <hl7:value root="2.16.840.1.113883.3.239.19.64" use="BUS" extension="8865432"/>
99                       </hl7:clientIDPub>
100                     </hl7:parameterList>
101                   </hl7:queryByParameter>
102                   <hl7:controlActEvent>
103                     <hl7:PRPA_I101106CA>
104                   </hl7:controlActEvent>
105                 </hl7:subject>
106               </hl7:registrationEvent>
107             </hl7:custodian>
108           </hl7:assignedDevice>
109         </hl7:name>
110       </hl7:assignedDevice>
111     </hl7:assignedDevice>
112   </hl7:custodian>
113 </hl7:subject>
114 </hl7:subjectOf>
115 </hl7:identifiedEntity>
116 </hl7:subject>
117 </hl7:agent>
118 </hl7:agentOrganization>
119 </hl7:acknowledgement>
120 </hl7:controlActEvent>
121 </hl7:registrationEvent>
122 </hl7:subject>
123 </hl7:subjectOf>
124 </hl7:identifiedEntity>
125 </hl7:subject>
126 </hl7:agent>
127 </hl7:agentOrganization>
128 </hl7:acknowledgement>
129 </hl7:controlActEvent>
130 </hl7:registrationEvent>
131 </hl7:subject>
132 </hl7:subjectOf>
133 </hl7:identifiedEntity>
134 </hl7:subject>
135 </hl7:agent>
136 </hl7:agentOrganization>
137 </hl7:acknowledgement>
138 </hl7:controlActEvent>
139 </hl7:registrationEvent>
140 </hl7:subject>
141 </hl7:subjectOf>
142 </hl7:identifiedEntity>
143 </hl7:subject>
144 </hl7:agent>
145 </hl7:agentOrganization>
146 </hl7:acknowledgement>
147 </hl7:controlActEvent>
148 </hl7:registrationEvent>
149 </hl7:subject>
150 </hl7:subjectOf>
151 </hl7:identifiedEntity>
152 </hl7:subject>
153 </hl7:agent>
154 </hl7:agentOrganization>
155 </hl7:acknowledgement>
156 </hl7:controlActEvent>
157 </hl7:registrationEvent>
158 </hl7:subject>
159 </hl7:subjectOf>
160 </hl7:identifiedEntity>
161 </hl7:subject>
162 </hl7:agent>
163 </hl7:agentOrganization>
164 </hl7:acknowledgement>
165 </hl7:controlActEvent>
166 </hl7:registrationEvent>
167 </hl7:subject>
168 </hl7:subjectOf>
169 </hl7:identifiedEntity>
170 </hl7:subject>
171 </hl7:agent>
172 </hl7:agentOrganization>
173 </hl7:acknowledgement>
174 </hl7:controlActEvent>
175 </hl7:registrationEvent>
176 </hl7:subject>
177 </hl7:subjectOf>
178 </hl7:identifiedEntity>
179 </hl7:subject>
180 </hl7:agent>
181 </hl7:agentOrganization>
182 </hl7:acknowledgement>
183 </hl7:controlActEvent>
184 </hl7:registrationEvent>
185 </hl7:subject>
186 </hl7:subjectOf>
187 </hl7:identifiedEntity>
188 </hl7:subject>
189 </hl7:agent>
190 </hl7:agentOrganization>
191 </hl7:acknowledgement>
192 </hl7:controlActEvent>
193 </hl7:registrationEvent>
194 </hl7:subject>
195 </hl7:subjectOf>
196 </hl7:identifiedEntity>
197 </hl7:subject>
198 </hl7:agent>
199 </hl7:agentOrganization>
200 </hl7:acknowledgement>
201 </hl7:controlActEvent>
202 </hl7:registrationEvent>
203 </hl7:subject>
204 </hl7:subjectOf>
205 </hl7:identifiedEntity>
206 </hl7:subject>
207 </hl7:agent>
208 </hl7:agentOrganization>
209 </hl7:acknowledgement>
210 </hl7:controlActEvent>
211 </hl7:registrationEvent>
212 </hl7:subject>
213 </hl7:subjectOf>
214 </hl7:identifiedEntity>
215 </hl7:subject>
216 </hl7:agent>
217 </hl7:agentOrganization>
218 </hl7:acknowledgement>
219 </hl7:controlActEvent>
220 </hl7:registrationEvent>
221 </hl7:subject>
222 </hl7:subjectOf>
223 </hl7:identifiedEntity>
224 </hl7:subject>
225 </hl7:agent>
226 </hl7:agentOrganization>
227 </hl7:acknowledgement>
228 </hl7:controlActEvent>
229 </hl7:registrationEvent>
230 </hl7:subject>
231 </hl7:subjectOf>
232 </hl7:identifiedEntity>
233 </hl7:subject>
234 </hl7:agent>
235 </hl7:agentOrganization>
236 </hl7:acknowledgement>
237 </hl7:controlActEvent>
238 </hl7:registrationEvent>
239 </hl7:subject>
240 </hl7:subjectOf>
241 </hl7:identifiedEntity>
242 </hl7:subject>
243 </hl7:agent>
244 </hl7:agentOrganization>
245 </hl7:acknowledgement>
246 </hl7:controlActEvent>
247 </hl7:registrationEvent>
248 </hl7:subject>
249 </hl7:subjectOf>
250 </hl7:identifiedEntity>
251 </hl7:subject>
252 </hl7:agent>
253 </hl7:agentOrganization>
254 </hl7:acknowledgement>
255 </hl7:controlActEvent>
256 </hl7:registrationEvent>
257 </hl7:subject>
258 </hl7:subjectOf>
259 </hl7:identifiedEntity>
260 </hl7:subject>
261 </hl7:agent>
262 </hl7:agentOrganization>
263 </hl7:acknowledgement>
264 </hl7:controlActEvent>
265 </hl7:registrationEvent>
266 </hl7:subject>
267 </hl7:subjectOf>
268 </hl7:identifiedEntity>
269 </hl7:subject>
270 </hl7:agent>
271 </hl7:agentOrganization>
272 </hl7:acknowledgement>
273 </hl7:controlActEvent>
274 </hl7:registrationEvent>
275 </hl7:subject>
276 </hl7:subjectOf>
277 </hl7:identifiedEntity>
278 </hl7:subject>
279 </hl7:agent>
280 </hl7:agentOrganization>
281 </hl7:acknowledgement>
282 </hl7:controlActEvent>
283 </hl7:registrationEvent>
284 </hl7:subject>
285 </hl7:subjectOf>
286 </hl7:identifiedEntity>
287 </hl7:subject>
288 </hl7:agent>
289 </hl7:agentOrganization>
290 </hl7:acknowledgement>
291 </hl7:controlActEvent>
292 </hl7:registrationEvent>
293 </hl7:subject>
294 </hl7:subjectOf>
295 </hl7:identifiedEntity>
296 </hl7:subject>
297 </hl7:agent>
298 </hl7:agentOrganization>
299 </hl7:acknowledgement>
300 </hl7:controlActEvent>
301 </hl7:registrationEvent>
302 </hl7:subject>
303 </hl7:subjectOf>
304 </hl7:identifiedEntity>
305 </hl7:subject>
306 </hl7:agent>
307 </hl7:agentOrganization>
308 </hl7:acknowledgement>
309 </hl7:controlActEvent>
310 </hl7:registrationEvent>
311 </hl7:subject>
312 </hl7:subjectOf>
313 </hl7:identifiedEntity>
314 </hl7:subject>
315 </hl7:agent>
316 </hl7:agentOrganization>
317 </hl7:acknowledgement>
318 </hl7:controlActEvent>
319 </hl7:registrationEvent>
320 </hl7:subject>
321 </hl7:subjectOf>
322 </hl7:identifiedEntity>
323 </hl7:subject>
324 </hl7:agent>
325 </hl7:agentOrganization>
326 </hl7:acknowledgement>
327 </hl7:controlActEvent>
328 </hl7:registrationEvent>
329 </hl7:subject>
330 </hl7:subjectOf>
331 </hl7:identifiedEntity>
332 </hl7:subject>
333 </hl7:agent>
334 </hl7:agentOrganization>
335 </hl7:acknowledgement>
336 </hl7:controlActEvent>
337 </hl7:registrationEvent>
338 </hl7:subject>
339 </hl7:subjectOf>
340 </hl7:identifiedEntity>
341 </hl7:subject>
342 </hl7:agent>
343 </hl7:agentOrganization>
344 </hl7:acknowledgement>
345 </hl7:controlActEvent>
346 </hl7:registrationEvent>
347 </hl7:subject>
348 </hl7:subjectOf>
349 </hl7:identifiedEntity>
350 </hl7:subject>
351 </hl7:agent>
352 </hl7:agentOrganization>
353 </hl7:acknowledgement>
354 </hl7:controlActEvent>
355 </hl7:registrationEvent>
356 </hl7:subject>
357 </hl7:subjectOf>
358 </hl7:identifiedEntity>
359 </hl7:subject>
360 </hl7:agent>
361 </hl7:agentOrganization>
362 </hl7:acknowledgement>
363 </hl7:controlActEvent>
364 </hl7:registrationEvent>
365 </hl7:subject>
366 </hl7:subjectOf>
367 </hl7:identifiedEntity>
368 </hl7:subject>
369 </hl7:agent>
370 </hl7:agentOrganization>
371 </hl7:acknowledgement>
372 </hl7:controlActEvent>
373 </hl7:registrationEvent>
374 </hl7:subject>
375 </hl7:subjectOf>
376 </hl7:identifiedEntity>
377 </hl7:subject>
378 </hl7:agent>
379 </hl7:agentOrganization>
380 </hl7:acknowledgement>
381 </hl7:controlActEvent>
382 </hl7:registrationEvent>
383 </hl7:subject>
384 </hl7:subjectOf>
385 </hl7:identifiedEntity>
386 </hl7:subject>
387 </hl7:agent>
388 </hl7:agentOrganization>
389 </hl7:acknowledgement>
390 </hl7:controlActEvent>
391 </hl7:registrationEvent>
392 </hl7:subject>
393 </hl7:subjectOf>
394 </hl7:identifiedEntity>
395 </hl7:subject>
396 </hl7:agent>
397 </hl7:agentOrganization>
398 </hl7:acknowledgement>
399 </hl7:controlActEvent>
400 </hl7:registrationEvent>
401 </hl7:subject>
402 </hl7:subjectOf>
403 </hl7:identifiedEntity>
404 </hl7:subject>
405 </hl7:agent>
406 </hl7:agentOrganization>
407 </hl7:acknowledgement>
408 </hl7:controlActEvent>
409 </hl7:registrationEvent>
410 </hl7:subject>
411 </hl7:subjectOf>
412 </hl7:identifiedEntity>
413 </hl7:subject>
414 </hl7:agent>
415 </hl7:agentOrganization>
416 </hl7:acknowledgement>
417 </hl7:controlActEvent>
418 </hl7:registrationEvent>
419 </hl7:subject>
420 </hl7:subjectOf>
421 </hl7:identifiedEntity>
422 </hl7:subject>
423 </hl7:agent>
424 </hl7:agentOrganization>
425 </hl7:acknowledgement>
426 </hl7:controlActEvent>
427 </hl7:registrationEvent>
428 </hl7:subject>
429 </hl7:subjectOf>
430 </hl7:identifiedEntity>
431 </hl7:subject>
432 </hl7:agent>
433 </hl7:agentOrganization>
434 </hl7:acknowledgement>
435 </hl7:controlActEvent>
436 </hl7:registrationEvent>
437 </hl7:subject>
438 </hl7:subjectOf>
439 </hl7:identifiedEntity>
440 </hl7:subject>
441 </hl7:agent>
442 </hl7:agentOrganization>
443 </hl7:acknowledgement>
444 </hl7:controlActEvent>
445 </hl7:registrationEvent>
446 </hl7:subject>
447 </hl7:subjectOf>
448 </hl7:identifiedEntity>
449 </hl7:subject>
450 </hl7:agent>
451 </hl7:agentOrganization>
452 </hl7:acknowledgement>
453 </hl7:controlActEvent>
454 </hl7:registrationEvent>
455 </hl7:subject>
456 </hl7:subjectOf>
457 </hl7:identifiedEntity>
458 </hl7:subject>
459 </hl7:agent>
460 </hl7:agentOrganization>
461 </hl7:acknowledgement>
462 </hl7:controlActEvent>
463 </hl7:registrationEvent>
464 </hl7:subject>
465 </hl7:subjectOf>
466 </hl7:identifiedEntity>
467 </hl7:subject>
468 </hl7:agent>
469 </hl7:agentOrganization>
470 </hl7:acknowledgement>
471 </hl7:controlActEvent>
472 </hl7:registrationEvent>
473 </hl7:subject>
474 </hl7:subjectOf>
475 </hl7:identifiedEntity>
476 </hl7:subject>
477 </hl7:agent>
478 </hl7:agentOrganization>
479 </hl7:acknowledgement>
480 </hl7:controlActEvent>
481 </hl7:registrationEvent>
482 </hl7:subject>
483 </hl7:subjectOf>
484 </hl7:identifiedEntity>
485 </hl7:subject>
486 </hl7:agent>
487 </hl7:agentOrganization>
488 </hl7:acknowledgement>
489 </hl7:controlActEvent>
490 </hl7:registrationEvent>
491 </hl7:subject>
492 </hl7:subjectOf>
493 </hl7:identifiedEntity>
494 </hl7:subject>
495 </hl7:agent>
496 </hl7:agentOrganization>
497 </hl7:acknowledgement>
498 </hl7:controlActEvent>
499 </hl7:registrationEvent>
500 </hl7:subject>
501 </hl7:subjectOf>
502 </hl7:identifiedEntity>
503 </hl7:subject>
504 </hl7:agent>
505 </hl7:agentOrganization>
506 </hl7:acknowledgement>
507 </hl7:controlActEvent>
508 </hl7:registrationEvent>
509 </hl7:subject>
510 </hl7:subjectOf>
511 </hl7:identifiedEntity>
512 </hl7:subject>
513 </hl7:agent>
514 </hl7:agentOrganization>
515 </hl7:acknowledgement>
516 </hl7:controlActEvent>
517 </hl7:registrationEvent>
518 </hl7:subject>
519 </hl7:subjectOf>
520 </hl7:identifiedEntity>
521 </hl7:subject>
522 </hl7:agent>
523 </hl7:agentOrganization>
524 </hl7:acknowledgement>
525 </hl7:controlActEvent>
526 </hl7:registrationEvent>
527 </hl7:subject>
528 </hl7:subjectOf>
529 </hl7:identifiedEntity>
530 </hl7:subject>
531 </hl7:agent>
532 </hl7:agentOrganization>
533 </hl7:acknowledgement>
534 </hl7:controlActEvent>
535 </hl7:registrationEvent>
536 </hl7:subject>
537 </hl7:subjectOf>
538 </hl7:identifiedEntity>
539 </hl7:subject>
540 </hl7:agent>
541 </hl7:agentOrganization>
542 </hl7:acknowledgement>
543 </hl7:controlActEvent>
544 </hl7:registrationEvent>
545 </hl7:subject>
546 </hl7:subjectOf>
547 </hl7:identifiedEntity>
548 </hl7:subject>
549 </hl7:agent>
550 </hl7:agentOrganization>
551 </hl7:acknowledgement>
552 </hl7:controlActEvent>
553 </hl7:registrationEvent>
554 </hl7:subject>
555 </hl7:subjectOf>
556 </hl7:identifiedEntity>
557 </hl7:subject>
558 </hl7:agent>
559 </hl7:agentOrganization>
560 </hl7:acknowledgement>
561 </hl7:controlActEvent>
562 </hl7:registrationEvent>
563 </hl7:subject>
564 </hl7:subjectOf>
565 </hl7:identifiedEntity>
566 </hl7:subject>
567 </hl7:agent>
568 </hl7:agentOrganization>
569 </hl7:acknowledgement>
570 </hl7:controlActEvent>
571 </hl7:registrationEvent>
572 </hl7:subject>
573 </hl7:subjectOf>
574 </hl7:identifiedEntity>
575 </hl7:subject>
576 </hl7:agent>
577 </hl7:agentOrganization>
578 </hl7:acknowledgement>
579 </hl7:controlActEvent>
580 </hl7:registrationEvent>
581 </hl7:subject>
582 </hl7:subjectOf>
583 </hl7:identifiedEntity>
584 </hl7:subject>
585 </hl7:agent>
586 </hl7:agentOrganization>
587 </hl7:acknowledgement>
588 </hl7:controlActEvent>
589 </hl7:registrationEvent>
590 </hl7:subject>
591 </hl7:subjectOf>
592 </hl7:identifiedEntity>
593 </hl7:subject>
594 </hl7:agent>
595 </hl7:agentOrganization>
596 </hl7:acknowledgement>
597 </hl7:controlActEvent>
598 </hl7:registrationEvent>
599 </hl7:subject>
600 </hl7:subjectOf>
601 </hl7:identifiedEntity>
602 </hl7:subject>
603 </hl7:agent>
604 </hl7:agentOrganization>
605 </hl7:acknowledgement>
606 </hl7:controlActEvent>
607 </hl7:registrationEvent>
608 </hl7:subject>
609 </hl7:subjectOf>
610 </hl7:identifiedEntity>
611 </hl7:subject>
612 </hl7:agent>
613 </hl7:agentOrganization>
614 </hl7:acknowledgement>
615 </hl7:controlActEvent>
616 </hl7:registrationEvent>
617 </hl7:subject>
618 </hl7:subjectOf>
619 </hl7:identifiedEntity>
620 </hl7:subject>
621 </hl7:agent>
622 </hl7:agentOrganization>
623 </hl7:acknowledgement>
624 </hl7:controlActEvent>
625 </hl7:registrationEvent>
626 </hl7:subject>
627 </hl7:subjectOf>
628 </hl7:identifiedEntity>
629 </hl7:subject>
630 </hl7:agent>
631 </hl7:agentOrganization>
632 </hl7:acknowledgement>
633 </hl7:controlActEvent>
634 </hl7:registrationEvent>
635 </hl7:subject>
636 </hl7:subjectOf>
637 </hl7:identifiedEntity>
638 </hl7:subject>
639 </hl7:agent>
640 </hl7:agentOrganization>
641 </hl7:acknowledgement>
642 </hl7:controlActEvent>
643 </hl7:registrationEvent>
644 </hl7:subject>
645 </hl7:subjectOf>
646 </hl7:identifiedEntity>
647 </hl7:subject>
648 </hl7:agent>
649 </hl7:agentOrganization>
650 </hl7:acknowledgement>
651 </hl7:controlActEvent>
652 </hl7:registrationEvent>
653 </hl7:subject>
654 </hl7:subjectOf>
655 </hl7:identifiedEntity>
656 </hl7:subject>
657 </hl7:agent>
658 </hl7:agentOrganization>
659 </hl7:acknowledgement>
660 </hl7:controlActEvent>
661 </hl7:registrationEvent>
662 </hl7:subject>
663 </hl7:subjectOf>
664 </hl7:identifiedEntity>
665 </hl7:subject>
666 </hl7:agent>
667 </hl7:agentOrganization>
668 </hl7:acknowledgement>
669 </hl7:controlActEvent>
670 </hl7:registrationEvent>
671 </hl7:subject>
672 </hl7:subjectOf>
673 </hl7:identifiedEntity>
674 </hl7:subject>
675 </hl7:agent>
676 </hl7:agentOrganization>
677 </hl7:acknowledgement>
678 </hl7:controlActEvent>
679 </hl7:registrationEvent>
680 </hl7:subject>
681 </hl7:subjectOf>
682 </hl7:identifiedEntity>
683 </hl7:subject>
684 </hl7:agent>
685 </hl7:agentOrganization>
686 </hl7:acknowledgement>
687 </hl7:controlActEvent>
688 </hl7:registrationEvent>
689 </hl7:subject>
690 </hl7:subjectOf>
691 </hl7:identifiedEntity>
692 </hl7:subject>
693 </hl7:agent>
694 </hl7:agentOrganization>
695 </hl7:acknowledgement>
696 </hl7:controlActEvent>
697 </hl7:registrationEvent>
698 </hl7:subject>
699 </hl7:subjectOf>
700 </hl7:identifiedEntity>
701 </hl7:subject>
702 </hl7:agent>
703 </hl7:agentOrganization>
704 </hl7:acknowledgement>
705 </hl7:controlActEvent>
706 </hl7:registrationEvent>
707 </hl7:subject>
708 </hl7:subjectOf>
709 </hl7:identifiedEntity>
710 </hl7:subject>
711 </hl7:agent>
712 </hl7:agentOrganization>
713 </hl7:acknowledgement>
714 </hl7:controlActEvent>
715 </hl7:registrationEvent>
716 </hl7:subject>
717 </hl7:subjectOf>
718 </hl7:identifiedEntity>
719 </hl7:subject>
720 </hl7:agent>
721 </hl7:agentOrganization>
722 </hl7:acknowledgement>
723 </hl7:controlActEvent>
724 </hl7:registrationEvent>
725 </hl7:subject>
726 </hl7:subjectOf>
727 </hl7:identifiedEntity>
728 </hl7:subject>
729 </hl7:agent>
730 </hl7:agentOrganization>
731 </hl7:acknowledgement>
732 </hl7:controlActEvent>
733 </hl7:registrationEvent>
734 </hl7:subject>
735 </hl7:subjectOf>
736 </hl7:identifiedEntity>
737 </hl7:subject>
738 </hl7:agent>
739 </hl7:agentOrganization>
740 </hl7:acknowledgement>
741 </hl7:controlActEvent>
742 </hl7:registrationEvent>
743 </hl7:subject>
744 </hl7:subjectOf>
745 </hl7:identifiedEntity>
746 </hl7:subject>
747 </hl7:agent>
748 </hl7:agentOrganization>
749 </hl7:acknowledgement>
750 </hl7:controlActEvent>
751 </hl7:registrationEvent>
752 </hl7:subject>
753 </hl7:subjectOf>
754 </hl7:identifiedEntity>
755 </hl7:subject>
756 </hl7:agent>
757 </hl7:agentOrganization>
758 </hl7:acknowledgement>
759 </hl7:controlActEvent>
760 </hl7:registrationEvent>
761 </hl7:subject>
762 </hl7:subjectOf>
763 </hl7:identifiedEntity>
764 </hl7:subject>
765 </hl7:agent>
766 </hl7:agentOrganization>
767 </hl7:acknowledgement>
768 </hl7:controlActEvent>
769 </hl7:registrationEvent>
770 </hl7:subject>
771 </hl7:subjectOf>
772 </hl7:identifiedEntity>
773 </hl7:subject>
774 </hl7:agent>
775 </hl7:agentOrganization>
776 </hl7:acknowledgement>
777 </hl7:controlActEvent>
778 </hl7:registrationEvent>
779 </hl7:subject>
780 &lt
```

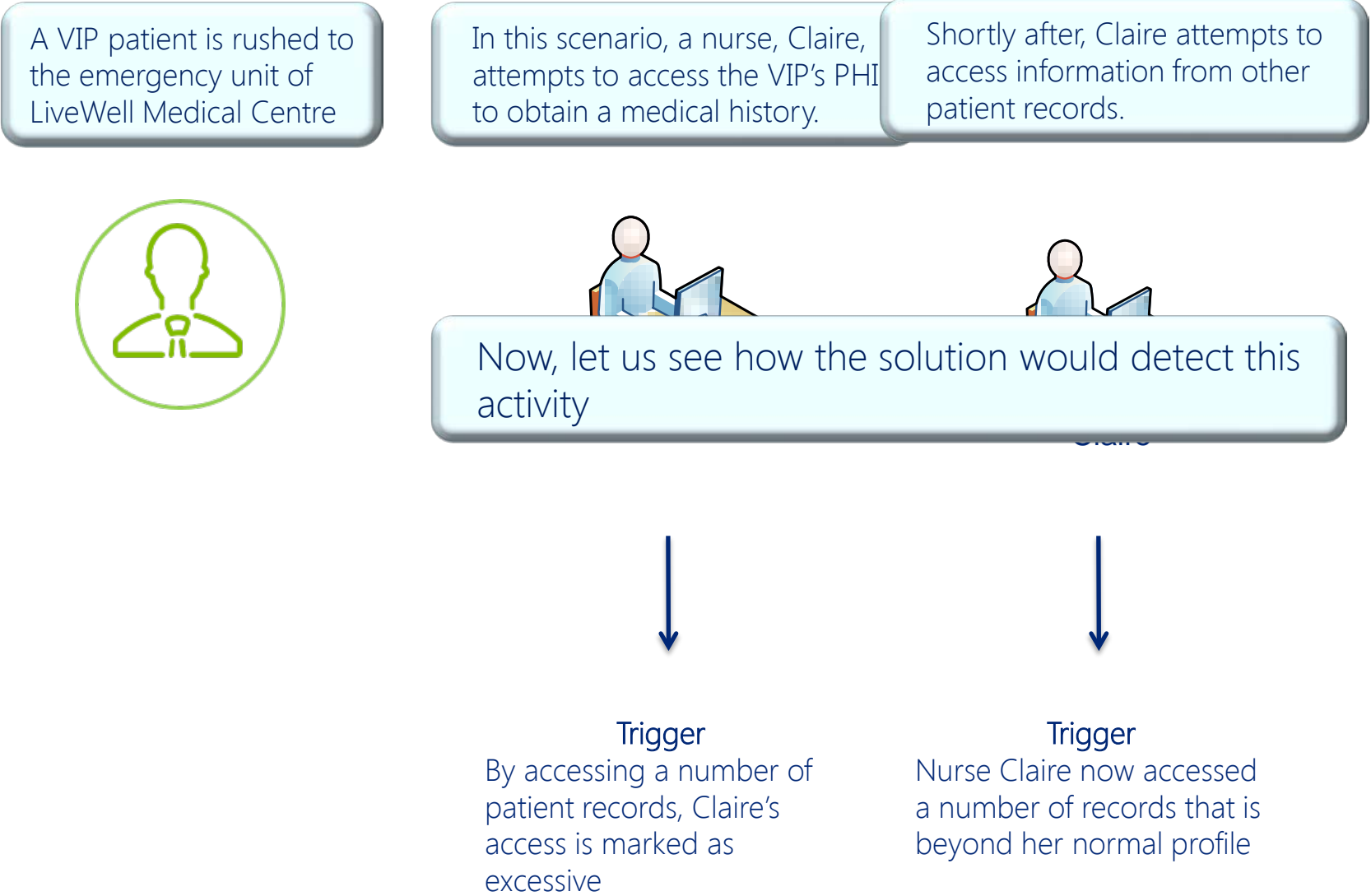


Use case walkthrough



Excessive access attempts to PHI leads to detecting an insider threat

User Story



Excessive access attempts to PHI leads to detecting an insider threat

The PHI monitoring solution extracts the relevant information from the health message to create corresponding audit event records:

Start Time:7 Apr 2015 16:50:00 EDT

End Time:7 Apr 2015 17:21:00 EDT

Filter:MatchesFilter ('PHI Transaction Events')

Online Filter: No Filter

Excessive access attempts to PHI leads to detecting an insider threat

The PHI monitoring solution triggers an alert based on the use case. The trigger identifies the base events associated to the alert:

The screenshot displays a security monitoring interface with several panels. At the top, there are tabs for 'PCR - Details Details', 'PCR - IDs Details', 'PR - Details Details', 'PR - IDs Details', and 'Notifications'. Below these, there are tabs for 'ThreatContent01', 'ThreatContent01_CorrelatedEvents', and 'TC01_ExcessiveAccessAttemptsToPHI'. The 'Active Channel: ThreatContent01_CorrelatedEvents' is selected, showing a 'Total Events: 1' and a 'Filter: (MatchesFilter ("Application Correlated Events") And Name StartsWith "ThreatContent_01")'. The 'Radar' section shows a single event. The 'Event Inspector' panel on the right shows a list of events, with 'ThreatContent_01 - Investigate 3004975' selected. This event is associated with five 'PHI Transaction Event' entries. The 'Event Details' panel shows the event name as 'ThreatContent_01 - Investigate 3004975', the message as 'Excessive Access Attempts To PHI by user: "nurse_csaunders" Detected', and the priority as 7.

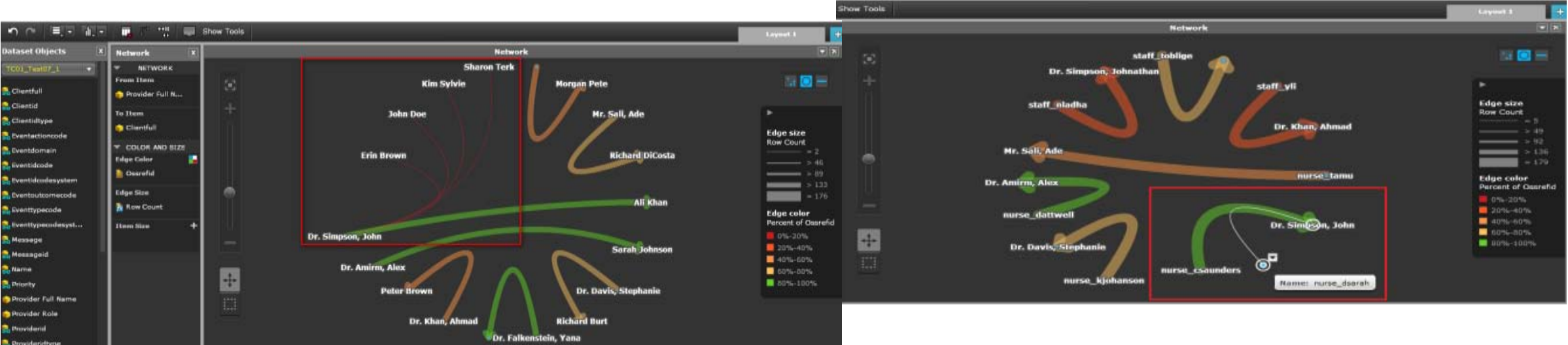
Time of Event	Name	Event ID	Message	Type
7 Apr 2015 17:18:23 EDT	ThreatContent_01 - Investigate 3004975	3004975	Excessive Access Attempts To PHI by user: "nurse_csaunders" Detected	Correl

Name	Value
Event	
Name	ThreatContent_01 - Investigate 3004975
Message	Excessive Access Attempts To PHI by user: "nurse
Threat	
Priority	7

Since Clair Saunders has an established limit of four (4) records to be accessed at a time, in this case, Clair has exceeded her limit by requesting access to five (5) patient records within a particular time period.

Excessive access attempts to PHI leads to detecting an insider threat

The privacy analyst investigates the occurrence leveraging analytics to identify patterns of access trends. The analyst identifies a trend where a particular provider is found to use multiple users to access patient records.



The analyst informs the Privacy office of the findings of the violation and confirms a closure of the incident investigation.

Pending (0)	Undeliverable (4359)	Not Acknowledged (0)	Acknowledged (1)	Resolved (308)	Informational (0)

Resolve

View Event

Help

Severity	Triggering Event	Notification Group	Escalation Level	CreateTime
High	ThreatContent_01 - ...	SOC Operators	1	4/7 17:18:46

Summary:

The PHI monitoring solution allows the analyst to confirm the threat scenario and identify root causes. In this example, Claire Saunders was being used as a proxy by Dr. Simpson, John, to access patient records on behalf of him. The Provider, Dr. Simpson, John should be further investigated, as opposed to Claire Saunders.



Is this solution for you?





Do you have visibility into who and when patient health records are accessed?



Has your institution performed a privacy impact analysis of a data breach?



Is your institution expending or anticipate spending material resources for addressing privacy concerns?



Patient record privacy and increased regulatory concerns?



Can withstand regulatory scrutiny?



Ability to attract and retain proper cyber security talents?



Q & A



Thank you



Beth Dewitt
Senior Manager
Data Protection and Privacy
bdewitt@deloitte.ca
1-416-643-8223



Ali Khan
Manager
Cyber Security
aliukhan@deloitte.ca
1-647-880-9149

Deloitte.

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 7,600 people in 57 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. Deloitte & Touche LLP, an Ontario Limited Liability Partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte & Touche LLP and affiliated entities.

Implementing a privacy monitoring solution will:

- ✓ Eliminate **manual monitoring** that is work-intensive and ineffective
- ✓ Support organizations in **meeting privacy compliance requirements**
- ✓ Provide a mechanism to **detect privacy breaches**
- ✓ **Reduce** possibility of **legal action**
- ✓ Ensure patient and provider's **trust** in the integrity of data and delivery of health care
- ✓ Systematically **identify users** who are engaging in patient access patterns that are indicative of snooping, identity theft or other risky behaviors
- ✓ **Address false positives** and bring potential incidents to the attention of appropriate privacy or compliance personnel
- ✓ Automate the **work-flow** and enhance enterprise risk management posture
- ✓ Enable **proactive** risk management processes

The solution is customizable and integrates with CIS and broader EHR platforms.