

Cybersecurity in healthcare: a narrative review of trends, threats and ways forward

Professor Lynne Coventry and Dr. Dawn Branley

Corresponding author

Lynne.coventry@northumbria.ac.uk

153 Northumberland Building, Northumbria University, Newcastle upon Tyne, NE1 8ST

Electronic healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery. However, there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities. Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data and its defences are weak. Cybersecurity breaches include stealing health information, ransomware attacks on hospitals and potential attacks on implanted medical devices. Breaches can reduce patient trust, cripple health systems and threaten human life. Ultimately, cybersecurity is critical to patient safety, yet has historically been lax. New legislation and regulations are in place to facilitate change. This requires cybersecurity to become an integral part of patient safety. Changes are required to human behaviour, technology and processes as part of a holistic solution.

Introduction

Healthcare technologies have the potential to extend, save and enhance lives. Technologies range from those providing storage of electronic health records (EHRs); devices that monitor health and deliver medication (including general purpose devices and wearables, and technology embedded within the human body); to telemedicine technology delivering care remotely - even across countries. Patients increasingly use their own mobile applications, which can now be integrated with telemedicine/telehealth into the medical Internet of Things [1] for collaborative disease management and care coordination.

As healthcare devices continue to evolve, so does their interconnectivity. Whilst traditionally standalone, many are now integrated into the hospital network. There are currently 10-15 connected devices per bed in US hospitals [2]. Interconnection has many benefits - e.g., efficiency, error reduction, automation and remote monitoring. These benefits are transforming the treatment of both acute and chronic long-term conditions. Interconnected technology outside of the clinical environment allow health professionals to monitor and adjust implanted devices without the need for a hospital visit or invasive procedures. EHRs can improve patient care by making health information more broadly available [3]. Unfortunately, interconnection introduces new cybersecurity vulnerabilities. Cybersecurity is concerned with safeguarding computer networks and the information they contain from penetration and accidental or malicious disruption. There are growing concerns that cybersecurity within healthcare is not sufficient and this has already resulted in a lack of medical information confidentiality [4] and integrity of data [5,6].

Of course, privacy breaches were a concern prior to the emergence of digital health records. However, the interconnectivity of today's records provides multiple potential gateways to access; the ability to access remotely (whereas historically paper records would have been safeguarded

60
61
62 within hospitals and only accessible via physical breaches); the ability for data theft to go unnoticed;
63 and access to a more complete health record providing a more valuable resource for potential
64 attacks (whereas previously health records may have been split between many different
65 hospital(s)/departments). Historically, misplaced paper records or a stolen laptop may have exposed
66 hundreds or thousands of patients to a potential data breach, now that this information is electronic
67 and available on numerous networks, a privacy breach has the potential to affect millions of people
68 [7]. To illustrate further, celebrity health records have always been a target for breaches [8].
69 However prior to the emergence of electronic records, these breaches were limited to hospital staff
70 who could gain access to the physical paperwork. Now celebrity health records can be potentially
71 remotely accessed – increasing the potential for breaches. That said, electronic records also have a
72 key privacy benefit over paper records – the ability to track staff access (a recent report suggests
73 that over half of healthcare breaches come from inside the organisation [8]). Whereas previously it
74 could be difficult to detect who had a ‘sneak peek’ at paper medical records, it is often easier to
75 track who has accessed electronic records. Although there are ways around this for more
76 sophisticated/external attackers.

77
78
79 As illustrated by breaches reported in the media, cybersecurity vulnerabilities are being exploited.
80 Healthcare is currently one of the most targeted sectors. Reports highlight the growth of attacks and
81 the rise in medical identity theft - with millions of medical records stolen globally [9–12]. Breaches
82 can arise from hacking, malware and insider threats. Hacking is defined as unauthorised access to a
83 computer system to gain information or cause disruption [13]. Malware (“malicious software”)
84 refers to programs designed to infiltrate computers without users’ consent and includes threats such
85 as viruses and ransomware. While insider threats are issues created by the mistakes or deliberate
86 actions of staff (e.g., responding to phishing emails - a social engineering attack to extract login
87 credentials or to launch a malware attack, erroneous security settings, misuse of passwords, losing
88 laptops and sending unencrypted emails).

89
90
91 The aim of this narrative review is to explore the following questions:

- 92 1. Why is healthcare vulnerable?
- 93 2. Why is healthcare targeted?
- 94 3. What threats and consequences is healthcare currently experiencing?
- 95 4. What is the role of legislation and standards?
- 96 5. How can the healthcare sector move forward?

97 98 99 Method

100 Data sources and search strategy

101 The PubMed database was searched for full text, English language, peer-reviewed articles from April
102 2012 to April 2018. The keywords used were cybersecurity and healthcare. This returned 2475 hits.
103 Since cybersecurity is constantly changing, this was changed to 2014-2018 which reduced the return
104 to 1249 articles. The bibliographies of key texts were then used to source further articles.

105
106
107 Article titles and abstracts were screened by the principal researcher. Articles were retained where
108 there was evidence of cybersecurity issues, clear implications for healthcare settings, organisational
109 practice, individual practice or health technology development. Also included were systematic
110 reviews regarding the education and behaviour of healthcare workers. Security research papers
111 exploring future technological solutions were excluded as were articles relating to medical research.
112 Key themes were agreed by consensus between the two researchers to limit bias.

Findings

The review of the literature revealed the following information relating to the research questions:

Why is healthcare vulnerable?

Traditionally people believed that no one would be motivated to attack healthcare systems and protective measures were not deemed necessary. No healthcare organisation exists to provide cybersecurity. Emphasis has traditionally – and understandably – been focused upon patient care. There are several issues that complicate healthcare cybersecurity and have increased vulnerability over time:

- Increasingly connected technology to provide efficient ways to care for patients, particularly with chronic conditions [14]. This provides multiple ways of connecting to medical devices [15]. Devices are often easily accessible which increases the likelihood that attackers will find them. A single device could provide a potential entry point to larger hospital networks, bypassing the firewalls. There also tends to be a time lag between an attack occurring and detection of the breach, helping to further increase vulnerability.
- More focus on keeping patients healthy leading to more continuous patient monitoring outside the clinical environment [14,16]. More devices being used in the wider healthcare setting increases vulnerability to breaches.
- Mobile consumer devices (e.g., smartphones) being widely adopted; making it difficult to protect health data from risks posed by general purpose devices [14]

Alongside this growth of new technologies, many healthcare organisations are still using legacy systems in other areas, for example Window XP has not been supported since 2014 [17] allowing hackers and malware to easily avoid detection – for instance, the recent Wannacry attack [18]. The propriety nature of medical device software means that healthcare IT teams may not be able to access the internal software in medical devices, so they depend on manufacturers to build and maintain security in those devices (which has been lacking).

Lack of funding for cybersecurity is also problematic, while organisations are spending funding to become more integrated; they are not spending enough time and money to keep software updated and systems secure. This is aggravated by a lack of cybersecurity expertise within the sector resulting from a general lack of technology and the prohibitive expense of cybersecurity personnel [14,19].

In summary, a rapid move to electronic health records and interconnected devices, alongside historic and continual lack of investment in cybersecurity and a failure to understand the security workaround behaviours of health staff has left the health sector vulnerable to attack.

Why is healthcare targeted?

While healthcare has vulnerabilities to exploit, attackers must be motivated to carry out attacks. Motivation includes the potential for financial and political gain and potentially to take lives in a form of cyberwarfare. The strongest of these motivations is financial gain. Healthcare data is substantially more valuable than any other data. The value for a full set of medical credentials can be over \$1000 [20]. Stolen medical identities can be used to obtain health services and prescription medication by assuming someone's identity or insurance credentials. Uses extend to sophisticated fraud perpetrated by organized crime. Fraudsters have earned billions in the last few years by filing fraudulent claims and dispensing drugs to sell on the dark web [21–23]. Sometimes there is even

178
179
180 sufficient information in medical records to open bank accounts, secure loans or obtain passports
181 [24].
182

183 Data held within health organisations also has political value. For example, the World Anti-Doping
184 Agency was attacked and the records of prominent athletes made public [25]. NHS websites are
185 accessed by millions of citizens, making them a prime site for publishing propaganda, e.g., NHS
186 websites were hacked by cyberterrorists and images of Syrian civil war were uploaded [26].
187

188 Over the past decade we have seen numerous headlines warning of the potential for medical
189 devices to be used as part of a futuristic cyberwar campaign. Nation state actors could disrupt
190 healthcare in a foreign country by denying access or targeting individuals through their medical
191 devices, or by collecting sensitive data.
192

193 Those with cybersecurity skills enjoy the challenge of finding and exposing security vulnerabilities in
194 networks and medical devices. For example, in 2016 an individual scanning for security
195 vulnerabilities was able to access a file containing data of people who had registered with the
196 Australian Blood Donor service [27].
197

198 In summary, healthcare is targeted due to the potential for financial or political gain, or to expose
199 vulnerabilities by cybercriminals, hacktivists and political activists.
200

201 What threats and consequences is healthcare currently facing?

202 As of 2015, hacking has become the leading cause of health data breaches [28]. Malware including
203 ransomware is also problematic. Hackers continue to take advantage of lax security to steal medical
204 health records, deny access to health services or cause intentional harm. Over the last few years the
205 health sector has experienced a dramatic rise in the number and size of data breaches [11,12,29].
206 Breaches result in financial loss, loss of reputation and reduced patient safety. In Australia the
207 medical card number of every citizen is reportedly for sale on the dark web [30]. Ponemon Institute
208 recently reported the average cost for each lost or stolen healthcare record containing sensitive and
209 confidential information as \$380 [31]. Ongoing publicity associated with large breaches may
210 compromise patient trust which could result in less willingness to share data. This is particularly
211 problematic for patients with stigmatising conditions such as sexual or mental health conditions [3].
212
213

214 Despite issued warnings and availability of security patches (many not installed), the scale of the
215 2017 WannaCry attack was unprecedented. WannaCry infected more than 300,000 computers
216 across the world demanding that users pay bitcoin ransoms [32]. Fifty UK hospitals experienced
217 system-wide lockouts, delays to patient care and function loss in connected devices such as MRI
218 scanners and blood storage refrigerators. This attack was not specifically directed at healthcare
219 organisations, yet the damage was widespread. Other ransomware has specifically targeted the
220 healthcare sector. Mansfield-Devine reports that between 2015 and 2016, half of UK NHS trusts
221 were hit by some form of ransomware [33]. While US media highlighted the case of the Hollywood
222 Presbyterian Medical Centre shut down for 10 days until it paid a \$17,000 ransom; in an attack
223 thought to have originated from a phishing email [34].
224
225

226 Other malware attacks have led to major incidents, for example one UK healthcare trust suffered an
227 unspecified cyberattack which led to the shutdown of its IT systems and cancellation of almost all
228 planned operations and outpatient appointments for four days [35]. Another attack known as
229 Medjack ("Medical Device Hijack") is an exploit that injects malware into unprotected medical
230 devices to move laterally across the hospital network [36]. Infected medical devices created weak
231 links in hospital security defences, including diagnostic equipment (e.g., MRI machines), therapeutic
232 equipment (e.g., infusion pumps) and life support equipment (e.g., ventilators). This equipment had
233
234
235
236

237
238
239 not been previously identified as a launchpad for wider attacks. Infection can then spread to other
240 devices, for instance to a nurse's workstation - which has access to medical records and internet
241 access to send the data to the attackers.
242

243 'White hacker' simulated attacks have highlighted that other vulnerabilities exist which mean that
244 "Medical devices are the next security nightmare" [37]. There is potential for attacks akin to what
245 was previously regarded as science fiction. For example, brainjacking - if it became possible to insert
246 an appropriate device [38]. Simulated attacks have been made on devices including pacemakers and
247 defibrillators [39], insulin pumps [40-42] and drug infusion pumps. These attacks have remotely
248 manipulated devices to alter operation or send fatal drug doses. While currently only simulated,
249 these attacks could happen in reality [43]. Risks will continue to grow if cybersecurity is not designed
250 in from the beginning of the product or project lifecycle.
251

252 What is the role of legislation and standards?

253 The US Health Insurance Portability and Accountability Act of 1996 [44] implemented safeguards to
254 ensure that certain electronic health information is protected. The Security Rule requires covered
255 entities to maintain reasonable and appropriate administrative, technical, and physical safeguards to
256 ensure the confidentiality, integrity, and availability of EHRs that they create, receive, maintain or
257 transmit.
258
259

260 The upcoming General Data Protection Regulation (GDPR) also comes into effect in the UK in May
261 2018. The GDPR is designed to harmonise data privacy laws across Europe to protect against privacy
262 and data breaches [45]. The GDPR aims to accomplish this by addressing gaps in the current
263 legislation, which was released in the 1990s prior to organisations holding vast electronic data. The
264 GDPR applies to all personal data held by an organisation. As part of the new legislation, 'all
265 breaches which may result in a risk to peoples' rights and freedoms' must be reported to the
266 Information Commissioner's Office (ICO). Breaches of health data would likely fall into this category,
267 therefore they will need to be reported to the ICO within 72 hours of the breach occurring. Non-
268 compliance risks fines of up to €20m. Other changes include the need for all practices to have a data
269 protection officer and the introduction of extra 'transparency and fair processing' legislation which
270 need to be included in patient privacy notices [45]. This new legislation will significantly increase the
271 cost of breaches (due to implemented fines) and may help to increase awareness around privacy
272 issues and the need for improved cybersecurity. As the NHS moves towards its aspiration of EHRs -
273 there are concerns around patient privacy and consent and the sharing of data with other
274 organisations [46]. As part of the national data opt-out scheme, patients must be given the choice to
275 opt out of their personal data being shared for purposes other than their individual care. Under the
276 GDPR, any request for data from an external organisation must be given in clear and easily accessible
277 language, including the purpose for requiring the data. This will allow clinicians to uphold patients'
278 data preferences. That said, it has been suggested that changes in infrastructure are required before
279 EHRs will becoming a useful reality. This is due to the NHS using different providers and different
280 systems, for example two labs may measure the same thing using very different scales; making it
281 difficult for two separate labs to share data in any meaningful fashion [46].
282
283
284
285

286 When it comes to medical devices, the US Food and Drug Administration (FDA) places responsibility
287 for cybersecurity with the medical product manufacturer. The FDA has published premarket [47] and
288 postmarket guidelines [48] that contain recommendations for management of medical device
289 cybersecurity risks throughout the product life cycle. This includes encouraging people to report
290 cybersecurity issues and making it mandatory for manufacturers and device user facilities to report
291 any device malfunction if it poses a risk to health.
292
293
294
295

296
297
298
299
300
301
302
303
304
305

European regulators have published high-level cybersecurity recommendations for industries including medical devices involved in the Internet of Things (IoT) paradigm. The recommendations are partially intended to help companies meet upcoming European data privacy requirements under the GDPR. How can the healthcare sector move forward?

306
307
308
309
310

There is no 100% effective way to prevent all cybersecurity breaches but cybersecurity must form part of the risk management process and cyber resilience must be ensured. Cyber resilience is a holistic view of cyber risk, which looks at culture, people and processes, as well as technology [49]. Several factors have been identified as a means to improve the situation:

311
312
313
314
315
316
317
318

As a minimum, basic cyber-hygiene must be maintained, see the 10 steps from the National Cyber Security Centre [50]. This includes regular, secure backups (essential to maintain resilience and be able to recover quickly if attacked) and keeping software up to date to ensure security patches are in place. Confidentiality must be maintained. This can be achieved through anonymization of data (including images), removal of patient identifiers when used for research purposes, and limiting access to online patient information. This requires investing in systems and processes which support secure data transfer (e.g., e-mail encryption and protection of online data).

319
320
321
322
323
324
325
326
327

Security must be a core part of the product lifecycle. This requires considering the trade-offs between security and other requirements from the start[51]. Appropriate incentives should ensure that future devices and networks have robust security designed in from the start and that these are not added later in a 'bolt on' fashion. This could be driven by security standards for information management, which take into consideration the unique healthcare context that tends to prioritise availability over confidentiality. Any standards, regulations or rules must ease burdensomeness and prevent temptation for staff to engage in insecure workarounds.

328
329
330
331
332
333
334
335
336
337
338
339
340
341
342

Cybersecurity should be a key part of patient care culture as convenient and insecure processes must be replaced with more secure, substantive approaches. This means not simply being seen to be secure (for example to comply with regulations) but building security into the culture. Levin & Christmann [52] point out that this may require active inspections and enforcement from accredited bodies. Culture change must be from the top-down and metrics should be applied through the Care Quality Commission [53] or similar to ensure effective engagement. An effective security culture has the potential to enhance employees acting in effect as a 'human firewall' that can help to protect electronic assets. This includes staff not being logged in as a domain administrator; no sharing of login credentials; and regular staff training to communicate the risks presented by lax security behaviours and how security can be attained without compromising patient care. It is possible that more sophisticated security logins (e.g., retinal imaging, fingerprints, face identification) could be used to prevent the sharing of logins and passwords. The recruitment of security personnel is also required.

343
344
345
346
347
348

Cyber-insurance is a rapidly growing business with estimated global sales of \$7.5 billion by 2020 [49]. With the losses associated with cyber breaches, more companies are turning towards insurance. Security improvements may be driven through appropriate insurance incentives. Protection against the consequences of cyberattacks may be part of the liabilities insured against in the same way as hospitals are insured against claims of criminal negligence [53]

349
350
351
352
353
354

Ponemon Institute [31] suggests the cost of a data breach could be reduced through participation in threat sharing. This could be facilitated through national support for incident reporting and

355
356
357 management. For instance in the UK, a Care CERT has been set up [54]. However, a joined up
358 approach to the creation of local and national response plans for major cyber-incidents should be in
359 place [55].
360

361 Limitations of this review

362 Due to the scope of this review, only English publications were included for analysis. Future work
363 should seek to broaden this further. Whilst we acknowledge that viewpoints and commentaries are
364 not scientific evidence, this is where the majority of information around healthcare technology
365 currently lies. Therefore, this approach was deemed appropriate to provide an overall view of the
366 current body of knowledge, the key issues around health technology security and to highlight areas
367 for moving forward.
368
369

370 Conclusions

371 While healthcare technologies play key roles in our population's health they are vulnerable to
372 security threats due to interconnected, easily accessible access points, outdated systems, and a lack
373 of emphasis upon cybersecurity. Focus has tended to be placed upon patient care, however
374 healthcare technologies hold vast amounts of valuable, sensitive data. In many cases financial gain is
375 the motivation for attacks, as medical identity is more valuable than other identity credentials. Other
376 attacks may be motivated by political gain, even cyberwarfare. However if critical health systems are
377 attacked, human lives are at risk. An attack could result in loss of functioning of critical equipment
378 within hospitals such as intensive care units or even at home where interventions rely on power
379 such as nebulisers [56].
380
381

382 The escalation of ransomware attacks on hospitals can bring whole health systems to a standstill as
383 seen in both the UK and US [57,58]. Concern has been further increased by 'White Hacker'
384 identification of health technology security weaknesses, which suggest that the remote
385 manipulation of medical devices such as pace makers and insulin pumps is an unnerving possibility.
386

387 Cybersecurity is an essential part of maintaining the safety, privacy and trust of patients. More
388 money and effort must be invested into ensuring the security of healthcare technologies and patient
389 information. Security must be designed into the product from conception and not be an
390 afterthought. Cybersecurity must become part of the patient care culture.
391

392 Funding

393 There is no funding associated with this research.
394
395

396 References

- 397
398 [1] D. V Dimitrov, Medical Internet of Things and Big Data in Healthcare., *Healthc. Inform. Res.* 22
399 (2016) 156–63. doi:10.4258/hir.2016.22.3.156.
400
401 [2] T. Walker, Interoperability a must for hospitals, but it comes with risks, *Manag. Healthc. Exec.*
402 (2017). [http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-](http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/interoperability-must-hospitals-it-comes-risks)
403 [executive/news/interoperability-must-hospitals-it-comes-risks](http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/interoperability-must-hospitals-it-comes-risks) (accessed February 28, 2018).
404
405 [3] A. Shenoy, J.M. Appel, Safeguarding confidentiality in electronic health records, *Cambridge Q.*
406 *Healthc. Ethics.* 26 (2017) 337–341. doi:10.1017/S0963180116000931.
407
408 [4] C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monticone, Cybersecurity in healthcare: A
409 systematic review of modern threats and trends, *Technol. Heal. Care.* 25 (2017) 1–10.
410 doi:10.3233/THC-161263.
411
412
413

- 414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
- [5] R.S. Ross, L. Feldman, G.A. Witte, Rethinking Security through Systems Security Engineering, ITL Bull. - December 2016. (2016). <https://www.nist.gov/publications/rethinking-security-through-systems-security-engineering> (accessed March 2, 2018).
- [6] Ò. Solans Fernández, C. Gallego Pérez, F. García-Cuyàs, N. Abdón Giménez, M. Berruezo Gallego, A. Garcia Font, M. González Quintana, S. Hernández Corbacho, E. Sarquella Casellas, Shared Medical Record, Personal Health Folder and Health and Social Integrated Care in Catalonia: ICT Services for Integrated Care, in: Springer, Cham, 2017: pp. 49–64. doi:10.1007/978-3-319-28661-7_4.
- [7] R. Kam, The human risk factor of a healthcare data breach - Community Blog, Heal. IT Exch. (2015). <https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-human-risk-factor-of-a-healthcare-data-breach/> (accessed April 10, 2018).
- [8] R.Z. Arndt, In healthcare, breach dangers come from inside the house, Mod. Healthc. (2018). <http://www.modernhealthcare.com/article/20180410/NEWS/180419999> (accessed April 10, 2018).
- [9] B.L. Filkins, J.Y. Kim, B. Roberts, W. Armstrong, M.A. Miller, M.L. Hultner, A.P. Castillo, J.-C. Ducom, E.J. Topol, S.R. Steinhubl, Privacy and security in the era of digital health: what should translational researchers know and do about it?, Am. J. Transl. Res. 8 (2016) 1560–80. <http://www.ncbi.nlm.nih.gov/pubmed/27186282> (accessed February 19, 2018).
- [10] R. Abelson, M. Goldstein, Anthem hacking points to security vulnerabilities of healthcare industry, New York Times. (2015). <http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html>.
- [11] G. Bell, M. Ebert, Health Care and Cyber Security, 2015. <https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf>.
- [12] Ponemon Institute, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, 2016. <https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1> (accessed February 19, 2018).
- [13] P.A. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem., Med. Devices (Auckl). 8 (2015) 305–16. doi:10.2147/MDER.S50048.
- [14] D. Kotz, C.A. Gunter, S. Kumar, J.P. Weiner, Privacy and Security in Mobile Health: A Research Agenda., Computer (Long. Beach. Calif). 49 (2016) 22–30. doi:10.1109/MC.2016.185.
- [15] A.J. Burns, M.E. Johnson, P. Honeyman, A brief chronology of medical device security, Commun. ACM. 59 (2016) 66–72. doi:10.1145/2890488.
- [16] A. Coulter, S. Roberts, A. Dixon, Delivering better services for people with long-term conditions Building the house of care, (2013). https://www.kingsfund.org.uk/sites/default/files/field/field_publication_file/delivering-better-services-for-people-with-long-term-conditions.pdf (accessed February 28, 2018).
- [17] R. Milliman, Nine in 10 NHS trusts still use Windows XP, IT Pro. (2016). <http://www.itpro.co.uk/public-sector/27740/nine-in-10-nhs-trusts-still-use-windows-xp> (accessed February 19, 2018).
- [18] National Audit Office, Investigation: WannaCry cyber attack and the NHS, 2017. <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf> (accessed January 24, 2018).

- 473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
- [19] H. Landi, Healthcare Industry Faces Shortage in Experienced Cybersecurity Experts, 2015. <https://www.healthcare-informatics.com/news-item/healthcare-industry-faces-shortage-experienced-cybersecurity-experts> (accessed February 19, 2018).
 - [20] A. Sulleyman, NHS cyber attack: Why stolen medical information is so much more valuable than financial data | The Independent, Indep. (2017). <http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html> (accessed February 19, 2018).
 - [21] J. Berlinger, Justice Department files record \$900 million healthcare fraud case, CNN. (2016). <http://edition.cnn.com/2016/06/23/health/health-care-fraud-takedown/index.html> (accessed February 19, 2018).
 - [22] Kindus, Medical Identity Theft, 2015. <https://kindus.co.uk/assurance/medical-identity-theft/> (accessed February 19, 2018).
 - [23] US Department of Justice, Three Individuals Charged in \$1 Billion Medicare Fraud and Money Laundering Scheme, (2016). <https://www.justice.gov/opa/pr/three-individuals-charged-1-billion-medicare-fraud-and-money-laundering-scheme> (accessed February 19, 2018).
 - [24] E. Kangas, Why Are Hackers Targeting Your Medical Records?, 2017. <https://luxsci.com/blog/hackers-targeting-medical-records.html> (accessed February 19, 2018).
 - [25] BBC, Wiggins and Froome medical records released by “Russian hackers,” BBC. (2016). <http://www.bbc.co.uk/news/world-37369705> (accessed February 19, 2018).
 - [26] K. Sengupta, Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images, Indep. (2017). <http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html> (accessed February 19, 2018).
 - [27] M. Davey, Red Cross Blood Service data breach: personal details of 550,000 blood donors leaked, Guard. (2016). <https://www.theguardian.com/australia-news/2016/oct/28/personal-details-of-550000-red-cross-blood-donors-leaked-in-data-breach> (accessed February 19, 2018).
 - [28] E. Snell, Hacking Still Leading Cause of 2015, Heal. IT Secur. (2015). <https://healthitsecurity.com/news/hacking-still-leading-cause-of-2015-health-data-breaches> (accessed February 19, 2018).
 - [29] HHS, Ransomware and HIPAA, 2016. <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (accessed February 19, 2018).
 - [30] P. Farrell, The Medicare machine: patient details of “any Australian” for sale on darknet, Guard. (2017). <https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet> (accessed March 2, 2018).
 - [31] Ponemon Institute, 2017 Cost of Data Breach Study: United States, 2017. <https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states> (accessed February 19, 2018).
 - [32] M. Scott, N. Wingfield, Hacking attack has security experts scrambling to contain fallout., New York Times. (2017). <https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html>.

- 532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
- [33] S. Mansfield-Devine, Ransomware: taking businesses hostage, *Netw. Secur.* 2016 (2016) 8–17. doi:10.1016/S1353-4858(16)30096-4.
 - [34] R. Winton, Hollywood hospital pays \$17,000 in bitcoin to hackers; FBI investigating, *Los Angeles Times*. (2016). <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html> (accessed February 19, 2018).
 - [35] L. Evenstad, NHS trust recovers after cyber attack, *Comput. Wkly.* (2016). <http://www.computerweekly.com/news/450402278/NHS-trust-recovers-after-cyber-attack> (accessed February 19, 2018).
 - [36] D. Storm, MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks, *Comput. World.* (2015) 8. <https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html> (accessed February 19, 2018).
 - [37] L.H. Newman, Medical Devices Are the Next Security Nightmare, *Wired.* (2017). <https://www.wired.com/2017/03/medical-devices-next-security-nightmare/> (accessed January 24, 2018).
 - [38] L. Pycroft, S.G. Bocard, S.L.F. Owen, J.F. Stein, J.J. Fitzgerald, A.L. Green, T.Z. Aziz, Brainjacking: Implant Security Issues in Invasive Neuromodulation, *World Neurosurg.* 92 (2016) 454–462. doi:10.1016/j.wneu.2016.05.010.
 - [39] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W.H. Maisel, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, in: 2008 IEEE Symp. Secur. Priv. (Sp 2008), IEEE, 2008: pp. 129–142. doi:10.1109/SP.2008.31.
 - [40] J. Finkle, Johnson & Johnson letter on cyber bug in insulin pump, 2016. <https://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-t/johnson-johnson-letter-on-cyber-bug-in-insulin-pump-idUKKCN12414G> (accessed February 19, 2018).
 - [41] A. Parmar, Hacker shows off vulnerabilities of wireless insulin pumps, *MedCity News.* (2012). <https://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps/> (accessed February 19, 2018).
 - [42] D. Takahashi, Excuse me while I turn off your insulin pump, *Ventur. Beat.* (2011). <https://venturebeat.com/2011/08/04/excuse-me-while-i-turn-off-your-insulin-pump/> (accessed March 2, 2018).
 - [43] D.C. Klonoff, Cybersecurity for Connected Diabetes Devices, *J. Diabetes Sci. Technol.* 9 (2015) 1143–1147. doi:10.1177/1932296815583334.
 - [44] US Department of Health and Human Services, Your Rights Under HIPAA, 1996. <https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html> (accessed February 28, 2018).
 - [45] E. Bower, How does the General Data Protection Regulation (GDPR) affect GPs?, *GP Online.* (2018). <https://www.gponline.com/does-general-data-protection-regulation-gdpr-affect-gps/article/1460998> (accessed April 10, 2018).
 - [46] S. Armstrong, Data deadlines loom large for the NHS., *BMJ.* 360 (2018) k1215. doi:10.1136/BMJ.K1215.
 - [47] US Food and Drug Administration, Content of Premarket Submissions for Management of

- 591
592
593 Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration
594 Staff, 2014.
595 <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf> (accessed March 2, 2018).
596
597
- [48] US Food and Drug Administration, Postmarket Management of Cybersecurity in Medical
598 Devices Guidance for Industry and Food and Drug Administration Staff Additional Copies,
599 2016.
600 <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf> (accessed March 2, 2018).
601
602
- [49] PWC Insurance, Insurance 2020 & beyond, 2015. www.pwc.com/insurance (accessed
603 February 19, 2018).
604
605
- [50] N.C.S. Centre, 10 Steps to Cyber Security, 2016.
606
607
- [51] D. Lyon, Making Trade-Offs for Safe, Effective, and Secure Patient Care, *J. Diabetes Sci. Technol.* 11 (2017) 213–215. doi:10.1177/1932296816676281.
608
609
610
- [52] D.Z. Levin, P. Christmann, Institutionalism, learning, and patterns of decoupling: The case of
611 total quality management., 2006.
612
613
- [53] G. Martin, P. Martin, C. Hankin, A. Darzi, J. Kinross, Cybersecurity and healthcare: how safe
614 are we?, *BMJ.* 358 (2017) j3179. doi:10.1136/BMJ.J3179.
615
616
- [54] S. Mansfield-Devine, Security guarantees: Building credibility for security vendors, *Netw. Secur.* 2016 (2016) 14–18. doi:10.1016/S1353-4858(16)30018-6.
617
618
- [55] Health Care Industry Cybersecurity Task Force, Report on improving cybersecurity in the
619 health care industry., (2017).
620 <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf> (accessed
621 February 28, 2018).
622
623
- [56] D. He, S. Zeadally, N. Kumar, J.-H. Lee, Anonymous Authentication for Wireless Body Area
624 Networks With Provable Security, *IEEE Syst. J.* 11 (2017) 2590–2601.
625 doi:10.1109/JSYST.2016.2544805.
626
627
- [57] C. Deane-McKenna, NHS ransomware cyber-attack was preventable, *Conversat.* (2017).
628 <http://theconversation.com/nhs-ransomware-cyber-attack-was-preventable-77674> (accessed
629 March 2, 2018).
630
631
- [58] H. Landi, Hancock Health Hit with Ransomware Attack, Pays \$55K to Recover Data, *Healthc. Informatics.* (2018). <https://www.healthcare-informatics.com/news-item/cybersecurity/hancock-health-hit-ransomware-attack-pays-55k-recover-data> (accessed
632 March 2, 2018).
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649