The NEW ENGLAND JOURNAL of MEDICINE

Perspective

AUGUST 3, 2017

Cyberattack on Britain's National Health Service — A Wake-up Call for Modern Medicine

Rachel Clarke, M.D., and Taryn Youngstein, M.D.

As you would expect in a pandemic, the headlines were alarmist: we were reportedly locked in a race against time to protect millions of patients from a new virus of unprecedented virulence that had crippled the United Kingdom's National Health Service (NHS) and was spreading rapidly across the country. Except in this case, the virus was not organic but digital.

On May 12, 2017, computer hackers attempted to hold the NHS hostage by exploiting a weakness in Microsoft operating systems. When NHS staff opened an apparently innocuous e-mail attachment, a ransomware worm known as "WannaCry" infiltrated their computers, encrypting data and locking out users. Throughout the United Kingdom, NHS doctors and nurses found themselves helplessly staring at screens that ordered them to pay a Bitcoin ransom to unlock their computers (see image).

Long before the headlines broke, those of us at work in the NHS that Friday sensed that something was amiss. Before official hospital alerts kicked in, we received messages from colleagues asking if we, too, had had our computers frozen. Rumors swiftly circulated: elective surgeries were being canceled, clinics rearranged, managers summoned to private meetings. A sense of unease began to build on the shop floor. As in every unfolding real-time crisis, confusion, bewilderment, and rumor were rife.

Eventually, official news of the cyberattack broke. Whole hospital and primary care networks were suspended, and the NHS went into electronic lockdown.

With lurid headlines lighting up our smartphones it would have been easy for staff and patients to panic. Information technology (IT) has become the linchpin of everything we do, with most NHS hospitals and general practices now using electronic notes, imaging systems, and drug-prescribing systems. We can just about survive without a stethoscope — once the symbol of our craft — but without our computer log-ins, modern medicine grinds to a halt.

In fact, in many places, the chaos was to some degree preemptive. In a slick and effective attempt to protect themselves from harm, even hospitals unaffected by WannaCry were self-imposing electronic quarantine, avoiding infection by shutting down entire networks.

Nevertheless, the cyberattack's impact was undeniably dramatic. In hospitals, frozen out of our electronic systems for ordering tests, viewing the results, tracking patients' locations, and typing in

Screen Shot from Ransomware Attack.

our notes, we were forced to take a radical step. We took old-fashioned pen to paper, and we wrote. It was slow, laborious, and frustrating — but when it's what your patients need, you simply get on with it. Ironically, most NHS hospitals' distance from their goal of being fully "paperless" proved in the crisis to be their greatest asset. Paper drug charts and notes are still tucked away on our wards, coming out whenever our operating systems crash — as they do, too frequently, without any external hackers' intervention. In essence, many frontline staff were therefore already well rehearsed in what to do in the sudden absence of computers. We stayed late into the night and weekend, writing up the paper prescriptions and notes that would keep our patients safe.

Less fortunate were NHS general practices, many of which are now fully electronic. With no backup paper systems for registering patients on arrival, recording consultations, or prescribing medications, they were forced to close their doors, turning their patients away. Certain aspects of hospital functioning were also impossible to sustain. Though the government denied that there were significant problems, as the NHS entered the weekend countless elective operations were canceled, ambulances were diverted away from stricken hospitals, and patients were urged to stay away. "However much they pretend patient safety is unaffected, it's not true," said one junior doctor in London. "At my hospital we are literally unable to do any x-rays, which are an essential component of emergency medicine."[1]

At one of the capital's biggest hospitals, the automated refrigerators used for dispensing blood products were shut down, compromising the capacity to conduct surgery safely. Another major London hospital closed its trauma, stroke, and heart attack centers, forcing patients to travel farther — and wait longer — for emergency treatments. For patients, there was inconvenience, fear, and disappointment. One described to a *Financial Times* reporter the abrupt cancellation of his open-heart surgery: "I'd been waiting for 18 months for this surgery, I was shaved ready for the operation but then the consultant said there had been a hack and there was nothing they could do. He was worried that if I needed a lot of blood for the operation, they wouldn't be able to access the right kind on their systems."[2]

Superficially, the NHS cyberattack appeared to expose the pitfalls specific to underresourced socialized medicine. The British press discovered that the NHS IT system was particularly vulnerable to the WannaCry infection since, despite cybersecurity warnings, former Prime Minister David Cameron had elected to cut costs by scrapping a £5.5 million ($7.07 million) annual deal with Microsoft to provide ongoing security support for the 14-year-old Windows XP system that's still running on several hundred thousand NHS hospital computers.[3] Worse, in March, Microsoft had issued a patch specifically to prevent this kind of malware attack, but many NHS computers were running software that was too old to benefit from it or that hadn't been patched in time.

Certainly, for frontline doctors like us who are used to wrestling with clunky NHS IT systems, the biggest surprise of the malware attack was not that it happened but why it had taken so long. It is an irony lost on no NHS doctor that though we can transplant faces, build bionic limbs, even operate on fetuses still in the womb, a working, functional NHS computer can seem rarer and more precious than gold dust.

But the NHS's cyberattack experience has more nuanced and generalizable implications. First, it exposed the fact that although much has been written about cy-

berattacks potentially breaching confidential patient information, health care providers have not truly considered the physical harm that could befall our patients should an external party with malicious intent take over health service computers.[4] This realization raises urgent questions about the necessity of equipping hospitals with fit-for-purpose IT. Digital security simply hadn't been an NHS priority until WannaCry's infection became the biggest cyberattack on critical infrastructure in U.K. history.

For NHS staff, the attack was stressful, grueling, and exhausting — not least for the legions of NHS IT workers who toiled all night to update and then patch thousands of health service systems. For doctors, it was a wake-up call. Underfunding ultimately left us horribly exposed to a predictable attack that threatened not just privacy but patient safety. If the WannaCry saga appears depressing, however — a realization of the perils of poorly funded health care — that was not the lesson we ultimately took from the experience. Facing adversity, with their backs against the wall, NHS staff quietly and resolutely got on with the job at hand.

But although — through our resilience — our most vulnerable patients were able to pull through the crisis this time, we cannot be complacent and wait for a next time. All health care workers now have a responsibility to educate ourselves about this emerging threat and demand that funds be made available to ensure that the software we use is as up to date as the medicines we prescribe. We wouldn't accept being told to use outdated equipment on our patients, and our now-critical IT should be no different.

Disclosure forms provided by the authors are available at NEJM.org.

From the Oxford University Hospitals NHS Foundation Trust, Oxford (R.C.), and the Imperial College Healthcare NHS Trust, London (T.Y.) — both in the United Kingdom.

This article was published on June 7, 2017, at NEJM.org.

1. Rawlinson K. NHS left reeling by cyber-attack: 'We are literally unable to do any x-rays.' The Guardian. May 12, 2017 (https://www.theguardian.com/society/2017/may/13/nhs-cyber-attack-patients-ransomware).
2. Jones S, Neville S, Chaffin J. Hackers use tools stolen from NSA in worldwide cyber attack. Financial Times. May 12, 2017 (https://www.ft.com/content/e96924f0-3722-11e7-99bd-13beb0903fa3).
3. Bienkov A. Jeremy Hunt was warned last year of "urgent" need to update NHS cyber security. Business Insider UK. May 15, 2017 (http://uk.businessinsider.com/jeremy-hunt-was-warned-of-urgent-need-to-update-nhs-cyber-security-2017-5?r=US&IR=T).
4. Perakslis ED. Cybersecurity in health care. N Engl J Med 2014;371:395-7.

DOI: 10.1056/NEJMp1706754

Gabapentin and Pregabalin for Pain — Is Increased Prescribing a Cause for Concern?

Christopher W. Goodman, M.D., and Allan S. Brett, M.D.

Treatment of chronic noncancer pain during the opioid epidemic has become challenging for clinicians. Patients want their pain to be adequately managed, and clinicians are searching for safe, effective alternatives to opioids. Recent guidelines from the Centers for Disease Control and Prevention (CDC) recommend that clinicians consider several other medication classes before turning to opioids for patients with chronic noncancer pain.[1] For example, acetaminophen and nonsteroidal antiinflammatory drugs (NSAIDs) are mentioned as first-line options for pain related to osteoarthritis and low back pain. However, acetaminophen is often ineffective, and NSAIDs are associated with adverse effects that limit their use, particularly in patients with complex conditions. The CDC guidelines also recommend gabapentinoids (gabapentin or pregabalin) as first-line agents for neuropathic pain. We believe, however, that gabapentinoids are being prescribed excessively — partly in response to the opioid epidemic.

The Food and Drug Administration (FDA) has approved gabapentinoids for the treatment of postherpetic neuralgia (gabapentin and pregabalin), fibromyalgia (pregabalin), and neuropathic pain associated with diabetes or spinal cord injuries (pregabalin). However, while working in inpatient and outpatient settings, we have observed that clinicians in our practice community are increasingly prescribing gabapentin and pregabalin for almost any type of pain. Our experience is supported by national prescribing data.[2] In 2016, gabapentin was the 10th most commonly prescribed medication in the United States: 64