care delivery reviews

Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect

Steven Ades, MD, MSc[1]; Diego Adrianzen Herrera, MD[1]; Tim Lahey, MD[2]; Alissa A. Thomas, MD[1]; Sakshi Jasra, MD[1]; Maura Barry, MD[1]; Julian Sprague, MD[1]; Kim Dittus, MD, PhD[3]; Timothy B. Plante, MD, MHS[2]; Jamie Kelly, MPAS[1]; Peter A. Kaufman, MD[1]; Farrah Khan, MD[1]; Cory J. Hammond, BSc[3]; Kelly Gernander, BSN, RN, OCN[3]; Polly Parsons, MD[2]; and Chris Holmes, MD, PhD[1]

abstract

PURPOSE Cyberattacks targeting health care organizations are becoming more frequent and affect all aspects of care delivery. Cancer care is particularly susceptible to major disruptions because of the potential of immediate and long-term consequences for patients who often rely on timely diagnostic testing and regular administration of systemic therapy in addition to other local treatment modalities to cure or control their diseases. On October 28, 2020, a cyberattack was launched on the University of Vermont Health Network with wide-ranging consequences for oncology, including loss of access to all network intranet servers, e-mail communications, and the electronic medical record (EMR).

METHODS This review details the immediate challenges faced by hematology and oncology during the cyberattack. The impact and response on inpatient, outpatient, and special patient populations are described. Steps that other academic- and community-based oncology practices can take to lessen the brunt of such an assault are suggested.

RESULTS The two areas of immediate impact after the cyberattack were communications and lack of EMR access. The oncology-specific impact included loss of the individualized EMR chemotherapy plan templates and electronic safeguards built into multistep treatment preparation and delivery. With loss of access to schedules, basic patient information, encrypted communications platforms and radiology, and laboratory and pharmacy services, clinical outpatient care delivery was reduced by 40%. The infusion visit volume dropped by 52% in the first week and new patients could not access necessary services for timely diagnostic evaluation, requiring the creation of command centers to oversee ethical and transparent triage and allocation of systemic therapies and address new patient referrals. This included appropriate transfer of patients to alternate sites to minimize delays. Inpatient care including transitions of care was particularly challenging and addressing patient populations whose survival might be affected by delays in care.

CONCLUSION Oncology health care leaders and providers should be aware of the potential impact of a cyberattack on cancer care delivery and preventively develop processes to mitigate the impact.

JCO Oncol Pract 18:23-34. © 2021 by American Society of Clinical Oncology

ASSOCIATED CONTENT

Appendix

Author affiliations and support information (if applicable) appear at the end of this article.

Accepted on July 2, 2021 and published at ascopubs.org/journal/op on August 2, 2021: DOI https://doi.org/10.1200/OP.21.00116

INTRODUCTION

On October 28, 2020, the University of Vermont Health Network (UVMHN) suffered a major ransomware attack with wide-ranging and immediate consequences, including total loss of access to all network intranet servers, e-mail communications, and clinical systems. Within minutes, we lost access to our electronic medical record (EMR), including laboratory, pathology, pharmacy, and radiology systems, significantly affecting both inpatient and outpatient care delivery. The complete shutdown continued until restoration of our EMR on November 22, secure e-mail on November 25, and access to radiology viewing systems on December 7 (see the timeline in Fig 1). This cyberattack has been rated as the worst for health care institutions in the United States for 2020.[1]

Although UVMMC had disaster recovery and business continuity plans in place for all major systems, as well as third-party consultant on retainer to provide guidance in the event of a major cybersecurity incident, it was clear within hours that this was a severe ransomware attack, with the potential to disrupt institutional

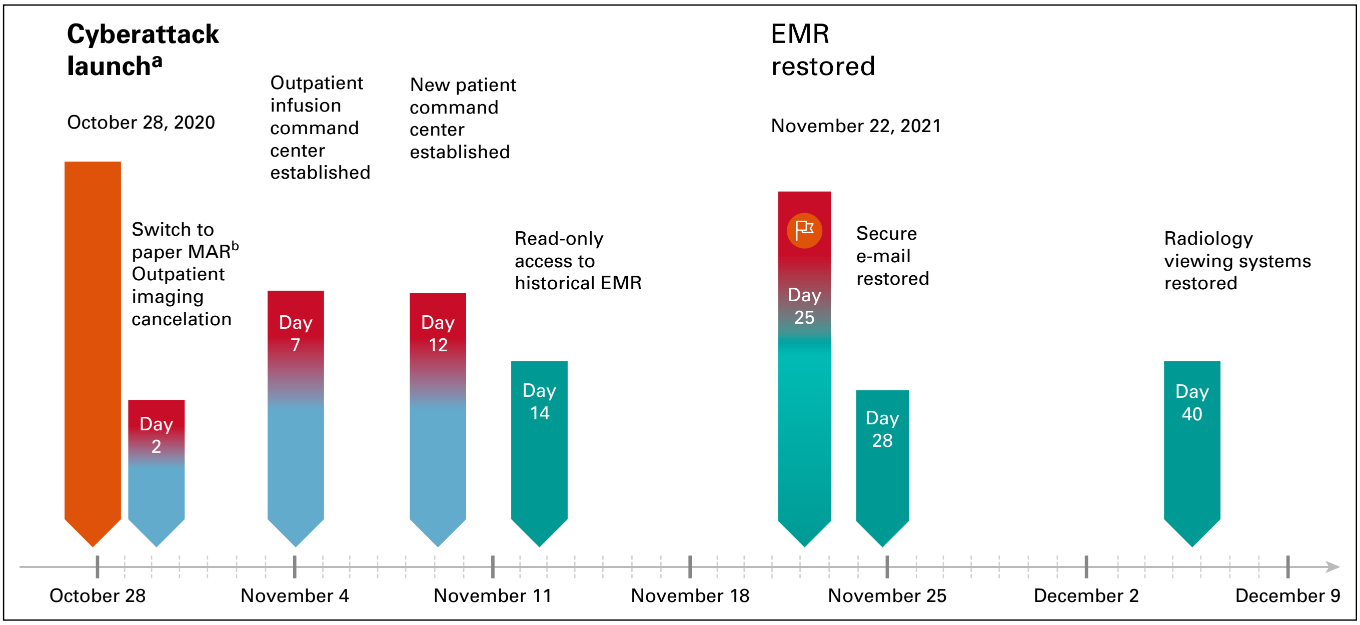

FIG 1. Cyberattack response timeline. [a]Loss of all internet servers, e-mail communication, and access to clinical systems including EMR, pharmacy, laboratory services, pathology, and radiology. [b]This included re-establishing standard protocols for order review, drug preparation, and administration that do not depend on electronic infrastructure support. EMR, electronic medical record.

provision of life-saving care. Both local and federal law enforcement agencies were immediately contacted for support. Per standard practice for any major system issue that affects end users, institutional leadership stood up an information technology (IT) incident command center and a second broader hospital command center to manage the operational impacts and communication. These two command centers worked together to ensure constant flow of information between the IT teams working to restore systems and clinical and operational leaders.

Multiple immediate damage containment measures included taking the EMR offline and cutting off all internet and other access both to and from UVMMC to prevent further incursion from the attackers or spread of malware to other sites. Unfortunately, the malware encrypted the files and data for virtually the entire hospital infrastructure and for most application servers. Although backups were available, it took almost an entire month to wipe all existing servers and end user devices clean, a process that required the assistance of the Vermont National Guard given the enormity of the undertaking.

The impact of the cyberattack in oncology centered around the loss of communication channels and the loss of the individualized EMR chemotherapy plan templates driving nursing and pharmacy processes to enable the safe delivery of systemic therapies to our cancer patient population. Loss of a reliable encrypted e-mail communications platform challenged efforts to organize and coordinate our response as the COVID-19 pandemic, and prevented regular, large, and in-person meetings. Given data documenting the impact of treatment delay on survival in select cancer patient populations[2] and the acute treatment toxicities managed as an outpatient,[3,4] the sustained effects of the cyberattack presented specific challenges related to oncology care.

This review describes the challenges faced in oncology and how we addressed them over the course of the cyberattack. Practical steps to mitigate the impact of cyberattacks are included.

COMMUNICATION FOLLOWING A CYBERATTACK

Disruption of communication was at the heart of the damage induced by the cyberattack and highlighted the multiple nonredundant ways used by physicians and staff to provide high-level multidisciplinary cancer care.[5] Modalities of communication are compromised, and our response and actions that other institutions can now take to mitigate the impact on communication are delineated in Table 1.

To facilitate interprofessional communication, SMS text groups were rapidly created and used to coordinate frequent secured videoconferencing sessions. These video conferences—in which all participants were painstakingly identified to avoid hacker intrusion—were critical to disseminate important up-to-date information and organize resources around patient care. In-person meetings were minimized because of the COVID-19 pandemic but could be used outside of pandemic restrictions. The health network e-mail system was initially disrupted and entirely unavailable for any communication, but then subsequently was both unreliable and unsafe to use because of serious

TABLE 1. Communications Impact During a Cyberattack

Technology System by Modality	Reality in Our Complete Computer Network Failure	Alternatives During Network Failure	Recommended Steps to Mitigate Future Cyberattack Damage Before Complete Network Failure
Internal communications with staff			
E-mail	E-mail server offline for 2 weeks for internal communication	Use of texting via personal cell phone Use of personal e-mails—limited as not HIPAA compliant	Leaders should establish group texts of providers, nurses, and key administration now Establish access to secondary or personal e-mails for all staff and store off-site
Secure text messaging	Centralized paging service could not retrieve lists of pagers and personal cell phones as they were stored on the network. Pagers still worked as they were managed by an offsite company. Lists of personal pagers available to the operators were outdated or incomplete	Ad hoc collection and distribution of cell phone numbers Some groups used alternative secure messaging services (eg, *Doximity*)	Maintain off-site listing of personal phone numbers Process for utilization of backup overhead intercom system for hospital communications Ensure that emergency text distribution service is independent of hospital network
Landline phones	The modern phone network primarily uses the computer network to relay calls, and there was widespread loss of phones across inpatient and outpatient services	Non-network phones were installed in clinics and on floors Extensive use of personal cell phones	Ensure excellent cell phone coverage in hospital and clinics Access to personal (cell or home) numbers of staff Have cell phone chargers available in clinic
External communications with patients			
Centralized call center for incoming patient calls	Unable to relay patient messages quickly from call center to the clinic offices	Operators took messages on paper, and they were couriered to clinics across the network	Establish robust paper-based downtime procedure for centralized call centers including methods and prioritization of message delivery
Calls from clinic to patients	Contact information for patients and families was stored in the EMR	Use of external internet resources (eg, Whitepages[16]) and HIE, which is a secure web portal that hosts patient-level data from several EMRs across a geographical region. These also store contact information for patients (VITL in Vermont)	Maintain off-site or off-line secure updated contact information for patients with basic demographics and communication requirements (eg, translator required) Determine if HIE is available in your region and ensure that all medical and support staff have access and that accessing the HIE does not require your hospital's network to be functioning (ie, login does not require single sign-on using hospital credentials)
External communications with other health care sites			
Faxes	A single fax machine was operational in the entire hematology-oncology clinic. All others were disabled because of cyberattack	All outside communications were funneled through this fax including laboratory results	Establish IT interconnectivity of fax machines and ensure ability to compartmentalize. Have large stockpile of toner and paper in clinic
Internet connectivity			
Wired network	Complete loss of wired network for all devices	None	Develop backup wired network with basic internet connectivity
Wireless network (Wi-Fi)	Complete loss of Wi-Fi networks intended to support wireless devices and staff	The guest Wi-Fi network was unaffected, so it was used to support staff's personal devices. Bandwidth became problematic with the high number of staff who began to use this network Devices that used Wi-Fi networks (eg, point-of-care devices, electrocardiograms, and label printers) would not work without network connectivity	Develop secondary Wi-Fi networks capable of handling staff and visitors Configure point-of-care devices so they can function if the Wi-Fi network is unavailable. Develop secondary systems to obtain data collected from wireless devices (eg, dockable printers for point-of-care devices or written forms)

NOTE. Affected high-priority areas, alternatives, and potential solutions to mitigate future impacts.
Abbreviations: EMR, electronic medical record; HIE, health information exchange.

concern of intrusion and was avoided outright for 28 days. Hospital leadership circulated important information on the cyberattack to administrative and clinical leaders via text who would pass this on to staff. Simultaneously, the urgent need to address oncology-specific impacts was communicated to hospital or administrative leadership to obtain necessary resources to stand up multiple command centers addressing the challenges that we faced.

Communication with patients was impaired following the cyberattack as basic demographic information was no longer available via the EMR and bidirectional systems of patient communication no longer existed. We had access to limited basic information including outpatient schedules for only the forthcoming 3 clinic days following the cyberattack. Alternative sources of information included the use of our regional health information exchange (HIE; in Vermont known as VITL) designed to enable EMR transferability, containing clinical summaries, demographics, and radiology or laboratory results, which were accessed but required individual provider registration.[6] Third-party internet-based services were also used to obtain contact information. Greeters, signage, and paper flyers were used to communicate in the clinic and inpatient settings.

Broad communication to the community was undertaken at an organization level. Communications to the public were limited by an ongoing Federal Bureau of Investigation and concern from leadership that perpetrators could take advantage of any information to undermine hospital IT response to the crisis. Initially undertaken as a broad message, communication regarding oncology-specific challenges and messaging was also required and relied on social media and integration into broader announcements. Timely and transparent communication to oncology patients via a centralized mechanism was delayed in our institution and should be addressed early following a cyberattack.

APPROACH TO PRIORITIZATION AND ALLOCATION OF RESOURCES IN THE WAKE OF A CYBERATTACK

Ethical principles for the fair and transparent allocation of scarce medical resources during times of pandemic or disaster have been published[7,8] and updated during the COVID-19 pandemic.[9,10] Chemotherapy shortages have enforced similar rationing approaches for patients[11,12] with cancer, but there is no published guidance regarding ethical allocation of scarce cancer care created by a cyberattack.

We used an ethical framework aligned to those used during COVID-19 and other disaster contexts, prioritizing rationing of cancer care according to the ethical values. These guiding principles and the specific prioritization strategy implemented are given in Table 2. To enact these principles, oncology leadership enacted a simple, pragmatic, and transparent process in collaboration with ethics leadership summarized in Figure 2. A detailed ethical process for rationing of health care resources during the cyberattack is described in Appendix 1 (online only).

Recognizing that mention of rationing could raise patient concerns and even engender legal liability, clinicians invested significantly in transparent public communication about the cyberattack and the institution's vigorous attempts to maintain the standard of care or, when not feasible, referral to other collaborating institutions.

IMPACT OF A CYBERATTACK ON SPECIFIC PATIENT POPULATIONS

Oncology Outpatients

Following the cyberattack, downtime procedures went into place across the health system. The backup downtime computer system failed in the outpatient infusion unit and oncology pharmacy, adding to the complexity of response. Preprinted schedules were available on the basis of the infusion unit policy of keeping a paper record of planned infusions 2 days in advance, but there was no access to treatment plans or schedules beyond 2 days after cyberattack. Documentation was immediately switched to paper medication administration records. Patients receiving outpatient treatment at the time of the attack completed their infusion on the basis of already prepared and verified chemotherapy. Patients scheduled for a new treatment or a new cycle were registered, but their treatment was held until a mechanism to safely verify that their regimen was deployed.

In total, compared with the preceding 2 months, the cyberattack resulted in an 41% decrease in total outpatient volume including a 39% decrease in new patient visits on the basis of weekly totals averaged over the cyberattack period. Both telemedicine and in-person visits were equally affected. In particular, infusion center visits dropped initially by 63% in the first week before rebounding gradually in response to corrective actions taken. Figures 3 and 4 further delineate the reduction in outpatient services resulting from a cyberattack.

The following protocols were used to determine which patients could be safely treated:

1. Identification of easy-to-verify regimens such as continuous infusions, frequent (mostly weekly) treatments, and fixed-dose regimens.
2. Capability for triple verification of infusion details including verification of treatment plans by pharmacist according to cancer diagnosis and national guidelines.

If these criteria were met, written orders were provided 24 hours in advance by the treating physician for verification by nursing and pharmacy and pharmacy staff provided written labels and compounding formulas. The process was streamlined further with availability of limited EMR read-only access for oncology to obtain previous electronic

TABLE 2. Ethical Rationing of Chemotherapy Access During a Cyberattack

Basic tenets	Maximization of lives saved Utilization of accepted medical prognostic criteria Equitable and fair assessment of all cases Transparency in decision-making process. Impartiality and neutrality of decision-makers
Potential pragmatic approach using a tiered prioritization	Tier 1: Patients with impending organ compromise or uncontrolled or escalating pain Patients undergoing curative-intent therapy Diagnosis with literature supporting the fact that delays in chemotherapy affect overall survival Tier 2: Gray zone including diagnosis with literature supporting the fact that delays in chemotherapy regimens affect progression-free survival or palliation of symptoms Tier 3: Patients receiving maintenance and palliative regimens

treatment plans 14 days after the cyberattack was launched. All other patients were screened by a command center. Laboratory delays required completion of blood work 24-48 hours before chemotherapy and, in some cases, required the use of outside facilities.

Outpatient Infusion Command Center. Computerization of order sets and pharmacy processes has become a cornerstone of our ability to deliver safe and efficient care to large numbers of patients.[13] With loss of electronic safeguards and clear communication from hospital leadership that resolution of the disruption would take weeks, an incident command center including oncology nursing educators, nursing navigators, and scheduling specialists was rapidly established to identify and guide all outpatient infusion treatments (Table 3). The command center accomplished the following:

1. Centralized mechanism to gather data: A paper database was created for all patients receiving treatment during downtime and individual paper charts for each patient in need of therapy including cancer diagnosis, chemotherapy regimen, and personal information from VITL including allergy history and last weight and height.
2. Coordinating body for prioritization: A list of patients with missed or upcoming therapy was provided to each physician for patient stratification. The goal was to classify infusion treatments as tier 1 (curative-intent, urgent or lifesaving, need for highly symptomatic disease, and proven survival advantage), tier 2 (safe to delay 1-2 weeks as palliative, adjuvant, or neoadjuvant), and tier 3 (safe to delay at least 2 weeks such as maintenance regimens and patients with long-term stable disease). The command center created each list and oversaw updating the tier classification for each patient by communicating directly with the treating clinician.
3. Expanding operating hours: With the goal of accommodating more patients, the command center coordinated the expansion of operating hours with

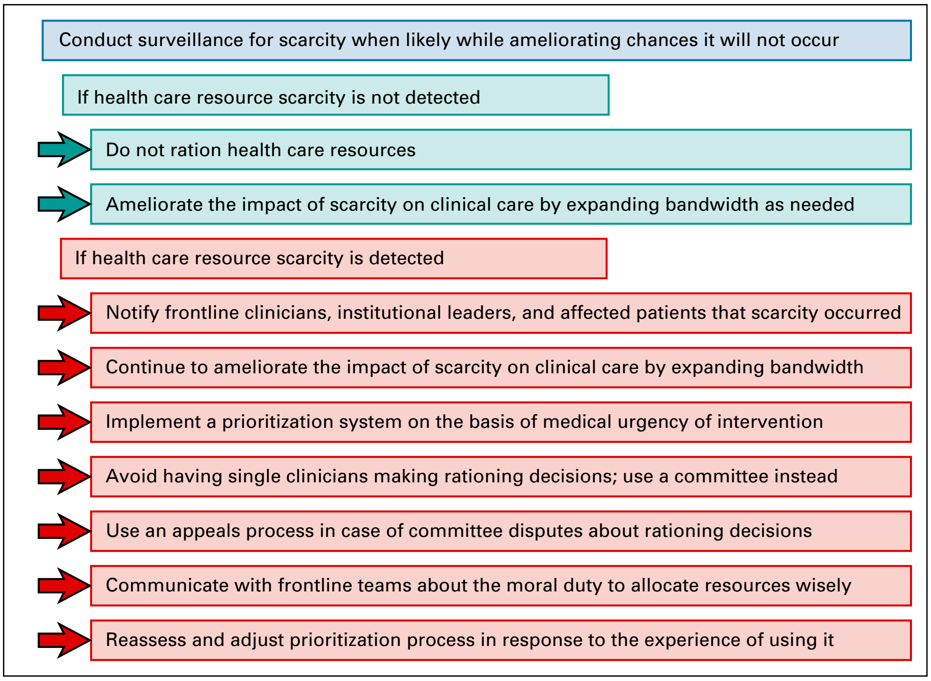
Conduct surveillance for scarcity when likely while ameliorating chances it will not occur
If health care resource scarcity is not detected
Do not ration health care resources
Ameliorate the impact of scarcity on clinical care by expanding bandwidth as needed
If health care resource scarcity is detected
Notify frontline clinicians, institutional leaders, and affected patients that scarcity occurred
Continue to ameliorate the impact of scarcity on clinical care by expanding bandwidth
Implement a prioritization system on the basis of medical urgency of intervention
Avoid having single clinicians making rationing decisions; use a committee instead
Use an appeals process in case of committee disputes about rationing decisions
Communicate with frontline teams about the moral duty to allocate resources wisely
Reassess and adjust prioritization process in response to the experience of using it

FIG 2. Pragmatic process for ethical allocation of cancer care during a cyberattack.

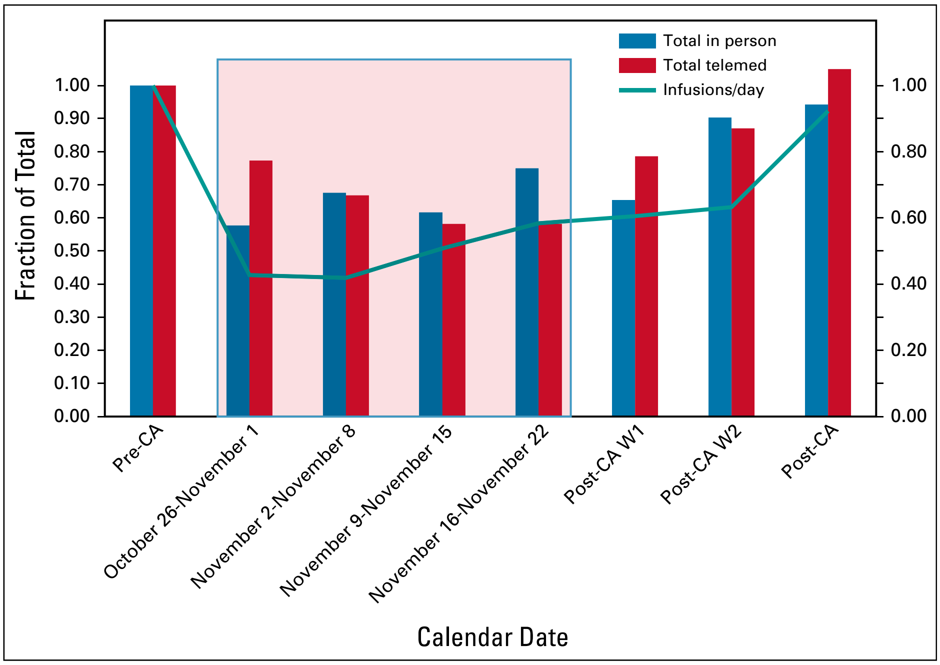

FIG 3. Impact[a] of the cyberattack on in-person and telemedicine visits[b] and daily average infusion visit rate[c] (cyberattack time period shaded). [a]Benchmarked relative to totals averaged over the preceding 2 months (pre-CA). [b]On the basis of weekly totals, primary *y* axis. [c]Averaged over a week, secondary *y* axis. CA, cyberattack; post-CA, postcyberattack; pre-CA, precyberattack.

additional shifts, traveling nurses, and covering physicians to include nighttime and weekends.

4. Managed network referrals: On the basis of stratification and resource capability, some patients were referred to network affiliates sites to complete their chemotherapy. The command center worked directly with the responsible provider to transfer written orders and copies of patients' records and facilitate direct report to the covering oncologist.

In the initial weeks of the crisis, this committee met daily for high-level executive updates and crisis management oversight, whereas a subset executed core operations

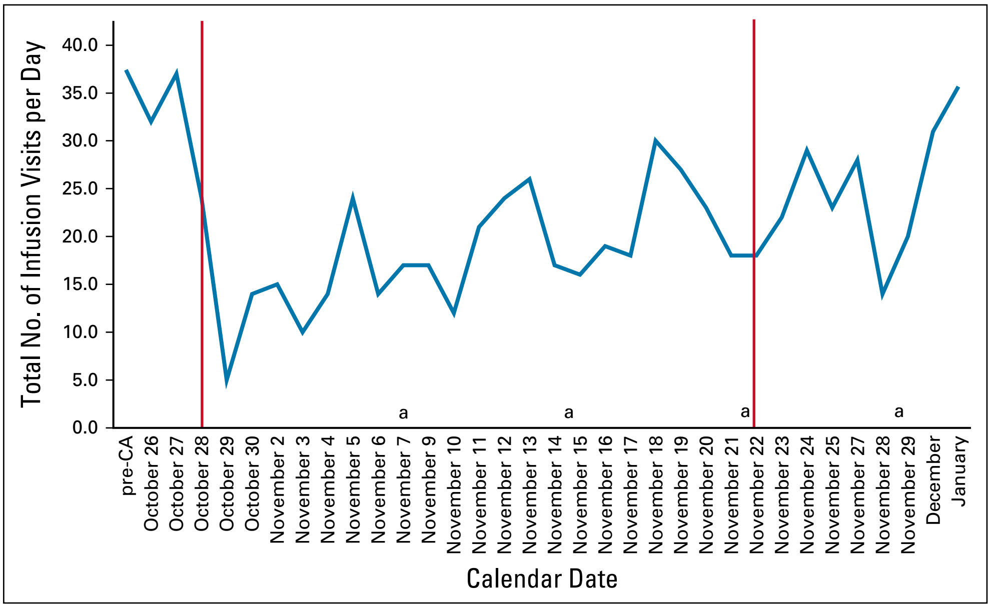

FIG 4. Impact of cyberattack of daily infusion visit totals. Precyberattack, December and January month visit rates averaged over 7-day periods. Precyberattack rate represents weekly averages over preceding 2 months. Vertical lines represent initial and final dates of CA network shutdown. [a]Weekend infusion overflow days. CA, cyberattack; pre-CA, precyberattack.

TABLE 3. Infusion and New Patient Command Center Objectives and Structure

UVMMC Hematology-Oncology Infusion Command Center
Objective: Facilitate infusion treatment for UVMMC Hematology-Oncology patients. Ensure that the process is consistent with ethical guidelines of care
Members:
Command Center Coleader or Sponsor—Vice President, Medical Group, UVMMC
Command Center Coleader or Sponsor—Assistant Director Medical Group, UVMMC
Command Center Coleader or Sponsor—Division Chief Hematology-Oncology
Command Center Project Manager—Senior Quality Improvement Partner
Nurse Educator Medical Group Training
Business Operations Partner, Medical Group Operations
Director Medical Group
Manager Pharmacy Oncology
Nurse Manager Oncology
Hematology-Oncology Nurses
Ethics Consultant
UVMMC New Hematology-Oncology Patient Command Center
Objective: Facilitate timely and appropriate care for all patients diagnosed with cancer referred to UVMMC. Ensure that the process is consistent with ethical guidelines of care
Members:
Command Center Coleader or Sponsor—Cancer Service Line Director, UVMMC
Command Center Coleader or Sponsor—Vice President Practice Development, Medical Group, UVMHN
Command Center Project Manager—Senior Quality Improvement Partner
Clinical Program Coordinator and Nurse Navigator
Division Chief Hematology-Oncology
Division Chief Pathology & Laboratory Medicine
Program Director Surgical Oncology
Vice Chair Radiology
Administrative Director Medical Group Practice Specialty Services UVMHN CVMC
Regional Vice President of Professional Services UVMHN AHMC & CVPH
Legal Risk Manager
Manager Patient and Family Experience
Ethics Consultant

Abbreviations: AHMC, Alice Hyde Medical Center; CVMC, Central Vermont Medical Center; CVPH, Champlain Valley Physicians Hospital; UVMHN, University of Vermont Health Network; UVMMC, University of Vermont Medical Center.

continuously throughout the day and on weekends. As the crisis abated in response to the committee's work, meeting schedule was altered accordingly. This command center also addressed follow-up visits for established patients, especially when linked to an infusion visit.

Hospitalized Patients Receiving Inpatient Systemic Therapy

The UVM Medical Center inpatient teams have standard downtime procedures, using paper orders and charts, for any instance where EMR might not be available. Although physicians and staff are trained for standard downtime procedures, the extent of an outage induced by a cyberattack affects multiple aspects of patient care.

Inpatient admissions. Patients requiring hospital admission for oncology-directed care included three groups: patients receiving a chemotherapy regimen necessitating inpatient care because of delivery requirements or potential toxicity, patients experiencing cancer or treatment-related side effects, and those with symptomatic malignancies requiring expedited workup. Patients with acute leukemias and/or lymphomas requiring immediate treatment were admitted as per usual protocol. For planned chemotherapy admissions, the outpatient triage process was used to determine patient prioritization.

Management of laboratory delays. Despite standard downtime procedures, all aspects of inpatient care were significantly backlogged. In particular, timely receipt of laboratory values quickly became a barrier. As the safe administration and monitoring of several chemotherapy regimens (eg, high-dose methotrexate protocols) depend on laboratory values, this was a critical issue. The laboratory established a system for prioritizing orders from inpatient units, with the goal of providing results within 2 hours for STAT orders. To meet this goal, release of the results was batched. Laboratory results needed to be delivered by runners to each floor since internet services and faxes were offline.

We closely communicated with the leadership in our laboratory to ensure that instead of a generic STAT label, the results were prioritized on the basis of their clinical relevance for treatment of oncology patients. The results for methotrexate levels, unfractionated heparin, critical values needing transfusion, and any positive infectious cultures were prioritized.

Transfer of oncology patients. We re-evaluated our criteria for transfer of patients to the medical intensive care unit and outside hospitals and lowered the threshold to include patients who needed close monitoring of chemotherapy drips or anticoagulation.

Administration of inpatient chemotherapy. Many of the same challenges faced in the outpatient setting were amplified for hospitalized patients including loss of access to all treatment plans in the EMR, any dose modifications made to standardized regimens, and access to contact information for patients and family members and insurance information. Medication reconciliation was a significant problem, and home medications could not be verified as local pharmacies were also affected by the cyberattack. Access to the patient's medical history, consultation documents with subspecialists, imaging studies, and pathology results was lost.

To address this, all chemotherapy orders were rewritten by the primary oncologist. We requested all patients to carry their medications and any available medical records with them. Chemotherapy plans were submitted for review at least 24 hours in advance. Although the information regarding dose modifications was limited, the primary oncologist made clinical decisions on the basis of the available information. To ensure proper timing of delivery and to avoid missed doses or transcription errors, the entire regimen was written in chemotherapy medication administration records, including supportive premedications and emergency contingencies, before administration. We compiled a set of chemotherapy templates for frequently used protocols that could be used for incoming patients. This system was particularly helpful for ensuring that chemotherapy admissions were not delayed.

New Patient Referrals

New patient command center. Another looming crisis with the cyberattack was managing a continuous influx of new patient referrals over the monthlong downtime period. Once it became clear from hospital and IT leadership that resolution of the disruption would take weeks, a separate command center was rapidly stood up to address new patient referrals and ensure that patients could receive timely and appropriate care (Table 3). All new or recent cancer diagnosis referrals were evaluated and screened by transdisciplinary team nurse navigators on the basis of cancer type. Each case was evaluated in conjunction with oncologists. Patients were divided into two groups:

1. Recently established patients: Intake coordinators identified all established patients and created written lists of recently evaluated patients. A treating physician was identified for each case and was responsible for communicating the needs of each individual case on the basis of two priorities: (1) expedited completion of diagnosis and staging and (2) timely initiation of treatment. The outpatient command center was responsible for coordinating diagnostic biopsies, genetic testing, and radiographic scans. It served as a centralized mechanism to communicate with the laboratory medicine, pathology, and radiology departments at both the University of Vermont Medical Center (UVMMC) and network affiliate sites to both plan the needed tests or procedures during downtime and provide a pipeline for accessing the results. Once the best option to complete each step in a patient's evaluation was identified, it was transmitted to the treating physician for verification.
2. New referrals: Intake coordinators identified all newly referred patients during downtime. Because of the limited resources, the general policy was to not accept new patients in our outpatient clinic. However, each individual case was reviewed by disease-specific multidisciplinary teams and classified: (1) urgent referrals in need for immediate attention (eg, acute leukemia) were prioritized for inpatient admission to expedite workup and treatment and (2) nonurgent referrals were further evaluated to determine the complexity level. Cases with completed diagnoses requiring standard of care were referred to community or network sites by the command center. Complex cases were scheduled for new patient visits at UVMMC on the basis of acuity and type of cancer. A pictural overview of the algorithm for new patient referral is provided in Appendix Figure A1 (online only).

Similar to the infusion command center, the full committee met daily in the initial weeks after being stood up to provide high-level direction and oversight, whereas a subset executed core operations continuously until resolution of the crisis. One critical shortfall faced by the new patient command center was the broader crisis affecting digital radiology services that rapidly became overwhelmed, rendering it impossible to work up and biopsy new cancer cases without having to send patients elsewhere even in instances where care could be provided locally.

Special populations

1. Neuro-oncology—cognitively impaired populations

Patients with primary and metastatic brain tumors frequently have neurocognitive symptoms, including short-term memory impairment, expressive and receptive aphasias, and auditory processing difficulty. Many neuro-oncology patients, as well as other patients with cognitive impairment, use adaptive strategies in day-to-day life to manage these symptoms. These strategies may rely heavily on technology, such as reliance on automated messages for appointment reminders, automated prescription refills from the pharmacy, use of EMR MyChart messaging system to send questions to physician and nursing staff in real time, rather than trying to remember questions for the next appointment, and use of MyChart for tracking appointments. This patient population also tends to rely more heavily on caregiver involvement to access appointments. With the loss of all our automated systems through the cyberattack, frequent phone calls and appointments were essential for keeping track of patients, managing essential medications, and monitoring symptoms. With the limitations on neuroimaging, we relied on patient- and caregiver-reported symptoms, changes in neurologic examination, and increases in steroid dosing to determine clinical progression or response and for chemotherapy monitoring.

2. Autologous Stem-Cell Transplant Patients

As an outpatient-based transplant program, the cyberattack required switching stem-cell patients to an inpatient-based treatment paradigm to reduce outpatient visits that were difficult to coordinate. Since the inception of the stem-cell program, a separate paper chart was created for each patient and this is continued until the present. This chart included consent forms for stem-cell collection and high-dose therapy, results of screening tests, stem-cell processing forms, COLST form, and treatment calendars. This system was leveraged further following the cyberattack. FACT documents are also available on paper and in the policy section of the EMR. Nevertheless, delays in transplant initiation increased following the cyberattack.

3. Research study patients

With the surge of COVID-19 cases in the state of VT, restrictions had already been placed on research personnel in the clinical space and the types of studies that were

TABLE 4. Cyberattack Challenges and Solutions Developed to Address Them

Problem	Solution	Preparation for Future Incidents
Loss of secure communication platforms	Texting groups created and used to disseminate information and organize meetings Personal e-mail addresses used for communications that did not involve PHI Use of couriers to relay important messages to clinics and throughout the hospital	Create an emergency cell phone system for all hospital services Backup overhead paging system Maintain a separate cell phone contact list or consider alternate secure message services
Loss of access to patient data	Use of regional HIE (VITL in Vermont) for limited access to basic patient information and health care records Creation of active patient list from memory of treating team providers During visits, requested insurance card, medication list, and any records/reports/data that patients collect that would help support their care. Command Center stood up to collate and curate active patients lists and obtain information from all available sources.	Create an active, updated patient roster with MRN, DOB, and contact and insurance information stored on a separate server if not otherwise available
Lack of electronic process of multilevel checks to ensure safe preparation and delivery of systemic therapy unavailable	Updated and reactivated older protocols addressing how orders will be written, verified, and documented Noncomputer-based pharmacy preparation protocol activated including safety checks Older paper orders before EMR era used to write treatment plans	Nonelectronic protocols should be created or updated and readily available for activation including buy-in from all stakeholders Delineate scope of impact on infusion center capacity a priori so contingency plans for addressing treatment backlog can be addressed Rapid availability of comprehensive paper orders with protocols
Inability to provide systemic therapy to the usual volume of patients with scheduled visits	Creation of an outpatient infusion command center with hospital support to establish an updated secure database of active treatment patients using an ethical triage process for prioritization of resources Engagement of community and academic partners to establish a process for temporary transfer of care for appropriate active treatment patients. Contracting temporary nursing staff and opening infusion center evenings and weekends to accommodate more patients	Establish a protocol for centralized triaging of actively treated patients and communication with patients Establish capabilities of partner hospitals to care for patients with cancer (protocols supported and patient groups supported)
Inpatient and outpatient laboratory processing delays	Protocols established for faxing or running reports to inpatient or outpatient environments Codification with laboratory medicine leadership, a plan for prioritizing hematology and oncology laboratories required for immediate treatment decisions Utilization of external laboratories and established process for ordering and obtaining these at least 1 day before scheduled infusion	Establish an operational plan to address significant laboratory delays in both inpatient and outpatient settings and move to a single outpatient clinic paper filing system to store laboratory reports
Inability to work up and treat patients with a new cancer diagnosis	Creation of a new patient referral command center with hospital support to work with nurse navigators for possible diversion of new patients requiring urgent workup and/or systemic therapy to other sites Develop centralized mechanism for recently established patients to order necessary testing at UVMMC, network affiliate sites, and other regional hospitals during downtime and access to results	Early recognition of unique challenges faced by patients with newly diagnosed cancers and recently established patients undergoing workup including tissue diagnosis and staging for their cancers
Loss of access to outpatient imaging studies	A radiology command center was established with a single phone number to reschedule urgent radiology studies at local and network affiliate hospitals	Awareness of significant challenges faced with loss of access to older films for comparison and inability to access local imaging services where clinical decisions hinge on availability of cross-sectional imaging

(continued on following page)

TABLE 4. Cyberattack Challenges and Solutions Developed to Address Them (continued)

Problem	Solution	Preparation for Future Incidents
Loss of electronic platforms for encounter documentation and billing	Providers used a range of documentation options including paper notes, secure documents, and phone dictation Activation of older paper billing sheets in use before EMR billing capture Processing of billing not directly addressed until after EMR reactivation and plans to capture visit documentation during the downtime	Establish consensus-based plan or options for documentation of clinic and infusion visits during downtime Availability of phone dictation or other noncomputer-based options for documentation Availability of paper billing sheets

Abbreviations: DOB, date of birth; EMR, electronic medical record; HIE, health information exchange; MRN, medical record number; PHI, personal health information; UVMMC, University of Vermont Medical Center.

allowed to remain open to enrollment. With the cyberattack, any new patient accrual was halted and focus was shifted to the safety of participants already enrolled on treatment studies and integrity of the collected data. The Cancer Center Clinical Trials Office operates on a secure College of Medicine server that sits outside of UVMMC and was not affected by the cyberattack. An additional immediate fallout because of lack of clarity around the nature of the cyberattack was the severing of related systems such as the College of Medicine network for security purposes.

Additionally, the Clinical Trials Office kept shadow research charts on all active trial patients, which served as a resource to contact and coordinate care for participants. Given the limitations imposed on our pharmacy staff, we reviewed all active cases and decided who needed prioritization versus deferment of testing and treatment. No study patient had to go off active treatment as a result of the cyberattack. However, deviations were reported because of inability to access radiology imaging that needed to occur within the window of the cyberattack systems shutdown.

Sponsors including industry and National Cancer Institute/Cancer Therapy Evaluation Program were contacted and provided updates regarding the safety of participants and collected data and personal health information.

RADIOLOGY CHALLENGES IN A CYBERATTACK

Among the systems affected by the cyberattack, our radiology services were severely affected. We lost access to radiology reports, which were stored within the EMR, and viewing access through the picture archiving and communications system, both locally and remotely. Radiology was able to rapidly stand up a limited number of workstations to accommodate urgent inpatient and emergency imaging, but all outpatient imaging was suspended for the duration of the cyberattack. For inpatient oncology care, imaging was prioritized for patients with symptoms requiring urgent evaluation, surgical planning, and staging for newly diagnosed patients requiring rapid treatment. Imaging reports were brought to nursing stations daily, and copies were also kept in the radiology workroom.

All outpatient imaging was canceled or postponed for the duration of the cyberattack. A radiology command center was established with a single phone number to reschedule radiology studies at local and network affiliate hospitals.

TABLE 5. Paper Forms to Have Available in Event of Loss of IT Infrastructure

Documentation	Progress note (general) New patient visit note Infusion note or flowsheet
Orders	Chemotherapy order form Laboratory order form Radiology order form Cardiology or vascular order form Prescription paper or pad
Billing	Outpatient billing sheets Inpatient billing Infusion billing
Data	Laboratory or bloodwork flowsheet Vital signs flowsheet
Others	Copies of paperwork that would usually be accessed online. Examples include send-out laboratories and medical paperwork (advanced directives, limitation of life-sustaining treatment forms, medical marijuana applications, etc) Letterhead Copy of commonly used chemotherapy protocols (NCCN guidelines or equivalent) for nursing and pharmacy to verify dosing.

Abbreviations: IT, Information Technology; NCCN, National Comprehensive Cancer Network.

Our division used a prior authorization specialist to obtain new approvals from insurance for these scans to be done at other locations. The lack of access to outpatient radiology services posed significant challenges for patients receiving chemotherapy for whom ongoing treatment decision depends on radiographic response. The inaccessibility of previous imaging meant that true restaging was not possible, because side-by-side comparison with baseline studies could not be done.

PATIENT ENCOUNTER DOCUMENTATION AND BILLING

While not initially a top priority following the cyberattack, there was confusion on best documentation practices in the absence of a functioning EMR. Providers used a variety of methods including phone dictation, typing notes directly into a secure word processor for later insertion into the EMR, and handwritten notes.

Outpatient billing was captured by individual providers using running lists for subsequent submission, while our legacy paper inpatient billing system was reactivated for providers on service. Much time was eventually spent reconciling different documentation and billing practices, which could have been saved had there been agreed-upon standard billing sheets readily available for both inpatient and outpatient encounters. Standard practices that could be adopted across the board for documentation in the absence of a functional EMR are imperative.

DISCUSSION

Cyberattacks are becoming increasingly frequent with more than 60% of firms targeted in 2018 compared with 41% the year before, at a significant cost to businesses.[14] The health care industry, in particular, has been plagued by cybersecurity threats as it shifted entirely to electronic infrastructure over the last decade, and issues can range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service attacks that disrupt facilities' ability to provide patient care.[15]

The UVMHN shut down its IT system after identifying an October 28 cyberattack that infected more than 5,000 network computers. The system outage was monthlong with immediate and wide-ranging consequences including complete EMR shutdown and loss of electronic communications. Oncology was significantly affected as it became rapidly clear that many of our active outpatients could not receive systemic treatments on schedule because of sudden loss of access to key information and electronic processes that ensure safe preparation and delivery of chemotherapy to patients. Additionally, we lost the ability to rapidly diagnose and stage patients with new cancer and communicate among health care providers and with patients and their families.

Table 4 outlines the multiple facets of the cyberattack that challenged our organization, with focus on our local response in oncology and suggestions for preparedness at other institutions. Table 5 provides a listing of paper documents that should be updated and readily available for use to allow for continuous safe provision of care to patients in the event of EMR shutdown.

In conclusion, many lessons were learned in our response to the cyberattack crisis including the immediate need for updated standardized processes to address the host of challenges that we faced with loss of EMR and communication systems and the realization that IT cannot be our only solution in the face of a cyberattack. Backup of physical copies of all forms and systemic therapy templates is essential as well as access to basic patient information and secure platforms for all communication. Coordination with hospital administration early on during the attack was key to mobilize resources to stand up necessary command centers that can respond to the most significant challenges that we faced in the safe delivery of systemic therapies to established patients and respond to the immediate needs of patients with a new cancer diagnosis.

AFFILIATIONS

[1]University of Vermont Cancer Center, Burlington, VT
[2]University of Vermont College of Medicine, Burlington, VT
[3]University of Vermont Medical Center, Burlington, VT

CORRESPONDING AUTHOR

Steven Ades, MD, MSc, University of Vermont Cancer Center, Burlington, VT; e-mail: steven.ades@uvmhealth.org.

AUTHORS' DISCLOSURES OF POTENTIAL CONFLICTS OF INTEREST

Disclosures provided by the authors are available with this article at DOI https://doi.org/10.1200/OP.21.00116.

AUTHOR CONTRIBUTIONS

Conception and design: Steven Ades, Adrianzen Herrera, Tim Lahey, Alissa A. Thomas, Sakshi Jasra, Maura Barry, Kim Dittus, Timothy B. Plante, Peter A. Kaufman, Polly Parsons, Chris Holmes
Administrative support: Cory J. Hammond, Polly Parsons
Collection and assembly of data: Steven Ades, Adrianzen Herrera, Sakshi Jasra, Maura Barry, Julian Sprague, Kim Dittus, Jamie Kelly, Cory J. Hammond, Kelly Gernander, Chris Holmes
Data analysis and interpretation: Steven Ades, Adrianzen Herrera, Tim Lahey, Alissa A. Thomas, Sakshi Jasra, Peter A. Kaufman, Farrah Khan, Cory J. Hammond, Chris Holmes
Manuscript writing: All authors
Final approval of manuscript: All authors
Accountable for all aspects of the work: All authors

ACKNOWLEDGMENT

We would like to acknowledge the efforts of our administrative, nursing, and pharmacy leadership including Kimberly Laroche, Naomi Bolognani, Stephanie Lamora, Emily Hoffman, Lisa LaPete, Ann Adsem, Blair Robinson, Michele Corriveau, and Nicole Courtois who were on the front line of the crisis, organizing and coordinating our response at all levels to ensure that patient care continued to the best of our ability without compromising safety or quality. We would also like to thank Hospital Leadership including Lisa Goodrich, Allen Mead, Claude Deschamps, and Erika Smart for recognizing the looming crisis in oncology early on during the cyberattack and making resources immediately available to support clinic infrastructure and patient care. We are also grateful to the leadership of our CMIO, Dr Douglas Gentile who coordinated the response and was an important resource for the writing of this manuscript. We thank our network administrative and physician partners at Central Vermont Medical Center, Champlain Valley Physicians Hospital, and Champlain Valley Hematology Oncology for their support as we sought to move patient care to other centers to avoid delays.

Last but not least, we owe a debt of gratitude to our amazing nurses, pharmacists, navigators, medical assistants, social workers, and clinic schedulers who came in day after day ready to solve the critical challenges that we faced and support our patients and their families through all the turmoil and stress that ensued in the aftermath of the attack. We could not have done it without them.

REFERENCES

1. Dyrda L: The 5 Most Significant Cyberattacks in Healthcare for 2020. Becker's Health IT, 2020. https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html
2. Hanna TP, King WD, Thibodeau S, et al: Mortality due to cancer treatment delay: Systematic review and meta-analysis. BMJ 371:m4087, 2020
3. Delpeuch A, Leveque D, Gourieux B, et al: Impact of clinical pharmacy services in a hematology/oncology inpatient setting. Anticancer Res 35:457-460, 2015
4. Gatwood J, Gatwood K, Gabre E, et al: Impact of clinical pharmacists in outpatient oncology practices: A review. Am J Health Syst Pharm 74:1549-1557, 2017
5. Fennell ML, Das IP, Clauser S, et al: The organization of multidisciplinary care teams: Modeling internal and external influences on cancer care quality. J Natl Cancer Inst Monogr 2010:72-80, 2010
6. Vermont Information Technology Leaders: Informing Health Care Decisions. https://www.vitl.net/about-vermont-information-technology-leaders
7. Altevogt BM, Stroud C, Hanson SL: Guidance for Establishing Crisis Standards of Care for Use in Disaster Situations: A Letter Report. Washington, DC, Institute of Medicine (US) Committee on Guidance for Establishing Standards of Care for Use in Disaster Situations: National Academies Press (US), 2009. https://www.ncbi.nlm.nih.gov/books/NBK219958/
8. Persad G, Wertheimer A, Emanuel EJ: Principles for allocation of scarce medical interventions. Lancet 373:423-431, 2009
9. Emanuel EJ, Persad G, Upshur R, et al: Fair allocation of scarce medical resources in the time of Covid-19. N Engl J Med 382:2049-2055, 2020
10. Truog RD, Mitchell C, Daley GQ: The toughest triage—Allocating ventilators in a pandemic. N Engl J Med 382:1973-1975, 2020
11. Hantel A: A protocol and ethical framework for the distribution of rationed chemotherapy. J Clin Ethics 25:102-115, 2014
12. Jagsi R, Spence R, Rathmell WK, et al: Ethical considerations for the clinical oncologist in an era of oncology drug shortages. Oncologist 19:186-192, 2014
13. Sklarin NT, Granovsky S, O'Reilly EM, et al: Electronic chemotherapy order entry: A major cancer center's implementation. J Oncol Pract 7:213-218, 2011
14. The Hiscox Cyber Readiness Report 2020. 2020; https://www.hiscox.com/sites/default/files/content/documents/2020-Hiscox-Cyber-Readiness-Report_USA.pdf
15. Cyber Attacks: In the Healthcare Sector: CIS Security. https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/
16. Whitepages Inc: Whitepages.com

AUTHORS' DISCLOSURES OF POTENTIAL CONFLICTS OF INTEREST

Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect

The following represents disclosure information provided by the authors of this manuscript. All relationships are considered compensated unless otherwise noted. Relationships are self-held unless noted. I = Immediate Family Member, Inst = My Institution. Relationships may not relate to the subject matter of this manuscript. For more information about ASCO's conflict of interest policy, please refer to www.asco.org/rwc or ascopubs.org/op/authors/author-center.

Open Payments is a public database containing information reported by companies about payments made to US-licensed physicians (Open Payments).

Steven Ades
Research Funding: Lilly, EMD Serono

Alissa A. Thomas
Research Funding: Novocure, Spectrum Pharmaceuticals, Spectrum Pharmaceuticals

Julian Sprague
Stock and Other Ownership Interests: Gilead Sciences, Johnson and Johnson, Merk and Company, Roche/Genentech, Pfizer

Peter A. Kaufman
Stock and Other Ownership Interests: Amgen
Honoraria: Lilly, Polyphor, Macrogenics, Eisai
Consulting or Advisory Role: Polyphor, Roche/Genentech, Lilly, Eisai, Macrogenics, Pfizer, Merck, AstraZeneca
Speakers' Bureau: Lilly
Research Funding: Eisai, Polyphor, Roche/Genentech, Lilly, Novartis, Macrogenics, Pfizer, Sanofi
Travel, Accommodations, Expenses: Lilly, Polyphor, Macrogenics

No other potential conflicts of interest were reported.

APPENDIX 1. DETAILED APPROACH TO ETHICAL ALLOCATION OF CHEMOTHERAPY DURING A CYBERATTACK

1. Conduct routine surveillance for scarcity including the following:
   a. Identify clinical interventions that are most likely to become infeasible because of the conditions following the cyberattack even despite workarounds such as utilization of paper-based order and records system, reduction in hospital admission, transfers from outside facilities, etc
   b. Use metrics monitored at least daily to determine if scarcity has arisen, ie, inability to deliver usual standard of care because of shortage of resources, eg, clinical infrastructure of care, shortage of medications, or other medical supplies.
2. Reduce the likelihood that scarcity will occur via measures that expand bandwidth such as the following:
   a. Task shifting from nonurgent duties to more urgent duties that could be affected by scarcity
   b. Deferral of nonurgent care to expand capacity to provide the most urgent care
   c. Delivery of temporizing or second choice medical intervention that can safely allow patients who were not prioritized to receive first choice care to await availability of first-line treatments most safely.
3. If scarcity occurs, notify frontline clinicians, institutional leaders, and affected patients:
   a. Signal to *frontline clinicians* that scarcity has occurred and describe the local system for addressing it
   b. Notify *institutional leadership*, ie, the chief medical officer that systems are being activated to address scarcity of medical resources
   c. Oversee tailored notification of *patients* whose health care will be affected by resource scarcity along with general communications to patients who may be aware that rationing is occurring in the face of scarcity.
4. Communicate with teams about the moral duty to allocate resources wisely to minimize likelihood of moral distress, helping clinicians understand that there is no duty to provide infeasible care but only to provide the *best possible* health care.
5. Upon detection of scarcity, implement a prioritization system on the basis of medical prognosis, including the following:
   a. Categorize patients into the following groups according to the short-term likelihood of death or major morbidity without access to the intervention that is in scarce supply.
   b. In the event that medical resource scarcity is severe enough to preclude provision of urgent care to all patients who need it, urgent care may be prioritized to patients with a greater likelihood of surviving in response to the urgent intervention on the basis of underlying prognosis, ie, who have urgent need for intervention but a better underlying long-term prognosis such as performance status, CURB-65 score (confusion, urea, respiratory rate, blood pressure), or other validated measures of illness severity.
   c. Regardless of prioritization, all patients will be treated with dignity and compassion.
   d. Prioritization schemes should not factor in potentially biased nonmedical metrics such as sex, race, and other demographics; disability; and wealth or profession, as detailed in Appendix Figure A1. This should help avoid exacerbation of pre-existing health disparities. If the health care intervention being rationed is delivered widely enough amid availability of real-time data on previous experience of health disparities, it is ethical to implement a rationing scheme that strives to redress health disparities in response to those data.
   e. Avoid having single clinicians making rationing decisions, favoring instead committee-based decisions using accepted criteria.
   f. Use an appeals process, ie, engaging ethics and/or hospital leadership in the event that disputes arise about proposed prioritization approach.
   g. Periodically reassess the results of prioritization of resources to determine if real-time adjustments need to be made in the prioritization process.

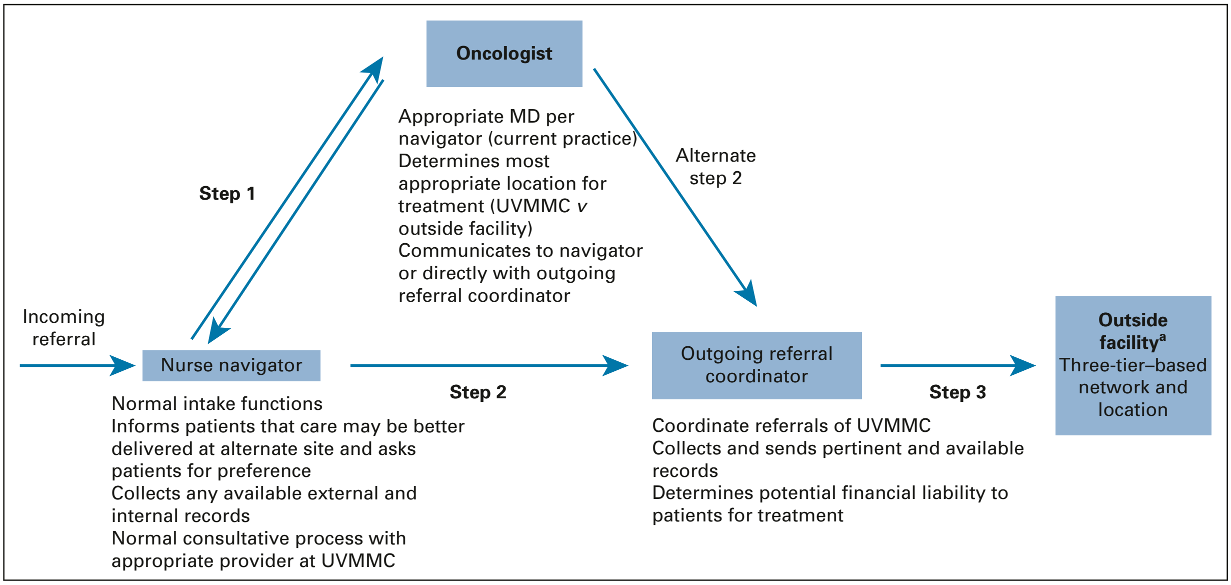
Oncologist
Appropriate MD per navigator (current practice)
Determines most appropriate location for treatment (UVMMC *v* outside facility)
Communicates to navigator or directly with outgoing referral coordinator
Step 1
Alternate step 2
Incoming referral
Nurse navigator
Normal intake functions
Informs patients that care may be better delivered at alternate site and asks patients for preference
Collects any available external and internal records
Normal consultative process with appropriate provider at UVMMC
Step 2
Outgoing referral coordinator
Coordinate referrals of UVMMC
Collects and sends pertinent and available records
Determines potential financial liability to patients for treatment
Step 3
Outside facility[a]
Three-tier–based network and location

FIG A1. Algorithm for new patient consultations and referrals to other sites where appropriate to ensure timely treatment. [a]Scripted communication of plan to new patients via phone or letter. MD, medical doctor; UVMMC, University of Vermont Medical Center.