

ROSWELL PARK CANCER INSTITUTE CORPORATION
IT Oversight Committee Meeting

A meeting of the Information Technology (“IT”) Oversight Committee of the Board of Directors of Roswell Park Cancer Institute Corporation was held on Wednesday, March 9, 2022 at 9:30 a.m. in the Patrick Lee Conference Room, 9th Floor, Scott Bieler Clinical Science Center.

- Present:** Meghan Corcoran (*via Teams*)
Gregory Daniel, MD (*via Teams*)
Chuck Fried (*via Teams*)
Candace Johnson, PhD, President & Chief Executive Officer
Jason LeRoy (*via Teams*)
Kenneth Manning, Esq. - Chair
Gail Mitchell, Esq. (*via Teams*)
Elyse NeMoyer (*via Teams*)
Genevieve Schimpfle (*via Teams*)
Shaun Stoltz (*via Teams*)
Hannah Taylor (*via Teams*)
- Staff:** Lauren Bruckner, MD, PhD, Chief Medical Information Officer (*via Teams*)
Eugene Cullen, Vice President, Internal Audit
Christopher Darlak, Deputy Chief Information Officer
Laurel DiBrog, Chief Marketing & Communication Officer (*via Teams*)
Betsy Doty-Lampson, Administrator for the Board of Directors
Thomas Furlani, PhD, Chief Information Officer
Ryan Grady, Chief Financial Officer
Boris Kuvshinoff, MD, Chief Medical Officer (*via Teams*)
Patrick Lee, Director, Enterprise Applications
Kathleen Mastrobattista, Compliance Officer (*via Teams*)
Leigh Palladino, Esq., Associate General Counsel
Adam Rosen, Chief Information Security Officer
Michael B. Sexton, Esq., Senior Vice President & Chief Legal Officer -
Secretary
Paul Visco, Vice President & Chief Technology Officer

Opening Remarks

Mr. Manning brought the meeting to order and welcomed all attendees to the Committee’s first meeting of the new calendar year. Mr. Sexton requested, and Mr. Manning agreed, to reserve five (5) minutes at the end of the meeting to discuss Roswell Park’s cybersecurity insurance options for the upcoming fiscal year. Mr. Manning then turned the meeting over to Mr. Furlani for an IT update.

IT Update

Mr. Furlani's IT update included summarized highlights of key IT and cybersecurity initiatives completed in calendar year 2021 and the IT Department's priorities established thus far for calendar year 2022. In addition to the Workday go-live, hospital-wide deployment of Imprivata's badge in/badge out technology, implementation of a new financial dashboard for clinical trials management, and the extension of the "bring your own device" program to mobile phones, Mr. Furlani detailed the following IT and cybersecurity accomplishments of 2021:

1.

2. ***Formal selection of a replacement revenue cycle management vendor.*** AthenaIDX was selected as Roswell Park's new revenue cycle management software and contract negotiations with Athena and Deloitte (implementation partner) relative to the planning and design phase of the implementation recently wrapped. Mr. Furlani and Mr. Grady presented a graphic of the current project implementation timeline, which extends through January 2025 and included overlaid related and required IT upgrades and installations and Roswell Park's accounts receivable run down on Cerner Invision. Related to the revenue cycle project implementation, Mr. Stoltz asked Mr. Furlani and Mr. Grady what risks Roswell Park was tracking.

To this point, Mr. Manning commended all teams involved and acknowledged that a lot of education happened on how to handle large, high-risk projects. Mr. Manning expressed satisfaction in how the revenue cycle project has been handled carefully and incrementally and with Mr. Cullen's involvement early on.

3. ***Improvements to the MyRoswell patient portal and mobile application.*** Mr. Furlani presented images showing functionality improvements made to the MyRoswell patient portal and corresponding mobile application, which now has almost equal functionality with the website, including the ability to receive push notifications when new

information is available for review and to exchange secure correspondence with Roswell Park providers.

4. **Improved cybersecurity.** The applications in Roswell Park's datacenters were recently micro-segmented to limit the ability of a breach to spread.
5. **Improved clinical workflows.** Mr. Furlani presented a pilot program championed by Dr. Michael Bax (Dermatology) and Dr. Carl Morrison (Pathology), which laid the foundation to make all pathology consult requests electronic regardless of originating department. Migrating pathology consult requests from a manual, paper workflow to an electronic workflow through Cerner reduces the opportunity for transcription errors, permits providers to spend more time with patients, and yields faster pathology results.
6. **Dr. Lauren Bruckner hired as Chief Medical Information Officer ("CMIO").** Mr. Furlani told the Committee that he could not understate the importance of Roswell Park hiring Dr. Brucker as its CMIO last year, and one of the reasons was because of her recent success in establishing the Provider Informatics Leadership Team ("PILT"), which serves as a central voice for Roswell Park's physicians and prioritizes physician IT initiatives. The PILT is comprised of "provider leads" from each major department (e.g., Internal Medicine, Pediatrics, Dermatology) and its primary goal is to optimize value from Roswell Park's IT investments.
7. **IT spend benchmarked.** An IT spend analysis relative to Roswell Park's total budget was presented at the Committee's last meeting. Roswell Park hired the Gartner consulting firm to assist with the analysis and compared Roswell Park's IT spend to that of a comparison group comprised of fifty-six (56) healthcare organizations with a total revenue of \$1 billion to \$10 billion (inclusive of five (5) cancer centers or academic healthcare organizations similarly situated with Roswell Park). Among the comparison group, the 50th percentile IT spend relative to total revenue was 4.3% (25th percentile being 3.5% and 75th percentile being 5.3%). Including major life cycle projects (Workday and revenue cycle), Roswell Park's total IT spend as a percentage of total revenue for fiscal year 2023 is 6.6%, however, when eliminating these outlier projects, the spend drops to 4.8%, which is close to the comparison group's 50th percentile. As requested by the Committee at its last meeting, Roswell Park leadership continues to prioritize monitoring IT spend in calendar year 2022.

Currently, for calendar year 2022, the IT Department's priorities are: (i) application rationalization, which requires IT leadership to review all applications utilized by Roswell Park to assess overlap and necessity, as duplicative applications waste resources; (ii) preparing for the imminent implementation of AthenaIDX; (iii) replacing OpenLink, the twenty (20)-year old integration engine software utilized by Roswell Park that permits applications from different vendors to communicate with each other (OpenLink is being replaced with InterSystems' HealthConnect and the replacement is required to implement AthenaIDX); (iv) patient access redesign; and (v) migrating Cerner Lab from an on-premise to hosted solution, which is expected to take ten (10) to twelve (12) months to complete.

Mr. Furlani closed his IT update by notifying the Committee that Allscripts has entered into an agreement with N. Harris Computer Corporation ("Harris") to sell the assets of its "hospitals and

large physician practice” business segment, which includes the EHR software utilized by Roswell Park. The transaction is expected to close in the second quarter of 2022.

Minutes

Before turning the meeting over to Mr. Rosen for an information security update, Mr. Manning asked for approval of the draft minutes of the Committee meeting held on November 23, 2021. At that time, a *motion for approval was made by Ms. NeMoyer, seconded by Mr. Fried and Ms. Mitchell, and unanimously carried.*

Information Security Update

Mr. Rosen opened his information security update by acknowledging the current conflict between Russia and Ukraine and the heightened threat of cyberattacks from Russia resulting therefrom. Numerous media outlets, Homeland Security, and the NYS Intelligence Center have reported on the increased likelihood of cyberattacks from Russia on regions and entities supporting Ukraine. In response, Roswell Park continues to monitor intelligence feeds and take appropriate preventive action, including blocking actively malicious IP addresses as recommended by various security agencies.

Mr. Rosen then informed the Committee that a large tabletop exercise simulating a ransomware attack was held last week for various clinical departments and Roswell Park leadership. Mr. Rosen and Mr. Furlani both noted that the exercise was very successful and an opportunity to demonstrate Roswell Park’s preparedness for a cybersecurity attack. The only question raised pertaining to the exercise was from Mr. Manning, who asked for a reminder of what Roswell Park’s phishing training consisted of. In response, Mr. Rosen explained that general phishing education is provided on a quarterly basis, however discussions are ongoing about changing the cadence to monthly. Additional discussions regarding dividing Roswell Park’s annual cybersecurity training into monthly micro training modules to increase the likelihood of retention are ongoing.

Mr. Rosen continued his information security update with a presentation of the following recently completed initiatives:

2. *Compensation review performed.* The cybersecurity job market is extremely tight at present, with over 500,000 job openings (most being remote). To stay competitive in the market and retain talent, a compensation review of Mr. Rosen’s team was completed, and compensation was raised to competitive standards.

3. *New Cybersecurity Analyst hired.* This new analyst will be the key member of Mr. Rosen's team to interface with the security operations center (primary point of contact for incident response) and will work to improve SOC detection and Roswell Park's incident response playbooks and processes.
4. *Onboarded Governance, Risk, and Compliance tool.* As explained by Mr. Rosen, this tool will improve the measurement of Roswell Park's information security program and third-party risk assessments and identify and prioritize risk and direct efforts and resources.

Mr. Rosen concluded his information security update by discussing ransomware trends, as requested by the Committee at its last meeting, and a new _____ system that Roswell Park is imminently employing (as a matter of best practice and also as recent requirement to be issued cybersecurity insurance).

Mr. Rosen presented the FBI Internet Crime Center's trend data from the last five (5) years to the Committee, showing that among publicly disclosed attacks, the trend has shifted from high volume/low loss to low volume/significant high loss, with the cost of payouts increasing exponentially from 2016 to 2020. Explained by Mr. Rosen and Mr. Sexton, a cause of the high payouts is the recent trend of hackers compromising (or threatening to compromise) the data, publicly releasing the data, and/or contacting patients with the threat of releasing the data absent a ransomware payment being made. Just a few years ago, the main threat was the risk of data encryption.

Cybersecurity Preparation

Mr. Rosen turned the meeting back to Mr. Furlani for a review of ongoing cybersecurity preparations undertaken by the IT and information security teams.

Preparations for Kronos-Like Event in Workday

To prevent extensive harm to Roswell Park's operations should Workday experience a Kronos-like cyber event, Mr. Furlani explained that Roswell Park continues

Independent of Roswell Park, Workday tests its disaster recovery plans twice per year. Workday also maintains a service level agreement with Roswell Park to restore downtime within twelve (12) hours, promising a maximum data loss of one (1) hour. So far, Workday has been able to restore all downtimes in less than five (5) hours with no data loss in its disaster recovery tests.

There being no further questions, Mr. Furlani turned to Mr. Visco for a presentation regarding Roswell Park's remediation of the LOG4J vulnerability identified in December 2021.


IT Cybersecurity Planning and Preparation

Mr. Furlani concluded the cybersecurity preparations portion of the agenda by detailing the various planning exercises that the information security and IT teams continue to perform to ensure optimal response in the event of a cyber event. With hospital operations being the main priority, Mr.

Furlani, Mr. Visco, and Mr. Rosen lead education and preparation efforts to proactively reduce vulnerabilities and improve recovery speed.

With no further business to conduct, *a motion to adjourn the meeting was made by Ms. NeMoyer, seconded by Ms. Taylor, and unanimously carried.*

Respectfully submitted,


Michael B. Sexton, Esq., Secretary