UCIRVINE | INTERNAL AUDIT SERVICES

Telehealth
Internal Audit Report No. I2022-207

June 24, 2022

Prepared By
Michael Shead, Senior Auditor
Larry Wasan, Principal IT Auditor
Reviewed By
Niran Joshi, Associate Director
Approved By
Mike Bathke, Director

UCI | Internal Audit Services

June 24, 2022

JOHN GROSS MD, FACS
VICE DEAN, FACULTY AND CLINICAL AFFAIRS
SCHOOL OF MEDICINE

RE: Telehealth Audit
　　　Report No. I2022-207

Internal Audit Services has completed the audit of Telehealth and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Sincerely,

Mike Bathke

Mike Bathke
Director

Attachment

C: Audit Committee
    J. Scott Joslyn, Chief Information Officer-Information Services Administration for UCI
        Health
    Doug Niedzwiecki, Executive Director Ambulatory – Ambulatory Care Administration for
        UCI Health
    Tatyana Popkova, Chief Strategy Officer – UCI Health
    Scott Rudkin, Chief Medical Information Officer – UCI Health

I.   MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2021-2022 audit plan, Internal Audit Services (IAS) performed an audit of the UC Irvine Telehealth (Telehealth) program. Specifically, IAS reviewed certain aspects and related internal controls of Telehealth. The aspects included regulatory compliance, governance, application and infrastructure security, privacy, and quality of care. Based on audit work performed, the following concerns were noted:

Telehealth Program Governance – In FY 2019, Telehealth was planned and became a work in progress. The UC Irvine School of Medicine (SOM) Dean provided seed funding to a founding group charged with establishing a telehealth program at UCI. A steering committee was created to implement Telehealth in a manner that emulated the telehealth business model at the University of California, San Francisco (UCSF). However, with the advent of the coronavirus disease (COVID-19) and subsequent pandemic, Telehealth developed rapidly and the planned steering committee never had a chance to meet. Ultimately, governance of Telehealth became the responsibility of Ambulatory Care Administration and Telehealth operations diverged somewhat from the UCSF business model. Further details are provided in Section V.1.

Telehealth Resource Center of Excellence (TRCoE) – In 2014, the first UC TRCoE was developed by UCSF in support of its telehealth program. Subsequently, other UC medical campuses discovered that a strong TRCoE is a necessary component for a successful telehealth program. UC Irvine Health should have a dedicated TRCoE to advance its own telehealth program. Further discussion is provided in Section V.2.

Use of Personal Devices by UCI Health Providers - Based on communication with UCI Health management, several UCI telehealth providers are using their personal devices to conduct telehealth services. Typically, desktops, laptops, tablets, and smartphones used at home are personal devices not managed by UCI Health Information Technology (IT). This issue is discussed in Section V.3.

Teladoc Health Security Controls - According to UCI Health management, an independent third-party security assessment report was not obtained as required. This issue is discussed in Section V.4.

II.   BACKGROUND

Telehealth

Telehealth encompasses a broad variety of tactics and technologies to deliver virtual medical, health, educational, and other services. To UCI Health in particular, Telehealth provides additional clinical "space" in which healthcare providers can schedule many more patient encounters at reduced capital investment costs while considerably increasing patient access to UCI Health.

In 2019, the SOM Dean provided seed funding to a founding group charged with establishing a telehealth program at UCI in step with many other California healthcare institutions at that time. Originally, the planned implementation timeline for Telehealth was nine months. However, in March 2020, the COVID-19 public health emergency emerged and the demand for virtual care increased exponentially. The planned implementation timeline for Telehealth was reduced from nine months to just three weeks. The founding group worked diligently to meet deadlines while rapidly expanding the Telehealth footprint.

The original plan for implementing Telehealth was based on a proven plan already in place at UCSF. UCSF Telehealth is placed in the Clinical Informatics department with complete autonomy, a dedicated management team, and a steadfast TRCoE. However, with the relatively rapid implementation of UCI Telehealth, governance became Ambulatory Care Administration's responsibility and consequently, diverged from the UCSF business model.

Telehealth Information Technology

There are two main applications used to provide telehealth services to UCI Health patients: 1) Teladoc and 2) Epic MyChart.

Teladoc is software as a service (SaaS), branded as OnCall, for UCI Health. It is supplied and managed by Teladoc Health, which has a contract with UCI Health to provide telehealth services. The contract includes the Teladoc application, as well as Teladoc healthcare providers (i.e., non-UCI Health doctors), who provide telehealth services to UCI Health patients. Because patient encounters are documented within Teladoc, personally identifiable information (PII) and protected health information (PHI) reside within the Teladoc application and servers.

MyChart is part of Epic, an electronic medical record system used by UCI Health, as well as many hospitals throughout the U.S. and worldwide. UCI Health uses MyChart to enable patients to view their health information online via a desktop computer or mobile device using the MyChart mobile app. Patients may use MyChart to view their medical records, communicate with their doctors, schedule appointments, track medications, and utilize its many other features. However, for telehealth services specifically, MyChart is used as an interface to Zoom, which is used by UCI Health providers to conduct video visits with their patients. According to documentation obtained and reviewed by IAS, the UCI Health Zoom account used for video visits is HIPAA compliant, which means that it meets the security standards required by the Health Information Portability and Accountability Act (HIPAA).

III.   PURPOSE, SCOPE, AND OBJECTIVES

The purpose of the audit was to assess processes and related internal controls for Telehealth, including regulatory compliance, governance, application and infrastructure security, privacy, and quality of care.

The audit scope included Telehealth services offered from March 2020 to June 30, 2021, that fall under federal, state, and other regulations; UC/UCI policies and procedures (P&P); UC Irvine Medical Center (UCIMC)/SOM intra/inter-departmental P&P; and/or best practices for telehealth services.

The audit included the following objectives.

1. Determine telehealth risks in the following areas: regulatory guidance, governance, application security (security of the telehealth platform), and infrastructure security.

   a. <u>Regulatory Guidance and Governance</u> – Determine whether adequate oversight of telehealth program(s) is in place (i.e., compliance with Medicare waivers, other regulatory requirements, UC/UCI P&P, and best practices). Determine whether telehealth governance is sufficiently integrated with the original, pre-COVID-19 plan and with existing UC/UCI security and cybersecurity programs.

   b. <u>Application Security</u> – Determine whether telehealth platforms are properly configured and approved technologies are used in providing telehealth services.

   c. <u>Infrastructure Security</u> – Determine the nature of risks to the technological infrastructure supporting the telehealth platform.

2. Determine whether telehealth programs and supporting technology adhere to current privacy requirements, to HIPAA, and whether they are designed to protect patient information and University assets.

3. Determine whether healthcare quality is monitored within the telehealth program.

IV.   CONCLUSION

Based on the results of the audit procedures performed, the current governance structure over Telehealth has not implemented the best practices demonstrated by the successful UCSF Telehealth program.

The potential for a conflict between programs increases when one department manages both "bricks and mortar" and Telehealth programs for healthcare delivery. UCI Health leadership should consider restructuring Telehealth's governance and reporting structure so that it is complementary with, rather than competing against, traditional healthcare delivery.

In addition, Telehealth needs a robust TRCoE so that the program can continue to advance and offer comparable services relative to services offered by several

competing telehealth programs in surrounding communities. Finally, immediate attention should be given to correcting IT audit concerns noted in this audit report.

Observations were discussed with management, who formulated action plans to address the issues. These details are presented below.

V.   OBSERVATIONS AND MANAGEMENT ACTION PLANS

Telehealth

1. Telehealth Program Governance

Background

The original plan developed by the UCI Telehealth Founding Group (TFG) was to launch Telehealth by replicating the successful design of the UCSF Telehealth plan. However, with the advent of COVID-19, key decisions concerning Telehealth leadership and reporting structure were made quickly during a rapid expansion in Telehealth services.

The original TFG implementation plan called for Telehealth to have an independent management team and reporting structure. However, the original plan and the steering committee supporting it never materialized. Telehealth was placed within Ambulatory Care Administration, and Ambulatory Care management assumed leadership of Telehealth.

Observation

As part of the Telehealth audit, IAS reviewed Telehealth governance and the reporting structure. Several concerns became evident, as follows.

a. When Telehealth was folded into Ambulatory Care, additional employees were not hired to operate Telehealth. Similarly, there were not any employees assigned with specific overall responsibility for Telehealth.

b. In current Telehealth operations, execution of administrative processes has been decentralized to the Ambulatory Care medical assistants. However, these medical assistants already have full-time jobs in supporting their service lines. Telehealth administrative duties were simply added on to their existing duties, thus reducing the amount of time medical assistants can spend on their clinical duties.

c. Discussions with management groups and review of documentation indicated that some UCIMC/SOM employees are concerned that Telehealth competes against traditional healthcare delivery for available patient encounters. Other employees are concerned that facility fee reimbursements are much less for

4

Telehealth encounters than for traditional encounters, resulting in a loss of facility fee revenue.

Without a TRCoE to handle functions currently performed by medical assistants, economies of scale and synergy between TRCoE team members cannot be realized, and the need for centralized, subject matter expertise will not develop. This scenario impedes optimum growth of Telehealth operations.

Conversely, development of the TRCoE would alleviate the heavy administrative burden currently carried by medical assistants, thus allowing their clinical duties to become better aligned with virtual patient encounters.

Recommendation

UCI Health leadership may want to complete an in-depth financial analysis that provides evidence as to whether the loss of facilities fee revenue resulting from an increase of Telehealth visits will harm the long-term financial viability of the Telehealth program.

Management Action Plan

A governance body has been created to provide Ambulatory/Telehealth oversight and will report up through Clinical Enterprise Leadership Committee (CELC) Ambulatory, a subcommittee which reports into the CELC Committee. The oversight committee will meet bi-monthly to review telehealth operations including volume, financials, billing updates, compliance, and patient experience. The members of the Telehealth Committee are being finalized to include leadership from Compliance, Medical Informatics, Clinical Affairs, Ambulatory Care, Scheduling, and Telehealth Workflows.

An FY 2022 Strategic Operating Plan (SOP) for Virtual Care was developed to optimize the Telehealth program, as it exists today, including the structure for oversight. There is a process to meet with the UCI Health senior leadership, which was kicked off in April 2022, to evaluate performance in this area, including monitoring of key performance indicators.

Due date: 12/31/2022

2. **Telehealth Resource Center of Excellence (TRCoE)**

Background

The UCSF TRCoE provides support to departments and clinics interested in providing telehealth care. Specifically, the TRCoE monitors the effectiveness of telehealth by reviewing patient satisfaction; compliance with federal, state, and other institutional requirements, as well as reviewing causal factors for failed telehealth video visits.

Additionally, the TRCoE provides guidance to clinics in scheduling visits and coding telehealth encounters so they can be billed appropriately. The TRCoE also provides other services, including, but not limited to, directions on how to use the telehealth platform and applications, best practices for telehealth workflow, and how to obtain interpreters for non-English speaking patients when needed.

Observation

As part of the Telehealth audit, IAS reviewed the need for a TRCoE at UCI. The review disclosed that UCI Health needs to implement many changes in the current telehealth program to effectively compete with healthcare competitors who have long since expanded their ability to provide effective telehealth services.

Specifically, UCI Health is at a critical juncture with the future of telehealth and the value that an effective telehealth program can bring to UCI Health. Additional management attention and investment is needed so that Telehealth can successfully transition to a higher level of maturity and to a program-focused strategy that enables a market-driven and care-delivery focused program. By making this transition, Telehealth will improve its competitive position, fulfill existing and future patient demand for remote care, and attract new patients by being able to match and/or exceed consumer expectations.

However, two key elements are missing to make this transition a reality:

a. **A single, dedicated TRCoE positioned at the enterprise level in the UCI Health organizational structure.** Ideally, the TRCoE would operate under a holistic, multi-year strategic plan that would be adequately resourced to meet consumer and provider expectations for remote care. This center would also have direct accountability for the product and services portfolio and accompanying budget. As a result, UCI Health would have a telehealth program better positioned for success in delivering efficient and effective telehealth experiences, including strong integration with the needs of the College of Health Sciences and the Center for Clinical Research.

b. **A small group of highly trained and experienced employees/subject matter experts (SMEs) with full-time dedication to telehealth endeavors.** A key objective of these individuals would be to partner with, and innovate on behalf of, all stakeholders including the digitally underserved. They would also be committed to adhering to the UCI Health "brand" and UC/UCI ethics, compliance, and internal control requirements.

Management Action Plan

A Virtual Care SOP for FY 2023 has been developed that identifies the need for a virtual visit innovation hub that may become a TRCoE with the appropriate focus and funding.

The Ambulatory Virtual Care Visit Oversight Committee will request an organizational commitment to a TRCoE from UCI Health Leadership and the necessary dedication of resources will be evaluated through FY 2023 for implementation in FY 2024.

Due date: 12/31/22 – request for organizational commitment
         6/30/23 – evaluation of resources
         12/31/23 – implementation of TRCoE

Telehealth Information Technology

3. Use of Personal Devices by UCI Health Providers

Observation

Based on communication with UCI Health management, there appears to be a large number of telehealth providers who are using their personal devices to conduct telehealth services. Typically, desktops, laptops, tablets, and smartphones used at home are personal devices not managed by UCI Health IT.

The exact number of personal devices being used by providers is unknown as there is no log or other method that is being used to track such information. In addition, many providers are conducting telehealth services from home. Various controls are in place when connecting to Zoom via MyChart, including the use of the Cisco Virtual Private Network (VPN) for desktops and laptops and Epic's secure mobile applications called Haiku and Canto for smartphones and tablets, respectively. However, the use of personal devices not managed by UCI Health IT may pose other security risks, such as unpatched security vulnerabilities, lack of encryption, inadequate access controls, among others, which would otherwise be mitigated on UCI Health IT-managed devices.

Recommendation

Management should either ensure that personal devices comply with university security standards or ensure that all telehealth providers are using UCI Health owned and managed devices. In addition, management should implement a system for tracking which providers are using personal devices and who are providing telehealth services from home.

Management Action Plan

Management will investigate the feasibility and cost/benefit of implementing a process that will identify the use of personal devices used to conduct Telehealth sessions. Management will also discuss with senior leadership the best course of

action to mitigate identified risks. Implementation will be based on their approval and support.
After the audit, management provided the following information:

Providers access Epic via two factor authentication then they utilize Epic to start the Telehealth visit. Our telehealth platform is encrypted, and providers are expected to utilize Zoom via Epic (secured platform). Providers follow the process they are trained on, utilizing their personal devices to provide telehealth services outside the UCI Network.

Due date: Completed

4. **Teladoc Health Security Controls**

Background

Since implementation and management of information security controls is the responsibility of the supplier of cloud services, as is the case with Teladoc Health, the most feasible method for verifying adequacy of controls is for UCI Health to obtain and review an independent third-party assessment report of Teladoc Health's information security controls.

Accordingly, the UC Data Security and Privacy Appendix (Appendix-DS), which is attached to the signed agreement between UCI Health and Teladoc Health ("Teladoc Agreement"), requires that, "Prior to agreeing to the terms of this Appendix, and periodically thereafter (no more frequently than annually) at UC's request, Supplier will provide assurance, in the form of a third-party audit report or other documentation acceptable to UC, such as SOC 2 Type II, demonstrating that appropriate information security safeguards and controls are in place."

Appendix-DS also states that, "Supplier will establish, maintain and comply with an Information Security Plan, which will contain, at a minimum, such elements as those set forth in Attachment 1 to this Appendix." Appendix-DS further states that, "On at least an annual basis, Supplier will review its Information Security Plan, update and revise it as needed, and submit it to UC upon request."

Observation

According to UCI Health management, an independent third-party security assessment report, such as a SOC 2 Type II, was not obtained, as required by Appendix-DS. In addition, although Appendix-DS does not require UCI Health management to obtain Teladoc Health's Information Security Plan, it is essential that management does so to verify that such a plan exists and that it complies with the UC "Computer System Security Requirements" set forth in Attachment 1 to Appendix-DS.

Recommendations

To verify that the Teladoc application, Teladoc Health's servers and network infrastructure, and the use of computer equipment by Teladoc Health doctors meet UC and regulatory requirements for information security, IAS recommends that UCI Health management:

a. Obtain an independent third-party audit report, such as a SOC 2 Type II, HITRUST, or other independent report, to verify that adequate safeguards are in place to meet UC and regulatory security requirements.

b. Obtain and review Teladoc's Information Security Plan to verify that it is in compliance with the UC "Computer System Security Requirements" as documented in Attachment 1 of Appendix-DS.

Management Action Plan

UCI Health management will obtain the following documents from Teladoc Health and verify compliance with UC and regulatory requirements for information security.

a. An independent third-party audit report, such as a SOC 2 Type II, HITRUST, or other independent report.

    Note: After the audit, a HITRUST letter of certification was provided to IAS. However, the actual HITRUST report was not provided.

    Due date: 8/31/22

b. Teladoc's Information Security Plan to verify that it is in compliance with the UC "Computer System Security Requirements" as documented in Attachment 1 of Appendix-DS.

    Note: After the audit, management provided documentation of Teladoc's Information Security Plan.

    Due date: Completed