UC RIVERSIDE UNIVERSITY OF CALIFORNIA
School of Medicine
Compliance Advisory Services

THE ADVISOR

News & Updates

June 16, 2020

Welcome Matthew Summerville, MBA, CISSP, CISA

Compliance Advisory Services would like to introduce Matthew Summerville, the new Information Security Officer for SOM. In this role, Matthew will provide strategic direction and leadership to ensure that data assets are protected, and will develop policies and security architectures to reduce cyber threats in order to keep SOM data secure. Matthew comes with expertise in developing synergistic partnerships across organizations and providing essential security oversight in various industries. Outside the office, he is a foodie, a gamer and enjoys traveling.
Please extend a warm welcome to Matthew as a new and important member of the SOM team!

Working Securely from Home

Some security professionals believe that the world will soon experience the largest security breach to date. Under normal circumstances, bad actors and nations do not target a typical home user because the value of one person's data is relatively small, compared to the value of an entire organization's data. Furthermore, organizations typically have security requirements for their own devices that makes it more difficult to compromise the data. The move to 'work from home' is driving up the ROI on targeting home users because they are using less secure consumer-grade devices and networks to access organizational data. Additionally, some nations are publishing disinformation on COVID and are targeting organizations where COVID research takes place; UC being one of them. Though many SOM faculty and staff have already been working from home for over two months at this point, please take this time to review the Telework Guidelines, the Zoom Guidelines, the Notice on COVID-19 Phishing Awareness, and the following tips and resources to help you work from home more securely and reduce the risk of breach.

- Please report missteps in HIPAA compliance to your manager or Compliance as necessary
- Utilize the OIT-provided resources for remote work
- Be conscious of your Duo authorizations and report any suspicious or buggy instances
- Report suspicious emails using the "Report Phish" button in Outlook
- Wherever possible, avoid using the University VPN on personal devices
- If setting up email or call forwarding, ensure your manager is involved
- Use the security measures for video conferencing

Resources

Many of us have been working from home for over two months at this point but please take this time to review the following guidelines:

Telework Guidelines
Zoom Guidelines
Notice on COVID-19 Phishing Awareness

and the following tips:
Telework Guidance— NSA & DHS CISA
Security Tips for WFH — FTC Consumer Information
User's Guide to Telework and BYOD Security — DOC NIST
Telework and Small Office Network Security Guide — CIS

Technology Purchases

Many technology purchases require additional review and approval processes that can delay the purchase request. In accordance with systemwide policy, Office of Information Technology (OIT), Business Operations (BO), Compliance Advisory Services, developed an IT Procurement Process to determine if the technology being purchased will be storing, processing, or transmitting sensitive data. Based on these determinations additional documents may be required from the vendor. To expedite purchases please review requirements and workflows at https://somit.ucr.edu under Faculty and Staff Services. As always, Compliance Advisory Services team members are available for questions and assistance.

COVID-19 CMS Telehealth Coding Update

CMS recently announced a change that greatly impacts providers' visit-to-visit documentation. This change being the level selection for office/outpatient E/M visits when furnished via Medicare Telehealth that would allow providers to use either Medical Decision Making (MDM) or to use Time as the defining factor in selecting the appropriate level of service for office/outpatient E&M (ONLY) telehealth encounters- as it will be effective January 1, 2021.

If time is used, the provider can include their total time associated with the service on the day of the encounter. Total time includes *face-to-face time* and *non-face-to-face time* like preparing to see the patient (e.g. review of tests) and documenting clinical information in the electronic health record. The appropriate history and exam components may be necessary to show medical necessity and the complexity of the service but will not be included in the scoring process of the E/M code. Keep in mind this is interim guidance- meaning post-PHE has the possibility of reverting to pre-PHE rules until January 1, 2021.

Attached is the latest Telehealth Fact sheet for more information on Time and MDM.

Policies and Procedures

The Compliance staff work collaboratively with stakeholders in the development of the School of Medicine's Policies and Procedures, ensuring compliance with State and Federal requirements as well as alignment with UCR and UCOP policy. Once policies have been drafted, they are reviewed and approved by the Compliance Committee before signature by the Dean. All approved Policies and Procedures can be viewed on the UCR SOM intranet located at:

https://medschoolcompliance.ucr.edu/policies-procedures

Below is the list of new and updated policies for the last quarter:

All GME Policies:
950-09-003 - Support for GME Programs During Disasters
950-09-004 - Moonlighting
950-09-006 - Transfer To and From GME Program
950-09-007 - Program Reduction-Closure
950-09-008 - Harassment and Reporting Procedure
950-09-009 - Duty Hours
950-09-010 - Interactions With Vendors and Health Care Product Manufactures
950-09-011 - Supervision of Residents
950-09-012 - Accommodation for Disabilities
950-09-013 - Alcohol and Substance Abuse
950-09-014 - Selection of Residents
950-09-015 - Non-Competition
950-09-016 - Resident Reporting of Concerns
950-09-017 - Special Review
950-09-018 - Leave and Time Off
950-09-019 - Promotion and Renewal Policy
950-09-020 - Academic Actions:

Compliance Policies:
950-02-008 – Observers and Vendors in Clinical Areas
950-02-011 – Sanctions
950-02-010 – Law Enforcement Policy
950-02-006 – Photography Multi-Media Privacy and Security Recording of Patients
950-02-015 – HIPAA Breach Risk Assessment and Mitigation
950-02-013 – Application of the Minimum Necessary Standard to Uses, Disclosures and Requests to Protected Health Information

UME Policies:
950-06-001 – International Co-and Extra-Curricular Travel Policy

Clinical Policies:
950-05-015 Vendor Exhibitors

UC RIVERSIDE UNIVERSITY OF CALIFORNIA
School of Medicine
Compliance Advisory Services

NEWSLETTER

News & Updates

June 3, 2020

Welcome Matthew Summerville, MBA, CISSP, CISA

Compliance Advisory Services would like to introduce Matthew Summerville, the new Information Security Officer for SOM. In this role, Matthew will provide strategic direction and leadership to ensure that data assets are protected, and will develop policies and security architectures to reduce cyber threats in order to keep SOM data secure. Matthew comes with expertise in developing synergistic partnerships across organizations and providing essential security oversight in various industries. Outside the office, he is a foodie, a gamer and enjoys traveling.

Please extend a warm welcome to Matthew as a new and important member of the SOM team!

Working Securely from Home

Some security professionals believe that the world will soon experience the largest security breach to date. Under normal circumstances, bad actors and nations do not target a typical home user because the value of one person's data is relatively small compared to the value of an entire organization's data. Furthermore, organizations typically have security requirements for their own devices that makes it more difficult to compromise the data. This move to work from home is driving up the ROI on targeting home users because they are using insecure consumer-grade devices to access organizational data. On top of that, some nations are publishing disinformation on COVID and are targeting COVID-related research. Please take the time to review the Telework Guidelines, the Zoom Guidelines, the Notice on COVID-19 Phishing Awareness, and the following tips and resources to help you work from home more securely and reduce the risk of breach.

- Please report privacy missteps in to your manager or Compliance, as necessary
- Utilize the OIT-provided resources for remote work
- Be conscious of your Duo authorizations and report any suspicious or buggy instances
- Report suspicious emails using the "Report Phish" button in Outlook
- Wherever possible, avoid using the University VPN on personal devices
- If setting up email or call forwarding, ensure your manager is involved
- Use the security measures for video conferencing

Resources

TELEWORK BEST PRACTICES - Cybersecurity and Infrastructure Security Agency
Online security tips for working from home - Consumer Information
Detailed User's Guide to Telework and BYOD Security – National Institute of Standards and Technology
Detailed Telework and Small Office Network Security Guide – Center for Internet Security

Technology Purchases

Many technology purchases require additional review and approval processes that can delay the purchase request. In accordance with systemwide policy, Office of Information Technology (OIT), Business Operations (BO), Compliance Advisory Services, developed an IT Procurement Process to determine if the technology being purchased will be storing, processing, or transmitting sensitive data. Based on these determinations additional documents may be required from the vendor. To expedite purchases please review requirements and workflows at https://somit.ucr.edu under Faculty and Staff Services. As always, Compliance Advisory Services team members are available for questions and assistance.

COVID-19 CMS Telehealth Coding Update

CMS recently announced a change thatgreatly impacts providers' visit-to-visit documentation. This change being the level selection for office/outpatient E/M visits when furnished via Medicare Telehealth that would allow providers to use either Medical Decision Making (MDM) or to use Time as the defining factor in selecting the appropriate level of service for office/outpatient E&M (ONLY) telehealth encounters- as it will be effective January 1, 2021.

If time is used, the provider can include their total time associated with the service on the day of the encounter. Total time includes *face-to-face time* and *non-face-to-face time* like preparing to see the patient (e.g. review of tests) and documenting clinical information in the electronic health record. The appropriate history and exam components may be necessary to show medical necessity and the complexity of the service but will not be included in the scoring process of the E/M code. Keep in mind this is interim guidance- meaning post-PHE has the possibility of reverting to pre-PHE rules until January 1, 2021.

Attached is the latest Telehealth Fact sheet for more information on Time and MDM.

Policies and Procedures

The Compliance staff work collaboratively with stakeholders in the development of the School of Medicine's Policies and Procedures, ensuring compliance with State and Federal requirements as well as alignment with UCR and UCOP policy. Once policies have been drafted, they are reviewed and approved by the Compliance Committee before signature by the Dean. All approved Policies and Procedures can be viewed on the UCR SOM intranet located at:

https://medschoolcompliance.ucr.edu/policies-procedures

Below is the list of new and updated policies for the last quarter:

All GME Policies:
950-09-003 - Support for GME Programs During Disasters
950-09-004 - Moonlighting
950-09-006 - Transfer To and From GME Program
950-09-007 - Program Reduction-Closure
950-09-008 - Harassment and Reporting Procedure
950-09-009 - Duty Hours
950-09-010 - Interactions With Vendors and Health Care Product Manufactures
950-09-011 - Supervision of Residents
950-09-012 - Accommodation for Disabilities
950-09-013 - Alcohol and Substance Abuse
950-09-014 - Selection of Residents
950-09-015 - Non-Competition
950-09-016 - Resident Reporting of Concerns
950-09-017 - Special Review
950-09-018 - Leave and Time Off
950-09-019 - Promotion and Renewal Policy
950-09-020 - Academic Actions:

Compliance Policies:
950-02-008 – Observers and Vendors in Clinical Areas
950-02-011 – Sanctions
950-02-010 – Law Enforcement Policy
950-02-006 – Photography Multi-Media Privacy and Security Recording of Patients
950-02-015 – HIPAA Breach Risk Assessment and Mitigation
950-02-013 – Application of the Minimum Necessary Standard to Uses, Disclosures and Requests to Protected Health Information

UME Policies: