June 1, 2015

KIM GILLESPIE
Chief Compliance Ofr
0836

KEN WOTTGE
Chief Information Security Ofr
8935

Subject: ***Enterprise Security – Phase II***
Project 2015-17

With input from the University of California, San Diego (UCSD) Health Sciences (HS) Chief Compliance Officer (CCO) and Chief Information Security Officer (CISO), Audit & Management Advisory Services (AMAS) designed and conducted surveys of UCSDHS members to obtain information on mobile device use on the UCSDHS network. This report provides an overview of this project and a summary of the survey results.

Background

In Phase One of Enterprise Security[1], it was determined that the UCSDHS Information Services and Telecommunications (IS) does not have control or knowledge over personally-owned (i.e. Bring Your Own Device – BYOD) and certain University-owned mobile devices that access sensitive information including electronic protected health information (e-PHI) and personally-identifiable information (PII) through the UCSDHS network. While there are instances when departments and users contact UCSDHS IS to acquire new mobile devices, faculty generally use discretionary funds to purchase mobile devices without UCSDHS IS coordination or intervention. Additionally, Health System users that do not have University-owned mobile devices have the ability to use their personal devices to connect to the network. Because UCSDHS IS is currently unable to limit the devices that connect to the UCSDHS network, there is potential that such devices are stolen and used to access sensitive information, which would leave the University at risk of a Health Insurance Portability and Accountability Act (HIPAA) reportable event.

For purposes of the survey, the UCSDHS CISO provided information on departments within the UCSDHS to determine which departments were most likely to access HIPAA-protected information and/or may not have information technology (IT) staff that coordinates their security efforts with UCSDHS IS. The original plan was to survey the department business officers (DBOs) of a range of departments and obtain a general understanding of the level of security implemented on University-owned mobile devices. From the survey responses, a sample of users from the higher risk departments were to be surveyed. After AMAS received responses from the DBO surveys, it was determined that it would be beneficial for information-gathering purposes to survey as many users as possible. Therefore, AMAS queried FinancialLink for the e-mail addresses of users whose home department was included in the DBO sample.

[1] The report for Phase One of Enterprise Security was called Health Science E-mail and Mobile Device Encryption, released in November 2014.

Audit Objective, Scope and Procedures

The objective of our survey was to obtain information on how University- and personally-owned mobile devices in UCSDHS are being used in order to determine how business processes related to securing ePHI and PII can be improved. In order to achieve our objective, we performed the following procedures:

- Interviewed the UCSDHS CISO to determine which UCSDHS departments to survey;
- Developed two web-based surveys (DBO Survey - ***Attachment A*** and User Survey – ***Attachment B)*** with input from the UCSDHS CISO and CCO;
- Reviewed DBO survey results and interviewed DBOs with follow-up questions;
- Administered the User Survey to approximately 4,700 users (including DBOs); and
- Compiled a summary of survey responses for selected questions (***Attachment C)***.

Summary

Responses were received from all ten department business officers surveyed. Based on follow-up conference calls with DBOs, most departments monitor at least some University-owned laptops. However, monitoring and managing tablets and smartphones is notably difficult. Additionally, most DBOs mentioned that faculty and staff members have the ability to purchase mobile devices without IT or Business Office intervention, so the DBOs are likely unaware of all University-owned mobile devices connecting to the network. When faculty or staff members purchase a mobile device under the supervision of IT or the Business Office, IT has the opportunity to configure the device to have certain security settings (e.g. password-protection, setting a limited number of password attempts, the ability to wipe the device remotely, etc.) as well as make security recommendations to the user. However, these security settings can easily be modified once full control of the device is given to the end user.

While the departments expressed interest in increasing the protection of the University's sensitive information, they pointed out that it would not be feasible to monitor these mobile devices without a proper policy to enforce or the resources available at the department level. Currently, the closest University policies are University of California Business and Finance Bulletin IS-3: *Electronic Information Security* and UCSD's PPM 135-3: *Network Security*, neither of which are well-known among most UCSDHS users, and neither specifically address BYOD. In Phase One, it was determined that UCSDHS IS, along with Compliance and Privacy, would develop guidance related to BYOD, specifically addressing security and management requirements for the personally-owned mobile devices. The development of this guidance, in addition to continually educating the users of the existing policies (including the minimum network connection standards necessary before connecting a device to the network), would benefit the University and decrease the University's risk of exposure.

We received six hundred thirty-one (631) responses to the user survey that were at least partially completed, which represents a response rate of approximately 13.4%. A summary of responses to select questions from the DBO and user surveys is included in ***Attachment C***. As can be seen

in the attachment, 46 users responded that they access sensitive information using University-owned mobile devices[2]. Most users answered that their devices are at least password/PIN-protected and about half responded they have anti-virus software. However, responses indicated that several users are unsure of the security settings on their devices, if any. Detailed information for each survey question was provided to the CCO and CISO under separate cover.

Audit & Management Advisory Services appreciates the cooperation and assistance provided during the review. Because this report contains no findings or recommendations, a management response is not required.

UC policy requires that all draft audit reports, both printed (copied on tan paper for ease of identification) and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel or destroy them at this time.

If you have any questions regarding this report, please call me at 534-3617.

David Meier
Director
Audit & Management Advisory Services

cc: E. Babakanian
D. Brenner
J. Bruner
S. Vacca
P. Viviano

[2] Question 14 on page 3 of Attachment C.

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

UCSD Health Sciences Mobile Device Questionnaire (DBO/MSO)

*1. Please enter your name.

Full Name:

*2. Please select your department.

- ◯ Department of Medicine
- ◯ Neurosciences
- ◯ Ophthalmology
- ◯ Psychiatry
- ◯ Moores Cancer Center
- ◯ Pediatrics
- ◯ Skaggs School of Pharmacy and Pharmaceutical Sciences
- ◯ Radiology
- ◯ Surgery
- ◯ Anesthesiology

Other (please specify)

University-Owned Mobile Devices

Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*3. Does your department purchase mobile devices for your users?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 2

The following questions relate to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*4. What would you estimate is the number of University-owned mobile devices in your department?

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

*5. What types of devices do you provide? Check all that apply.

- [ ] Tablet
- [ ] Smartphone
- [ ] Laptop
- [ ] Chromebook
- [ ] Netbook
- [ ] iPod

Other (please specify)

*6. How are the mobile devices purchased? Check all that apply.

- [ ] Purchased through the UCSD Bookstore
- [ ] Purchased by department directly from the vendor
- [ ] Facilitated through Information Services

Other (please specify)

*7. Do you actively manage or monitor mobile device usage?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 3

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*8. How are the mobile devices managed? Check all that apply.

- [ ] AirWatch
- [ ] Casper Suite
- [ ] User manages device
- [ ] MS Intune
- [ ] SCCM (System Center Configuration Manager)
- [ ] Do not know
- [ ] None

Other (please specify)

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

University-Owned Mobile Devices Pg 4

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 9. Do you have any local or University policies that you follow for managing mobile devices?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 5

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 10. What policies do you follow for managing mobile devices?

University-Owned Mobile Devices Pg 6

The following question relates to University-Owned Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 11. Do you have any challenges managing mobile devices?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 7

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 12. Please describe the challenges you have had when managing mobile devices.

University-Owned Mobile Devices Pg 8

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

*13. Are security configurations set or software installed on the mobile devices? Check all that apply.

- [ ] Yes - We recommend users install security software
- [ ] Yes - Require users install security software
- [ ] Yes - installed by department
- [ ] No - Do not require or recommend the installation of security software.

University-Owned Mobile Devices Pg 9

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*14. What configurations or type(s) of software are required or recommended?

University-Owned Mobile Devices Pg 10

The following question relates to UNIVERSITY-OWNED Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*15. Are there any challenges or problems with security software on the mobile devices?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 11

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*16. Please describe the challenges or problems you have had with security software on the mobile devices.

University-Owned Mobile Devices Pg 12

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

* 17. Are users permitted to access sensitive information (e.g. HIPAA, PII, or PCI, etc.) via these mobile devices?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 13

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 18. Please provide types of sensitive information accessed (if known) and how the information is accessed (Epic app, web browser, etc.) on mobile devices.

University-Owned Mobile Devices Pg 14

The following questions relate to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 19. What are your expectations of your users' use of the mobile devices?

* 20. Who is assigned mobile devices (request only, by job description, everyone, etc.)?

* 21. Who approves device assignments?

* 22. Do you provide training on how to use the device?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices Pg 15

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

* 23. Please describe the training you provide (e.g. the format, who attends, how often it's offered, whether it's required, etc.).

University-Owned Mobile Devices Pg 16

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 24. Are the devices standardized?

- ◯ Yes
- ◯ No

Personally-Owned Mobile Devices

The next few questions relate to PERSONALLY-OWNED mobile devices.

Personally-Owned Mobile Devices

The following question relates to PERSONALLY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 25. Does the department have a Bring Your Own Device (BYOD) policy that limits or restricts the use of personal devices on University networks?

- ◯ Yes
- ◯ No

Personally-Owned Mobile Devices Pg 2

The following question relates to PERSONALLY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 26. Please provide additional information on the department's BYOD policy.

Thank you for completing the survey!

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

UCSD Health Sciences Mobile Device Questionnaire (User)

Disclaimer: Your responses will remain anonymous.

*1. Please select your department.

- ◯ Department of Medicine
- ◯ Neurosciences
- ◯ Ophthalmology
- ◯ Psychiatry
- ◯ Moores Cancer Center
- ◯ Pediatrics
- ◯ Skaggs School of Pharmacy and Pharmaceutical Sciences
- ◯ Radiology
- ◯ Surgery
- ◯ Anesthesiology
- ◯ Other

Other (please specify)

University-Owned Mobile Devices

The following questions relate to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*2. What University-supplied/owned mobile devices are you currently using? Check all that apply.

- ☐ Tablet
- ☐ Smartphone
- ☐ Laptop
- ☐ Chromebook
- ☐ Netbook
- ☐ iPod
- ☐ N/A, I do not have a University-owned mobile device
- ☐ Other

Other (please specify)

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

*3. When did you receive your first business mobile device?

*4. How did you obtain a business mobile device?

- ◯ Department assigned
- ◯ Submitted requested

Other (please specify)

*5. Were you given a choice in the type of device?

- ◯ Yes
- ◯ No

*6. How long have you had your current mobile device(s)?

*7. Did you receive any training on how to use your device (current or previous)?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices (Cont.)

The following questions relate to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

*8. Please describe the training you received for your mobile device.

University-Owned Mobile Devices (Cont.)

The following questions relate to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

* 9. Who is responsible for installing new software/system updates, etc.?

- ◯ IT support staff
- ◯ Self
- ◯ Both
- ◯ Other

Other (please specify)

* 10. Who purchases the software used on the mobile device?

- ◯ IT support staff
- ◯ Self
- ◯ Both
- ◯ Other

Other (please specify)

* 11. Who do you go to when your mobile device is malfunctioning?

* 12. What type(s) of security settings/software, if any, are enabled/installed on the mobile device(s) (e.g. password/PIN entry, virus software, limited number of password attempts, etc.)?

* 13. What do you use your mobile device(s) for? Please include any personal and business uses.

* 14. Do you use your device to access sensitive information (e.g. HIPAA, PII, PCI, etc.)?

- ◯ Yes
- ◯ No

University-Owned Mobile Devices (Cont.)

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

The following question relates to UNIVERSITY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 15. What type of sensitive data do you access and how do you access it (e.g. via Epic application or web browser)?

* 16. How do you ensure the information is secure or appropriately cleared from the device at the end of the session?

Personally-Owned Mobile Devices

The next few questions relate to PERSONALLY-OWNED mobile devices.

Personally-Owned Mobile Devices

The following question relates to PERSONALLY-OWNED mobile devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 17. Do you use your personally-owned device(s) for business purposes?

- ◯ Yes
- ◯ No

Personally-Owned Mobile Devices (Cont.)

The following question relates to PERSONALLY-OWNED mobile devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 18. Do you use your personally-owned device(s) to access University-housed sensitive information (e.g. PII, ePHI, etc.) ?

- ◯ Yes
- ◯ No

Personally-Owned Mobile Devices (Cont.)

The following question relates to PERSONALLY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

UCSD Audit & Management Advisory Services Mobile Device Questionnaire

* 19. Do you follow any local or University policies when using your personally-owned devices to access University-housed sensitive information (e.g. PII, ePHI, etc.)?

- ◯ Yes
- ◯ No

Personally-Owned Mobile Devices (Cont.)

The following question relates to PERSONALLY-OWNED Mobile Devices.
Note: Mobile devices are portable computing devices such as tablets, smartphones, laptops/Chromebooks/netbooks, iPods, etc.

* 20. Please provide additional information on the policies you follow when using your personally-owned devices to access University-housed sensitive information.

Thank you for completing the survey!

Enterprise Security - Phase II
Project 2015-17

Attachment C

DBO Survey Responses - Select Questions

Question 5. How many departments provide each type of device? (9 responses)	
Tablet	8
Smartphone	9
Laptop	9
Netbook	1
iPod	2

Question 6. How are the mobile devices purchased by each department? (9 responses)	
Purchased through the UCSD Bookstore	9
Purchased by department directly from the vendor	8
Facilitated through Information Services	3

Question 7. Does the department actively manage or monitor mobile device usage? (10 responses)	
Yes	2
No	8

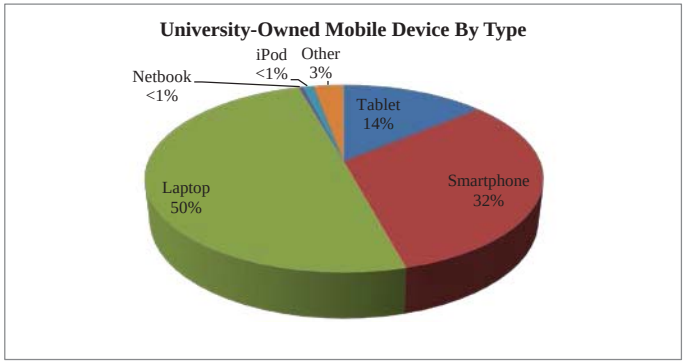
Question 13. Number of departments recommending, configuring, or installing security settings and/or software on mobile devices. (9 responses)	
Yes - We recommend users install security software	7
Yes - Require users install security software	3
Yes - installed by department	4
No - Do not require or recommend the installation of security software	0

Question 25. Does the department have a Bring Your Own Device (BYOD) policy that limits or restricts the use of personal devices on University networks? (9 responses)	
Yes	0
No	9

User Survey Reponses - Select Questions

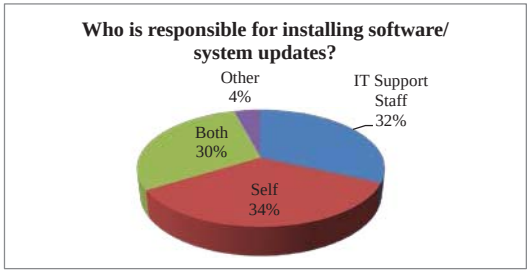
University-Owned Mobile Devices

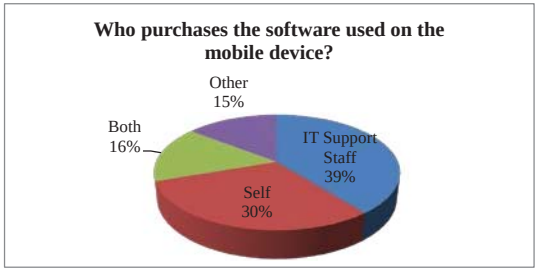
	Department											
Q2. Type of Device	**Anesthesiology**	**Dept of Medicine**	**Moores Cancer Center**	**Neurosciences**	**Ophthalmology**	**Pediatrics**	**Psychiatry**	**Radiology**	**Skaggs**	**Surgery**	**Other**	**Total**
Tablet	0	13	3	3	2	9	1	2	3	1	1	**38**
Smartphone	0	17	7	14	4	16	8	1	5	14	1	**87**
Laptop	2	43	15	16	7	20	16	6	6	5	0	**136**
Chromebook	0	0	0	0	0	0	0	0	0	0	0	**0**
Netbook	0	0	0	0	0	0	1	0	0	0	0	**1**
iPod	0	1	1	0	0	0	0	0	0	1	0	**3**
Other	1	5	0	0	1	1	0	0	0	0	0	**8**
Total Number of Mobile Devices	**3**	**79**	**26**	**33**	**14**	**46**	**26**	**9**	**14**	**21**	**2**	**273**
No University Owned Device	15	139	38	38	11	44	67	32	17	23	2	**426**
Number of Responses Received	18	197	58	60	22	77	90	39	25	41	4	**631**



Q9. Who is responsible for installing software/system updates?	
IT Support Staff	46
Self	50
Both	43
Other	6
Total # of Responses	145

Q10. Who purchases the software used on the mobile device?	
IT Support Staff	57
Self	44
Both	23
Other	21
Total # of Responses	145

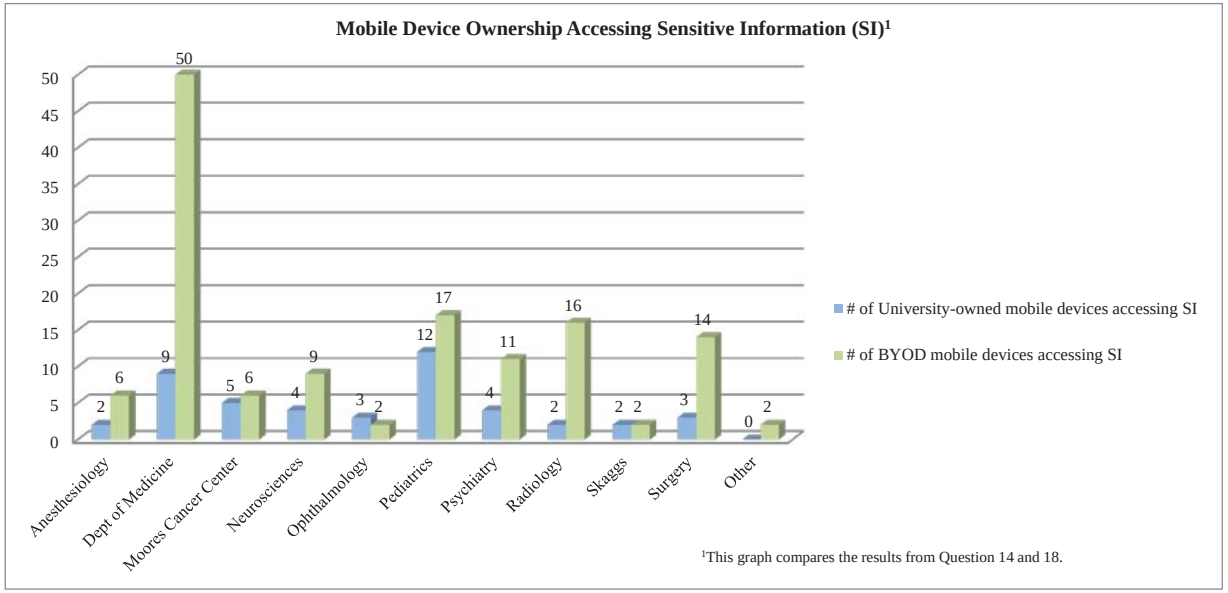




Q14. How many users use their University-owned mobile devices to access sensitive information (SI) (e.g. HIPAA, PII, ePHI, etc.)?			
	# of University-owned mobile devices accessing SI	# Of Responses	% of Business Devices used to access SI
Anesthesiology	2	2	100%
Dept of Medicine	9	36	25%
Moores Cancer Center	5	16	31%
Neurosciences	4	14	29%
Ophthalmology	3	9	33%
Pediatrics	12	23	52%
Psychiatry	4	15	27%
Radiology	2	6	33%
Skaggs	2	8	25%
Surgery	3	15	20%
Other	0	1	0%
Total	46	145	32%

Personally-Owned Mobile Device Use

	Q17. Do you use your personally-owned device(s) for business purposes?			Q18. Do you use your personally-owned device(s) to access University-housed sensitive informatnoi (e.g. PII, ePHI, etc.)?		
	# of Personal Devices used for Business Purposes	# Of Responses	% of Business Use on Personal Devices	# of BYOD mobile devices accessing SI	# of Responses	% of users accessing SI on Personal Devices
Anesthesiology	12	16	75%	6	16	38%
Dept of Medicine	141	175	81%	50	174	29%
Moores Cancer Center	38	53	72%	6	53	11%
Neurosciences	30	51	59%	9	51	18%
Ophthalmology	12	19	63%	2	19	11%
Pediatrics	46	66	70%	17	64	27%
Psychiatry	60	79	76%	11	79	14%
Radiology	33	38	87%	16	38	42%
Skaggs	13	23	57%	2	23	9%
Surgery	28	37	76%	14	37	38%
Other	3	3	100%	2	3	67%
Total	416	560	74%	135	557	24%



[1]This graph compares the results from Question 14 and 18.