



Adding Privacy Questions To Your Vendor Security Assessment and Why it is Important

SCCE HIGHER EDUCATION COMPLIANCE CONFERENCE

JUNE 2022

1



MICKI JERNIGAN, JD, MPH, CHC, CHPC, CCEP
AVP, ETHICS & COMPLIANCE, ENTERPRISE PRIVACY OFFICER
AUGUSTA UNIVERSITY and AUGUSTA UNIVERSITY HEALTH

DOUG WELCH, JD
ASSOCIATE GENERAL COUNSEL & CHIEF PRIVACY OFFICER
BAYLOR UNIVERSITY

2

2

POLLING QUESTION #1

- What is your primary role at your organization?
 - A. Privacy Officer
 - B. Security Officer
 - C. Legal counsel
 - D. Privacy office staff
 - E. Security office staff

3

3

WHY PRIVACY QUESTIONS ARE AN IMPORTANT PART OF VENDOR REVIEWS

Federal Laws and Regulations that govern data (non-exhaustive)

- ❖ FERPA
- ❖ HIPAA
- ❖ Common Rule
- ❖ The Privacy Act of 1974
- ❖ FTC's: COPPA; Health Breach Notification Rule; Red Flags Rules; GLBA; FCRA; FDCPA;

4

4

WHY PRIVACY QUESTIONS ARE AN IMPORTANT PART OF VENDOR REVIEWS

- ❖ EXPANDING NUMBER OF STATE SPECIFIC PRIVACY AND SECURITY LAWS AND REGULATIONS
- ❖ GDPR
- ❖ CHINA
- ❖ MULTITUDE OF OTHER NATIONS' LAWS AND REGULATIONS


5

POLLING QUESTION #2

- Where are privacy/security/data risk assessments conducted at your organization?
 - A. Privacy office
 - B. Security office
 - C. Legal office
 - D. Purchasing/procurement
 - E. Unsure

6


6



WHY PRIVACY QUESTIONS ARE AN IMPORTANT PART OF VENDOR REVIEWS

- ❖ OFTEN DE-CENTRALIZED AND INCONSISTENT REVIEWS OF VENDOR AGREEMENTS
 - Contracts
 - MOUs
 - Service Agreements
 - Purchase Orders
 - Work Orders

7



WHY PRIVACY QUESTIONS ARE AN IMPORTANT PART OF VENDOR REVIEWS

- ❖ OFTEN DE-CENTRALIZED AND INCONSISTENT REVIEWS OF VENDOR AGREEMENTS
 - Business Associate Agreements
 - Statements of Work
 - Research Agreements
 - Click-through Agreements

8

POLLING QUESTION #3

- When are privacy/security/data risk assessments conducted at your organization?
 - A. During RFP or similar process
 - B. Continual risk assessments with data mapping
 - C. During contract review (and renewal) process
 - D. When IT Security has time
 - E. Unsure

9

9

POLLING QUESTION #4

- Which documents are reviewed during privacy/security/data risk assessments at your organization?
 - A. Contract/MOU/Services Agreement
 - B. Business Associate Agreement only
 - C. Security review analysis
 - D. All of the above
 - E. Unsure

10

10

PRIVACY QUESTIONS TO ASK

- ❖ WHAT TYPES OF DATA WILL THE VENDOR HAVE?
- ❖ ARE ALL TYPES ADDRESSED/PROTECTED IN THE AGREEMENT?
- ❖ HOW WILL OUR DATA BE USED?
- ❖ HOW WILL OUR DATA BE DISCLOSED?

11

PRIVACY QUESTIONS TO ASK

- ❖ WHO AT THE VENDOR WILL HAVE ACCESS?
- ❖ WHAT LEVEL OF ACCESS IS GRANTED?
- ❖ HOW WILL VENDOR COMPLY WITH APPLICABLE LAWS AND REGULATIONS ON OUR BEHALF?
- ❖ WHEN WILL OUR DATA BE DESTROYED?


12



PRIVACY QUESTIONS TO ASK

- ❖ DOES THE VENDOR HAVE ADEQUATE CYBER INSURANCE COVERAGE AND INDEMNIFICATION LANGUAGE?
- ❖ CHOICE OF LAW
- ❖ STATE AGENCY OR PUBLIC UNIVERSITY PROTECTIONS


13



PRIVACY QUESTIONS TO ASK

- ❖ WHO IS RESPONSIBLE FOR PRIVACY NOTICES TO STUDENTS, EMPLOYEES, PATIENTS, RESEARCH PARTICIPANTS, the PUBLIC?
- ❖ ARE THE PRIVACY NOTICES ADEQUATE?


14



PRIVACY QUESTIONS TO ASK

- ❖ IS THE VENDOR ALLOWED TO AGGREGATE OR DE-IDENTIFY OUR DATA FOR THEIR PURPOSES?
- ❖ WATCH FOR DISGUISED WORDING THAT ALLOWS THE VENDOR TO MONETIZE YOUR DATA (sale, lease, license).


15



STRATEGIES TO ADD PRIVACY QUESTIONS TO THE VENDOR REVIEW PROCESS

- ❖ DETERMINE WHAT PROCESSES EXIST AT YOUR ORGANIZATION
- ❖ ARE THERE OPPORTUNITIES TO HAVE A PRIVACY REPRESENTATIVE ADDED TO EXISTING REVIEWS?


16



STRATEGIES TO ADD PRIVACY QUESTIONS TO THE VENDOR REVIEW PROCESS

- ❖ DOES YOUR INSTUTION UTILIZE THE HECVAT FROM EDUCAUSE?
- ❖ ADD PRIVACY QUESTIONS TO THE INFORMATION SECURITY REVIEW PROCESS, but remain involved

17



PRIVACY QUESTIONS and PURPOSES WILL CONTINUE TO EVOLVE

- ❖ LAWS AND REGULATIONS CHANGE
- ❖ INDIVIDUALS BECOME MORE AWARE OF THEIR PRIVACY RIGHTS

18

