

# Information Security Education Form

# Beaumont

<b>Privacy Investigation #</b> ██████████	<b>Employee Name</b> ██████████
<b>Describe Error (redact PHI)</b>	
Employee failed to lock his computer that resulted in an inappropriate use of Epic. A co-worker's demographic information was viewed in Epic, which is a HIPAA violation.	
<b>Who conducted the investigation?</b>	<b>Investigator Contact Information</b>
Shannon Robertson	Shannon M. Robertson   Compliance Coordinator Privacy Office   Compliance, Audit & Risk Department P: 248-602-1958

We identified a mistake that occurred in your work area. We were unable to identify the employee who made the mistake. Mistakes happen, however, this mistake resulted in patient information being shared inappropriately and may have had a **HIPAA Reportable Breach**.

### What is a Breach?

A breach occurs when a patient's protected health information ("PHI") is used, accessed or disclosed in a way that the law doesn't allow AND we were unable to mitigate the disclosure. When we have a Breach the law requires that we notify the patient of the error in writing and also the federal government's Office for Civil Rights (OCR). Corporate Privacy will notify the patient and OCR for our organization.

### What are violations of our information security policies?

A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results. No matter how minor, any security infraction must be reported directly so that the incident may be assessed and any appropriate action taken. **By not logging out of your computer, you allowed others to use your computer log on and password to access PHI. You are required to lock your computer or log out when you step away from the computer.**

### Other examples of Security Violations include:

- Sharing your computer logon and password with someone else or not safeguarding your password
- Placing protected health information on your home computer
- Using a flash drive that is not encrypted to store electronic PHI
- Walking away from a computer without logging out of your account or locking your screen
- Sending PHI outside Beaumont domain via unsecured email

### What are the consequences?

- The patient may suffer medical identity theft
- The patient may no longer trust that his/her information is protected at Beaumont Health
- The patient may leave the system/practice to seek care elsewhere
- Beaumont Health may suffer from a negative public perception (consider discussions in community/social media)
- There may be investigations by government agency (OCR), fines and penalties of up to \$1,500,000

**Please be mindful of keeping our patients' health information secure.** Continued errors may result in corrective action for workforce member. This communication is not meant to be punitive but as a reminder that these types of errors can have a far-reaching impact.

**If you have questions, you may always ask your manager or the Privacy Department. You may call 877-471-2422 to ask questions or report compliance concerns.**

You may report concerns anonymously to the Beaumont Health Trust Line at 800-805-2283, anytime.

_____ Employee Name (print)	_____ Employee Signature	_____ Date
_____ Manager Name (print)	_____ Manager Signature	_____ Date