Information Breach FAQs – Updated 6/23/17

What Happened?

On March 14, 2017 the Trios Health Information Management department identified electronic health record (EHR) access activity outside the normal job functions for one particular employee. An investigation was immediately started. The employee who impermissibly accessed patient records had access to our EHR applications to perform job responsibilities; however the employee utilized the EHR application to look up additional patients, where there was no obvious direct correlation to job responsibilities. The EHR fields that may have been impermissibly accessed include Trios Health dates of service/visits, diagnoses, and demographic information including address, date of birth, social security number, driver's license number, phone numbers, and email addresses.

Upon learning of this incident, Trios Health immediately took steps to limit EHR access by the individual and began conducting an extensive investigation. Further EHR application permissions were restricted to all staff within the employee's department as the investigation progressed. In response to our findings, and in accordance with our policies, we took disciplinary action against the employee including involuntary administrative leave, followed by termination upon confirming the nature and extent of the breach.

Trios Health completed its investigation into the situation on June 22, 2017, and is deploying additional and extensive privacy training to employees, and implementing standard auditing processes to protect patient health information.

Did the Breach affect hospital or clinic records?

The impermissible access was within our hospital EHR system. The majority of the access was within application functionality used by the employee for normal job-related functions; however that functionality was used to view patient data with no direct job-related correlation.

When were the affected records created?

Impermissible access activity from the employee occurred between 10/23/2013 and 3/31/2017. Affected records were created throughout the life span of the Kennewick Public Hospital District [formerly dba Kennewick General Hospital (KGH) and now dba Trios Health]. Any visits prior to the implementation of an EHR in 2009 have limited information available.

How many people were affected by this incident?

Investigation of the breach has revealed that the EHRs of 1,603 patients were accessed by the employee outside of normal job functions.

What actions did Trios Health take in response to this incident?

Trios Health immediately took a number of steps to investigate and limit the exposure of this information.

- Reviewed preliminary findings to rule out a legitimate business purpose for viewing the patient information in question.
- Placed employee on administrative leave pending investigation.
- Conducted interviews with the employee, as well as meetings with the employee and department manager.
- Upon breach confirmation, filed appropriately with the Office of Civil Rights and the Washington State Attorney General.
- Set up free identity theft protection services offering for one year for each affected patient, including a call center established to answer frequently asked questions and connect those seeking additional information with the Trios Health Information Management department.
- Posted a disclosure about the data breach with a link to these frequently asked questions on the Trios Health website.
- Deploying additional privacy training to employees, completing a full security risk assessment for privacy matters, auditing privacy policies, and implementing standard auditing processes to further protect patient information.

Does Trios Health have any indication that anyone has suffered identity theft as a result of this incident?

Trios Health has no way to know whether information has been or will be misused. However, it is recommended as a precautionary measure that patients affected by the information breach enroll in the free identity theft protection program being offered at no charge by Trios Health.

If my personal information was accessed by an unauthorized party, does that mean I will become a victim of identity theft?

Not necessarily. Even if someone did access your information, this does not mean that you have been, or will become, a victim of identity theft or that the unauthorized individual intends to use your personal information to commit fraud. Trios Health notified you about this incident so you can protect yourself. Trios Health recommends that affected patients enroll in the free identity theft protection program being offered.

What is credit monitoring?

Credit monitoring services protect primarily against new account fraud. This form of fraud occurs when a criminal uses your personal information to open credit card, mobile phone, or other financial accounts using your name, Social Security Number and other personal information. Beginning on the date of enrollment and for the specified time period, credit monitoring provides an alert whenever changes occur to your credit files.

Does Trios Health provide credit monitoring services?

Trios Health is offering people affected by this incident a one-year subscription to an **IdentityForce** identity theft protection and advanced fraud monitoring (which includes credit monitoring) service. Trios Health is communicating with these people directly by mail about how they can pursue this option, including the individual verification code they will need to access the service at Trios Health's expense.

How does The IdentityForce identity theft protection service offered by Trios Health work?

IdentityForce protects your identity, privacy, and credit by continuously monitoring your personal information, providing you with early warning notifications if any discrepancies are found.

My access code for advanced fraud monitoring doesn't work. What should I do?

Trios Health has partnered with **IdentityForce** to provide identity theft protection. You may contact the dedicated Trios Health **IdentityForce** support phone line at 1-877-288-4664 to speak with an **IdentityForce** membership services technician.

I did not receive a notification letter. Does this mean my personal information was not compromised?

During the week of May 29, 2017, Trios Health began sending letters to the last known home address of every individual believed to be affected by this incident and for whom Trios Health has current address information. Following the conclusion of the investigation on June 22, 2017, similar letters were also prepared for distribution to additional patients identified as having been affected beyond those initially notified.

If you have moved recently and you believe Trios Health does not have your current address, please call the Trios Health Information Management department at 509-221-5720 (option 2), Monday through Friday, between the hours of 7 a.m. and 4 p.m. Pacific Standard Time. You may also send any questions not answered in these FAQs directly to the Trios Health Information Management department at Privacy@trioshealth.org, and a Trios Health employee will contact you.

Should I contact the Social Security Administration to change my Social Security Number if my Social Security Number was part of the information that potentially was accessed/viewed?

The Social Security Administration is unlikely to change your Social Security Number in the absence of any evidence that your Social Security Number is actually being misused. In addition, according to information on the Social Security Administration's website, https://www.ssa.gov/pubs/EN-05-10064.pdf, changing your Social Security Number may create additional problems because you would lose your existing credit history and because other government agencies (including the Internal Revenue Service and the Department of Motor Vehicles) and private businesses (such as banks and credit reporting companies) are likely to have records under your current Social Security Number.