Key Message

- At Presbyterian, we are committed to protecting the privacy of our patients and members. Recently, Presbyterian discovered that an unauthorized person may have accessed some employee email accounts that contained health information. We are not aware of any improper use or attempted use of patient and member information. We are continuing to investigate and conduct a thorough review of each impacted Presbyterian email account.

- To help prevent this type of incident from happening again, Presbyterian is taking several steps to implement additional security measures to further protect our email system.

What Happened

- On June 6, 2019, Presbyterian discovered anonymous, unauthorized access was gained through a deceptive email to some of Presbyterian's workforce members around May 9, 2019.

- We believe that the unauthorized access to these email accounts was part of a scam or deceptive email trying to get information, known as "phishing."

- These email accounts included patient and/or health plan member names and might have contained dates of birth, Social Security numbers and clinical and/or health plan information.

- We deeply regret that unauthorized access to some of our workforce members' emails occurred.

- While our investigation is ongoing, we have no evidence indicating that any patient or member data has been used in any way.

- Once we became aware of this incident, Presbyterian secured these email accounts and alerted federal law enforcement.

- We are continuing to investigate and conduct a thorough review of each impacted Presbyterian email account.

What We Are Doing

- We take the responsibility of protecting the privacy of our patients and members very seriously.

- To help prevent this type of incident from happening again, Presbyterian is taking several steps to implement additional security measures to further protect our email system.

- In addition, all workforce members must successfully complete annual mandatory training about the importance and requirement to safeguard all information.

Affected Patient and Member Resources

- We are notifying affected patients and members via U.S. mail on August 2, 2019. This letter will explain what occurred, share steps we are taking to help prevent this from happening again and offer resources for affected patients and members.

- We recommend that affected patients and members review the statements that they receive from their health plan or health care provider(s) regarding their health care services.
    - If a patient or member sees any service that they believe they did not receive, they should contact the health plan or provider immediately.

- In addition, we are offering free identity theft protection services through ID Experts to patients and members whose ***Social Security information*** was involved in this breach.

    - These services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy and fully managed ID theft recovery services.
    - With this protection, MyIDCare will help affected patients and members resolve issues if their identity is compromised.
    - Those whose Social Security information was involved in this breach can also visit https://ide.myidcare.com/presbyterian-protect.

- All affected patients or members who have any questions can call 833-297-6405, Monday through Friday, 7 a.m. to 7 p.m. Mountain Time.

General FAQs

1. **What happened?**
   Presbyterian is committed to protecting the security and confidentiality of our patients' and members' information. On June 6, 2019, Presbyterian discovered anonymous, unauthorized access was gained through a deceptive email to some of Presbyterian's workforce members around May 9, 2019. We believe that the unauthorized access to these email accounts was part of a scam or deceptive email trying to get information, known as "phishing."

   These email accounts included patients' and members' names and might have contained dates of birth, Social Security numbers and clinical and/or health insurance information.

   We are not aware of any improper use or attempted use of patient and member information. We are continuing to investigate and conduct a thorough review of each impacted Presbyterian email account.

2. **What personal information was exposed?**
   These email accounts included patient and/or health plan member names and might have contained dates of birth, Social Security number and clinical and/or health plan information.

3. **If a patient or member has a question, where should I direct them to?**
   If impacted patients or members have any questions, they can call (833) 297-6405, Monday through Friday, 7 a.m. to 7 p.m. Mountain Time.

4. **What is Presbyterian doing to prevent this kind of data breach from happening again?**
   To help prevent this type of incident from happening again, Presbyterian is taking several steps and implementing additional security measures to further protect our email system. In addition, all workforce members must successfully complete annual mandatory training about the importance of and requirements related to protecting all information.

5. **Has the affected patient and member information been misused?**
   We are not aware of any improper use, or attempted use of patients and member information. We recommend that affected patients and members review the statements that they receive from their health plan or health care provider(s) regarding their health care services. If a patient or member sees any service that they believe they did not receive, they should contact the health plan or provider immediately.

6. **Why didn't you tell affected individuals about the loss of the data sooner?**
   With any such event, it takes time to investigate what happened, identify the affected individuals and arrange for the assistance services that are being offered.

   Once we became aware of this incident, Presbyterian secured these email accounts and alerted federal law enforcement.