

RMH

**RANSOM
MEMORIAL
HEALTH**

1301 S. Main Street
Ottawa, KS 66067

October 12, 2018

South Carolina Department of Consumer Affairs
PO Box 5757
Columbia, SC 29250-5246

RECEIVED

OCT 19 2018

**DEPT. OF CONSUMER
AFFAIRS**

RE: Security Breach Notification

To Whom It May Concern:

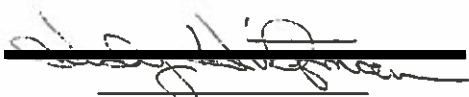
I serve as the Director and Chief Privacy Officer at Ransom Memorial Hospital in Ottawa, Kansas.

We are contacting you regarding a recent data security incident. On September 24, 2018, computer forensics revealed that nine employee email accounts were subject to unauthorized access. This resulted from phishing attacks from employee email accounts on May 31, 2018 and June 11, 2018. As a result of this incident, 16,366 records were subjected to unauthorized access, including one South Carolina resident. This includes some combination of personal health information, social security numbers, bank account numbers, credit card numbers, driver's license numbers, biometric data, and passport information may have also been exposed.

Please be assured that we have taken every step necessary to address the incident and worked with data privacy experts and other professionals. Ransom Memorial promptly notified the affected individuals in writing on or about October 12, 2018. In addition, Ransom Memorial has offered all affected persons credit monitoring for one year at Ransom Memorial's expense. Ransom Health has also implemented new security policies, adopted new security measures and encryption technology and additional security training procedures. A copy of the notification letter is attached hereto. Ransom Memorial is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Sincerely,



Judy Hintzman
Director and Privacy Officer



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

Address

October 12, 2018

RE: Important Security Notification. Please read this entire letter.

Dear Member:

We are contacting you regarding a recent data security incident. On September 24, 2018, computer forensics revealed that nine employee email accounts were subject to unauthorized access. This resulted from phishing attacks from employee email accounts on May 31, 2018 and June 11, 2018. As a result of this incident, 16,366 records were subjected to unauthorized access. This includes some combination of personal health information, social security numbers, bank account numbers, credit card numbers, driver's license numbers, biometric data, and passport information may have also been exposed. As a result, your personal information may have been potentially exposed to others.

What Did We Do to Protect Your Information?

Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us. Ransom Memorial Health worked with data privacy experts and other professionals to further protect your privacy. We are concerned about both our valued work force and patients that we serve, are dedicated to serving our patients who depend on Ransom Memorial Health for their care and have been victims of this attack. We have already taken steps to fix the issue and strengthen our systems, and will continue to do so throughout this response process and beyond. Ransom Memorial Health has undertaken the following measures to further protect your information:

- Changed the account passwords and usernames for all affected accounts;
- Retained forensic IT assistance to conduct a detailed audit to determine the extent of any unauthorized access;
- Retained outside cybersecurity counsel;
- HIPAA training for all employees;
- Safety Protocol and Policies;
- Implemented Additional Security for WorkStation Security and Access Controls for all employees; and
- Retained a forensic firm to perform an additional security audit to implement new security procedures.

In addition, and to help protect your identity, we are offering a complimentary one-year membership in TransUnion's *myTrueIdentity* Credit Monitoring Service. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.