



Attn: Compliance Department
200 Wood Hill Road
Rockville, MD 20850

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

«AddressBlock»

August 25, 2022

Re: «PATIENT_FIRST_NAME» «PATIENT_LAST_NAME»

«GreetingLine»

The privacy and security of the personal information we maintain is of the utmost importance to Jewish Social Service Agency ("JSSA"). We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident and let you know that we continue to take steps to protect your information. **Please note we have no evidence that any of your information has been misused.**

What Happened?

As a result of an internal investigation conducted beginning on June 24, 2022, JSSA became aware of an impermissible disclosure of your protected health information (PHI) or personally identifiable information (PII). The incident involving your PHI or PII was the unauthorized disclosure by a former employee to her personal email account.

What We Are Doing.

After an extensive and comprehensive manual document review, we discovered that on June 15th and June 23rd the former employee improperly disclosed PHI and PII to her personal email account. The unauthorized disclosures contained some of your PHI or PII.

We have taken steps to address the incident and to protect your and others' personal information from further improper use or disclosure. We also have taken steps to prevent similar incidents from recurring in the future. JSSA has:

- Sanctioned the employee involved by terminating their employment at JSSA;
- Requested an attestation from the former employee confirming that all PHI and PII has been permanently deleted from their email account;
- Addressed and will continue to monitor operational and technology updates or changes triggered by the incident to improve confidentiality, such as strengthening technology safeguards or administrative policies and/procedures; and
- Re-trained our employees on patient security practices and use of personal email.

What Information Was Involved.

After reviewing the information contained in these emails, we determined that the emails may have contained some of your protected health information, including your first and last name (or first initial and last name), and may have also included one or more of the following: date of birth, diagnosis, doctor's name or practice type, and/or treatment information. Significantly and fortunately, your social security number and financial information were not included in the improper disclosure.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also offering steps you can take to protect your medical information on the following page.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard all sensitive information maintained by JSSA. We will continue to evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 888-437-7055. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 5 p.m. EST.

Sincerely,

A handwritten signature in dark ink, appearing to read "Beatrice Turner".

Beatrice Turner
Privacy Officer

Protecting Your Medical Information.

We have no evidence that your personal information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.



Attn: Compliance Department
200 Wood Hill Road
Rockville, MD 20850

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

«AddressBlock»

August 25, 2022

Re: «PATIENT_FIRST_NAME» «PATIENT_LAST_NAME»

«GreetingLine»

The privacy and security of the personal information we maintain is of the utmost importance to Jewish Social Service Agency ("JSSA"). We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident and let you know that we continue to take steps to protect your information. **Please note we have no evidence that any of your information has been misused.**

What Happened?

As a result of an internal investigation conducted beginning on June 24, 2022, JSSA became aware of an impermissible disclosure of your protected health information (PHI) or personally identifiable information (PII). The incident involving your PHI or PII was the unauthorized disclosure by a former employee to her personal email account.

What We Are Doing.

After an extensive and comprehensive manual document review, we discovered that on June 15th and June 23rd the former employee improperly disclosed PHI and PII to her personal email account. The unauthorized disclosures contained some of your PHI or PII.

We have taken steps to address the incident and to protect your and others' personal information from further improper use or disclosure. We also have taken steps to prevent similar incidents from recurring in the future. JSSA has:

- Sanctioned the employee involved by terminating their employment at JSSA;
- Requested an attestation from the former employee confirming that all PHI and PII has been permanently deleted from their email account;
- Addressed and will continue to monitor operational and technology updates or changes triggered by the incident to improve confidentiality, such as strengthening technology safeguards or administrative policies and/procedures; and
- Re-trained our employees on patient security practices and use of personal email.

What Information Was Involved.

After reviewing the information contained in these emails, we determined that the emails may have contained some of your protected health information, including your first and last name (or first initial and last name), and may have also included one or more of the following: date of birth, diagnosis, doctor's name or practice type, and/or treatment information. Significantly and fortunately, your social security number and financial information were not included in the improper disclosure.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also offering steps you can take to protect your medical information on the following page.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard all sensitive information maintained by JSSA. We will continue to evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 888-437-7055. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 5 p.m. EST.

Sincerely,

A handwritten signature in dark ink, appearing to read "Beatrice Turner".

Beatrice Turner
Privacy Officer

Protecting Your Medical Information.

We have no evidence that your personal information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.