Volume 17 • December 2024

Ready to Serve

A Newsletter for USFHP Network Providers

Message from our Directors

Dear USFHP Family,

The holiday season is a time of reflection and renewal where we take stock of the year ending and look forward to fresh starts in the New Year. We hope each of you can take a moment to reflect on 2024 and all you were able to accomplish. We wish for everyone your winter season is full of peace, warmth, and good tidings.

Thank you so much for being part of our healthcare family. It is a privilege for everyone here at US Family Health Plan (USFHP) to assist you in supporting our members with their healthcare. Your choice and trust in our health plan allows us the honor of serving our members and their families. Each of our dedicated team members understand the dedication, commitment, and sacrifice you and your healthcare teams provide to serving our members. Our goal is to assist you in providing a healthcare of extraordinary quality to our members. Please do not hesitate to reach out to us at USFHP.

Along with everyone here at USFHP, we wish you happy holidays and a wonderful New Year!

With warm regards,

Diana Dass
US Family Health Plan
Executive Director

Alexander Park, MD
US Family Health Plan
Medical Director

In this Issue

US FAMILY HEALTH PLAN at PacMed

urac ACCREDITED HEALTH NETWORK

INFORMATION SECURITY TEAM MESSAGE:

Nine Cyber Security Tips for the Holidays and Always

Deterrence is the best defense. A big part of cyber security is being prepared for any attack. These tips can mean the difference between staying safe and having your data or identity compromised:

1. Avoid public Wi-Fi

Anyone can access public Wi-Fi, including cyber criminals. That's why it's called "public." Many public Wi-Fi services don't require any kind of authentication. Cyber criminals can put themselves between you and the connection point and gain access to the data you're sending or receiving.

It's also wise to avoid public computers when shopping online, booking plane tickets, transacting with your credit card, or logging into your personal accounts.

2. Beware of phishing scams

Phishing scams often target holiday shoppers. Urgent asks and unusual attachments are red flags for phishing scams.

Bad actors start 80-95% of cyber attacks with phishing, according to credible research.

The most common holiday phishing scam is the "shipping email scam." If you ever receive an email that appears to come from a shipping company, don't open the attached file or link. There's a high likelihood it's malware.

3. Don't click on links in emails or answer calls from numbers you don't recognize

Cyber criminals often send out fake emails or text messages with links that lead to malicious websites. Don't click on links if you receive an email or text message from an unknown sender. Even if you know the sender — if it looks like it's from your bank or insurance company, for example — it's best ***not*** to click on any links in the email. Instead, navigate to the site in your web browser to get the information. That way you can make sure it's legitimate.

Social engineering scams are also common during the holiday season. Most attackers will pose as representatives of your bank or credit card company and call you to report a transaction on your card. When this happens, don't engage in the conversation immediately. Instead, hang up and call the number on the back of your card to make sure you're speaking with a legitimate bank representative.

4. Review your credit card statements

When shopping online or booking hotels, flights, and activities for travel during the holidays, make it a habit to review your credit card statements regularly. You can quickly spot discrepancies and unusual or unauthorized charges.

Should you find any, report them immediately. It's also recommended that you set up notifications to inform you of any transactions or changes to your bank accounts and credit cards.

continued on page 3

INFORMATION SECURITY TEAM MESSAGE

continued from page 2

It's also a good practice to avoid throwing away papers, receipts, invoices, etc., that contain your credit card information or other personal data. Shred or burn confidential documents to prevent identity thieves from accessing them in the trash.

5. Keep your software up to date

One of the best ways to protect yourself from cyber-attacks is to keep your software current. This includes your operating system, web browser, and other software you use regularly.

Updating your software may seem like a chore. But it's vital to patch any security vulnerabilities that cyber criminals may have discovered. Attackers are constantly looking for new ways to exploit systems. Software updates help keep them at bay.

6. Use strong passwords

In its 2023 Data Breach Investigations Report, Verizon revealed that 81% of breaches used stolen or weak passwords.

Using strong passwords is one of the most important things you can do to protect your online accounts. Avoid using easily guessed words or phrases like "12345" or "abcdef." Most accounts now recommend a combination of letters,

numbers, and symbols to make a stronger password. Be sure to include them.

Try to use a different password for each of your online accounts so that a hack in one doesn't affect the others.

7. Be careful what you share online

Limit the personal information you share on social media and other websites. You don't want to make it easy for cyber criminals to get your personal information. Never put your real birthday anywhere online unless absolutely necessary. You my even consider using an alias instead of your real name for subscriptions, site registrations, etc. on 'noncritical' sites.

8. Shop on familiar and safe websites

Bookmark your favorite shopping sites to get there quickly and safely. As much as possible, avoid typing the name of the website in the URL bar. This will prevent you from typos that could take you to a fake site that looks identical to the real site.

9. Trust Your Gut

If you question the site's trustworthiness, move on. Take any doubt as a sign that you should not make any transactions on the site. Remember, if an offer looks too good to be true, it probably is.

USFHP at PacMed Information Security Team

Don Carter
Information Security Manager

McCall Paxton
Senior Information Security Engineer

Abolaji Filani
Information Security Analyst

PHARMACY UPDATE:

Take a Prudent Approach to Antibiotics

Antibiotic stewardship has long been an important topic. But changes in recent years require an updated approach to antibiotic utilization to ensure efficacious treatment and prevent antibiotic resistance. Keep these guidelines in mind:

Use appropriate durations of therapy, which are often shorter than in the past.	**Avoid antibiotics for:** • Sinusitis (if needed, 5-7 days is often sufficient) • Bronchitis (except COPD exacerbations for <5 days) • Otitis media in patients >2 years of age (5-7 days if necessary)
	3-Day Courses • UTI when using SMX/TMP
	5-Day Courses • Community Acquired Pneumonia (7 days for MRSA) • Cellulitis • UTI when using nitrofurantoin
Avoid certain antibiotics in patients on certain potentially interactive medications or who have reduced renal function.	**Ciprofloxacin** • Avoid combining with warfarin and theophylline • Avoid if CrCl <30ml/min
	Macrolides • Monitor closely with warfarin
	Nitrofurantoin • Avoid if CrCl <30ml/min • Avoid chronic use
	SMX/TMP • Avoid combining with warfarin and phenytoin • Avoid if CrCl <30ml/min • Monitor potassium if CrCl 30-60 and on an ACE/ARB

Other Health Insurance

The US Family Health Plan takes pride in paying claims right the first time, including claims where there is other health insurance (OHI) — that is, other than TRICARE. OHI can be an employer-sponsored or other private insurance program. Determining which payer is primary can be difficult and have an impact on timely and proper claim reimbursement. Below is some guidance to understanding the interaction between TRICARE and OHI.

USFHP at PacMed does not coordinate federal benefits. By law, TRICARE pays after all other health insurance, except for:

- Medicaid
- TRICARE supplements
- State victims of crime compensation programs
- Other federal government programs identified by the director, Defense Health Agency

Providers should submit claims for processing to a patient's OHI before submitting to TRICARE. Once primary benefits are received, forward the explanation of benefits along with a paper claim to:

USFHP at PacMed
Attention: Claims Department
1200 12th Ave.
Seattle, WA 98144

For Active-Duty Family Members:

- TRICARE coverage is for family only
- OHI can be primary; must be verified

For Patients on Medicare for End-Stage Renal Disease:

- USFHP at PacMed TRICARE is always primary unless the patient has Medicare End-Stage Renal Disease (ERSD) coverage

As a reminder, verify your patient's health insurance by reaching out to the health plan or plans if they have any other health insurance. This keeps your records up-to-date and allows for timely claim processing and accurate reimbursement.

ATTENTION: 2025 Copay Reference Guide

THE COPAY REFERENCE GUIDE FOR 2025 CAN BE FOUND HERE:

https://s3-us-west-2.amazonaws.com/images.provhealth.org/other/Provider_Copay_Reference_Guide.pdf

Reminder: Register with InstaMed for Direct Claims Payment

For accelerated access to claim payments, USFHP at PacMed uses InstaMed for direct deposit into your existing bank account. You should experience no disruption to your current workflow—just choose to have electronic remittance advices (ERAs) routed to your existing clearinghouse.

Register for free for InstaMed Payer Payments:
www.instamed.com/eraeft

With InstaMed, USFHP at PacMed delivers claim payments via ERA and electronic funds transfer (EFT). ERA/EFT is a convenient, paperless and secure way to receive claim payments. Funds deposited directly into your designated bank account include the TRN Trace Reassociation Number, in accordance with CAQH CORE Phase III Operating Rules for HIPAA standard transactions.

TOOLS YOU CAN USE:

USFHPNW Provider Portal

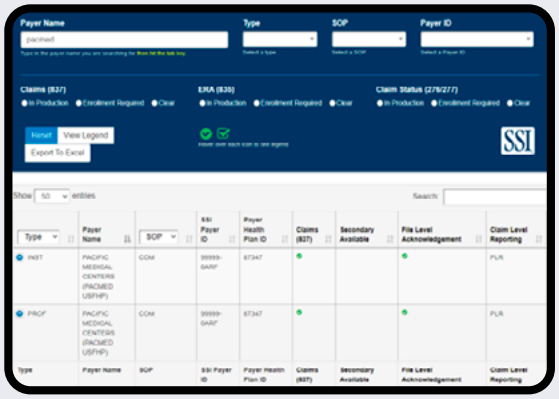
US Family Health Plan providers can view USFHP eligibility and claims status electronically through our provider portal. In addition, referral coordinators can submit referrals and view authorization status on the portal. Our goal is to make working with us that much easier!

To set up your account, contact USFHP Provider Relations at ProviderRelations@USFHPpacmed.org

Already have a portal account? Please let your caregivers know they can gain access by reaching out to designated administrators in your organization.

Electronic Referral Now Available

We are pleased to announce providers can now submit referrals electronically through the **USFHP HealthTrio provider portal**. Users with a 'Referral Coordinator Active" role assigned to their profile can submit referrals for specialist, outpatient or facility admission services. Local administrators should contact ProviderRelations@USFHPpacmed.org for training on how to use this new feature and to get set up.



BILLING TIPS

Commercial insurance is always the primary plan. While US Family Health Plan is the primary plan for benefits and the primary manager of care, it's the secondary payor when a patient has commercial insurance.

Always submit a claim to the primary payor—*even if the balance is zero.* Per the Department of Defense, USFHP must report all insurance reimbursement amounts collected by any provider.

Our member cannot be billed for any remaining balance. When the primary payor issues payment, bill USFHP and include the Explanation of Payment from the primary payor.

All claims for all USFHP beneficiaries should be mailed to:

US Family Health Plan
1200 12th Avenue S
Seattle, WA 98144-2712

Payment will be based on the amount the primary payor indicates the patient is responsible for, up to the contract/CMAC allowed amount.

DON'T BILL MEDICARE. Some of our Medicare-aged enrollees are grandfathered into US Family Health Plan. USFHP enrollees who are Medicare beneficiaries have waived their use of Medicare. Do not bill Medicare for care provided to these enrollees. ***All*** claims for ***all*** our beneficiaries should be mailed to US Family Health Plan.

INVITATION:

Help USFHP Advance Quality, Safety and Utilization Management

US Family Health Plan encourages you to serve as a member of the USFHP Quality, Safety, and Utilization Management Committee.

We welcome your ideas and suggestions on how service may be improved for providers and health plan members. To express interest in serving on this committee, or other committees that may be formed by USFHP, please contact USFHP Provider Relations: ProviderRelations@USFHPpacmed.org

ATTENTION: TRICARE PROGRAM MANUAL

Please be aware that we will be switching over to using the **2021 EDITION OF THE TRICARE PROGRAM MANUALS**.

You can view the updated manual here: https://manuals.health.mil/

CONTACT US

We are here to answer your questions, and we welcome your suggestions or feedback.

MEMBER SERVICES
(800) 585-5833, option 2

NETWORK CONTRACTING & PROVIDER RELATIONS
ProviderRelations@USFHPpacmed.org

(800) 585-5883, option 2

Elizabeth Maltos
Senior Provider Network Contract Specialist
(206) 774-5660

Brian Keeffe
Senior Provider Network Contract Specialist
(206) 774-5709

CREDENTIALING
Credentialing@USFHPpacmed.org

Lisa Velotta
Credentialing Manager
(206) 774-5679

Miranda Suggitt
Credentialing Manager
(206) 774-5690

www.usfhpnw.org

US Family Health Plan

A health plan sponsored by the Department of Defense (DoD) that offers the TRICARE Prime® benefit to uniformed services beneficiaries in the Puget Sound region.
The plan is administered by Pacific Medical Centers, which has performed this role for over 40 years.

Mission

To provide quality health care for uniformed services family members, retirees and their family members; to have extremely satisfied members; to demonstrate quality, value and operational effectiveness; and to be an integral and respected health care partner in the DoD's Military Health System.

US FAMILY HEALTH PLAN at PacMed

REMINDER:

USFHP and TriWest Healthcare Alliance Are Different Organizations

To avoid complication and frustration for you and US Family Health Plan members, please make sure that bills/claims/referrals and anything else intended for USFHP does **not** go to TriWest Healthcare Alliance. We are not the same organization.

Claims are processed by date of service, and USFHP reimburses facility-based care at the TRICARE/CHAMPUS DRG or contracted rate. TRICARE rates are updated annually. To access information about TRICARE fee schedule changes, as well as our current Provider Manual, please visit www.usfhpnw.org.