Part B Insider (Multispecialty) Coding Alert

Physician Notes: Feds Plan to Ramp Up Payment Scrutiny

Plus: CMS alerts providers to Blue Button 2.0 bug.

Due in part to the skyrocketing costs of healthcare, Medicare wants to reduce improper payments from the get-go.

Details: Back in September, the Centers for Medicare & Medicaid Services (CMS) released a final rule in the Federal Register titled "Program Integrity Enhancements to the Provider Enrollment Process." The rule outlined the agency's initiative to utilize the Medicare enrollment system to stop fraudsters before they joined the program.

Now: CMS expanded on this integrity plan with its "five-pillars program" to combat improper payments and cut Medicare fraud before it starts.

"Our progress on improper payments is historic, but there's more work to be done," says CMS Administrator **Seema Verma** in a release. "CMS has taken a multifaceted approach that includes provider enrollment and screening standards to keep bad actors out of the program, enforcement against bad actors, provider education on our rules and requirements, and advanced data analytics to stop improper payments before they happen."

Take a look at the five-pillars program's focus areas:

- **Bad actors:** CMS aims to use a variety of resources to "stop bad actors" from taking advantage of federal healthcare programs.
- **Prevention:** Using screening and background information, the feds hopes to nip issues in the bud and prevent fraud, abuse, and waste on the front end.
- **Risk reduction:** Value-based care remains one of Medicare's primary focuses, and the agency plans to protect its cost-saving, pro-patient initiatives by exploring "ways to identify and reduce program integrity risks" by utilizing experts in the field, the release suggests.
- **Administration cutbacks:** CMS made administrative burden rollbacks a priority a while ago, and the pillars build on that by promoting simplified coverage and payment rules, paperwork reductions, and duplication cuts.
- **Health IT:** The agency wants to utilize technologies like artificial intelligence and machine learning to streamline the payment process and reduce claims burdens for providers.

Verma adds, "These initiatives strike an important balance between preventing improper payments and reducing the administrative burden on legitimate providers and suppliers."

In other news…

Apparently, even Medicare struggles with data security and protecting patients' data, reports suggest.

Details: One of the Centers for Medicare & Medicaid Services' (CMS) third-party associates discovered a "data anomaly" in its Blue Button 2.0 API (BB2.0), an agency blog post states. After looking into the incident, a bug in the BB2.0 codebase was found, and it may have exposed some Medicare beneficiaries' protected health information (PHI).

"BB2.0 was truncating a 128-bit user ID to a 96-bit user ID," CMS explains. "The 96-bits remaining were not sufficiently random to uniquely identify a single user. This resulted in the same truncated user ID being assigned to different beneficiaries."

CMS continues, "Because BB2.0 was truncating the user ID provided by the identity management system, some beneficiaries with the same truncated ID were passed data pertaining to other users via BB2.0."

Though the technical issue impacted less than 10,000 individuals and only 30 BB2.0 apps, CMS instituted more in-depth code reviews, testing, and cross team collaboration.

After a full review, CMS "corrected the faulty code, implemented additional protections, and is resuming normal operations of the system," the agency said in a Dec. 27, 2019 update.

Find out what apps were impacted at https://bluebutton.cms.gov/blog/bbapi-update.html.