January 20, 2025 | Volume 39, Issue 4

Part B News
partbnews.com
COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES


## In this issue



*Compliance*

# New HIPAA rule makes the 'addressable' required, even before it's finalized

A proposed rule from HHS would confirm that cybersecurity measures such as multi-factor authentication (MFA) and encryption of electronic protected health information (ePHI) are not optional safeguards, but something covered entities such as physician practices are required to implement to stay compliant with HIPAA. Because of the way the policies are directed, experts say you should work to meet the proposed rule's requirements whether or not the rule is finalized.

The proposed rule, "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information," published on January 6, addresses the massive and growing threat of cybersecurity breaches such as the ransomware attack on Change Healthcare covered entities (CE) that exposed tens of millions of patient records and cost tens of millions of dollars to clean up after (*PBN 7/1/24*).

Practice managers note: HHS says while that "many people, including regulated entities, inaccurately believe that only large regulated entities that maintain electronic records about millions of individuals are likely to face a cyberattack … smaller regulated entities may also be the target of, or adversely affected by, cybercrime, partly because of the interconnectedness of health care and partly because they are less likely to have invested in cybersecurity, making them easier targets."



decisionhealth®
an hcpro brand

("Regulated entities" include both CEs and business associates [BA] that work with CEs. Under this rule, BAs, in a change from previous policy, would be obliged to meet the same elevated security standards as CEs.)

## HHS clarifies what is 'addressable'

HHS says that regulated entities may have the wrong impression about their duty under the Security Rule to implement specifications that are described as "addressable."

Previous guidance on this may seem ambiguous. For example, HHS' HIPAA pages include a FAQ from 2022 on the difference between addressable and "required" actions that says regulated entities "must implement an addressable implementation specification if it is reasonable and appropriate to do so" or else "must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative." CEs are expected to document and explain whatever "equivalent alternatives" they employ.

But in the new rule HHS says that some CEs and BAs "believe that flexibility overrides the need for them to protect all ePHI and do not uniformly treat addressable implementation specifications as needing to be met if they are reasonable and appropriate."

That is, HHS adds: "'addressable' is misunderstood to be optional, leading regulated entities to choose not to adopt the implementation specification, even when it would be reasonable and appropriate for them to do so."

This may sound like hair-splitting. But Alisa L. Chestler, attorney and chair of the data protection, privacy and cybersecurity team at Baker Donelson in Nashville, explains that it hinges on the difference between what some practices think is reasonable to expect of them and what HHS thinks is reasonable — which often is more than many practices do.

For example, while "10 years ago nobody had multi-factor authentication, and for most it was likely too expensive and complicated to implement," Chestler says, now "one could argue, especially for a larger organization, that when it's easy to add multi-factor authentication, it's already [in that sense] required."

HHS not only proposes regulated entities use MFA but also gets specific about it, saying that their MFA must be based on "at least two of three categories of factors of information about the user," including "information known by the user" (e.g. a password), "item possessed by the user" (e.g. a token), or "personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics."

Similarly, HHS says that "encryption is built into most software today, and where it is not, there are affordable and easily implemented solutions that can encrypt sensitive information. Thus, it generally would be reasonable and appropriate for regulated entities

decisionhealth®

**SUBSCRIBER INFORMATION**

Have questions on a story? Call or email us.

***PART B NEWS* TEAM**

**Maria Tsigas**
*Product Director*
maria.tsigas@hcpro.com

**Marci Geipe**
*Senior Manager, Product and Content*
marci.geipe@hcpro.com

**Richard Scott**
*Content Manager*
richard.scott@hcpro.com

**Roy Edroso**
*Editor*
roy.edroso@hcpro.com

**Julia Kyles, CPC**
*Editor*
julia.kyles@hcpro.com

**Medical Practice & Hospital community!**

www.facebook.com/DecisionHealthPAC
www.twitter.com/DH_MedPractice
www.linkedin.com/groups/12003710

**SUBSCRIPTIONS**
Direct questions about newsletter delivery and account status, toll free, to 1-855-CALL-DH1 or email: customerservice@hcpro.com

**DECISIONHEALTH PLEDGE OF INDEPENDENCE:**
At DecisionHealth, the only person we work for is you, the provider. We are not affiliated with any special interest groups, nor owned by any entity with a conflicting stake in the health care industry. Every reasonable effort has been made to ensure the accuracy of the information contained herein. However, the ultimate responsibility for correct billing and compliance lies with the provider of services. DecisionHealth, its employees, agents and staff make no representation, warranty or guarantee that use of the content herein ensures payment or will prevent disputes with Medicare or other third-party payers, and will not bear responsibility or liability for the results or consequences resulting from the use of the content found herein.

**CONNECT WITH US**
Visit us online at: www.partbnews.com.

**CEUS**
*Part B News* offers prior approval of the American Academy of Professional Coders (AAPC) for 0.5 CEUs for every other issue. Granting of this approval in no way constitutes endorsement by the Academy of the program, content or the program sponsor. You can earn your CEUs by passing a five-question quiz delivered through the *Part B News* CEU website (https://ceus.coursewebs.com).

**ADVERTISING**
To inquire about advertising in *Part B News*, call 1-855-CALL-DH1.



*Part B News*® is a registered trademark of DecisionHealth, a division of HCPro LLC. *Part B News* is published 48 times/year by DecisionHealth, 35 W. Wacker Drive, 16th floor, Chicago, IL 60601-5809.
ISSN 0893-8121. pbncustomer@decisionhealth.com Price: $699/year.



decisionhealth® an hcpro brand

to implement a mechanism to encrypt ePHI, and regulated entities should already have done so in most circumstances."

Entities will be allowed only "limited exceptions" to these requirements. However, the requirements are not all spelled out in the proposed rule. You can expect many suggestions in the comments period.

"I don't mean to make this one size fits all," Chestler says, "but as the costs come down and the solutions become ubiquitous it becomes harder to argue that you don't need to address it."

## Not just new tools

The proposed rule doesn't limit its instructions to specific security tools. It also expands what regulated entities must consider when they do their security planning, as they must do as part of their HIPAA-required security risk assessments.

The current Security Rule says CEs must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that a covered entity creates, receives, maintains, or transmits." Some providers may take this to mean they just need to check due-diligence boxes.

But the new rule says a regulated entity must "take into account how effectively its application of a particular security measure to achieve compliance with a standard and its associated implementation specifications would support its resiliency in the face of an event that adversely affects the entity" — for example, a ransomware attack.

This would require regular, intense scrutiny of your IT structures, including a network map and an asset inventory, and a whole new testing regimen, including "vulnerability scans" of your system every six months, and annual penetration testing — the kind of high-level "pen tests" security experts have been advising to prepare for cyberattacks for years (*PBN 4/26/21*).

The rule also would require that entities have a plan to, in the event of such an incident, "restore loss of critical relevant electronic information systems and data in 72 hours or less." In addition to auditing their plans every year, and scanning their systems every six months, they must maintain and regularly update their asset inventories and network maps.

Todd Thorsen, chief information security officer at data resilience and governance company CrashPlan, believes this will require regular high-intensity tests such as tabletop exercises and other disaster recovery reviews, and "should include partnering with all relevant business unit leaders and risk owners to ensure the recovery is holistic and meets the organization's standards."

Chestler says this calls for IT people "with the skillset to do proper network segmentation and documentation. There's a cost to that, and if you bring in a consultant and they give you something at the end of the year, within six months, if it's not kept up to date by your internal resources, it will already be out of date."

Elizabeth H. Johnson, an attorney with Wyrick Robins in Raleigh, N.C., and member of the firm's privacy and data security practice group, sees some wiggle room on the 72 hours requirement: "The organization has discretion about which systems are 'critical,'" she notes, and while "the contingency plan needs to accommodate getting things back online in 72 hours … it's not an immediate violation if it actually takes longer, provided the delay is not egregious."

But Johnson finds other parts of the rule very demanding: "Ask any privacy professional who has tried to data-map," she says. "It's a full time job in a decent-sized organization."

Your legal and security team should comb the rule for other significant nuances. Avery A. Dial, partner with Kaufman Dolowich LLP in Fort Lauderdale and chair of the firm's data privacy and cybersecurity practice group, notes that the rule states that you must be able to not only authenticate persons requesting ePHI, but also authenticate "technology assets" such as servers and apps that make those requests. The rule also requires that your "electronic information systems are segmented to limit access to ePHI to authorized workstations." That means, Dial says, "you only allow people to access what [ePHI] they need to do their jobs."

Matt Fisher, partner at Hancock, Daniel & Johnson P.C. in Glen Allen, Va., believes the expansion and added scrutiny of risk analysis were pretty much inevitable.

"Almost every OCR settlement on alleged noncompliance with HIPAA has found that the risk analysis was either deficient or had not been conducted," Fisher says. "OCR has been signaling for years and trying to do it in a nicer way. Now you're starting to get the hammer of stricter regulation."

## BAs' burden — and yours

The added responsibilities for BAs also amount to more responsibility for CEs, because, Fisher explains, "they'll have to be in contact with all their business associates and then make sure they're collecting all of those certifications — probably requiring a FTE [full-time employee] for the larger covered entities: A hospital system [for example] probably has thousands upon thousands of business associates."

As for the BAs, Mark Knight, a partner at Armanino Advisory LLC and Armanino LLP in Austin, bluntly expects "some service providers will go under as a result of this, because they can't meet their requirements." But Michael Madderra, an associate with the Morgan Lewis law firm in Seattle, expects others with the capacity to handle the work to flourish: "I think this rule would create additional demand and work for compliance and risk management vendors," he says. "The vendors I know are already busy; this is only going to make them busier."

## Impact of the incoming administration

Most experts think that the upcoming change in administrations should not affect the rule too much — apart from speed and scope of finalization.

"I think there's universal understanding that the number of breaches occurring in the health care industry is not sustainable," Knight says. "I think that's a bipartisan issue. No one wants to see sensitive health information being marketed across the dark net."

Deborah A. Cmielewski, a partner with Schenck, Price, Smith & King in Florham Park, N.J., points out that in his first term Donald Trump signed into law the Cybersecurity and Infrastructure Security Agency Act that established the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security. "Given the impact that emerging threats can have to homeland security and national security, the incoming administration knows that cybersecurity initiatives remain vital," she says.

Whether the rule is finalized or not, HHS is making a statement about what it currently expects. "Fully ignoring the proposal also ignores a pretty strong signal about what the agency expects under the current rule," Johnson says.

If the rule is delayed, "you're still not going to be able to say, well, it's not a final rule yet," Chestler says. "You do not want to be caught flat-footed with not enough time for strategic planning necessary to implement in a cost-effective manner."

## Takeaway: Get to work

However you slice it, there's more HIPAA work ahead for nearly every CE.

"The proposal does implement quite a few concepts that are either clear expectations from HIPAA guidance and enforcement, or which would be 'good hygiene' for a cyber-conscious organization," Johnson says. "However, from a high level, what makes the proposal's requirements difficult is that flexibility is largely taken out of the equation."

Matt Fisher worries about the burden on smaller health care entities and "whether they're going to be able to address the findings in a pen testing report — and, if they don't have the resources to address the vulnerabilities [it reveals] and something happens because of it, what the [compliance] fallout is going to be."

Fisher expects a flood of comments to the rule that address these and similar topics. "You want to allow flexibility to account for different types of entities across health care while at the same time still promoting the enhancement and evolution of security," he says.

On the positive side, the rule's clarity will give IT teams a mandate to implement effective security, which is a real industry-wide concern and the point of the rule.

"[It] gives the IT team the power to go to their finance team and say, 'we have to invest in these areas because it specifically says so,' instead of saying it implies that we should do this," Knight says. — *Roy Edroso* (*roy.edroso@decisionhealth.com*)

**RESOURCES**

- HHS, "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information," Jan. 6, 2025: *https://public-inspection.federalregister.gov/2024-30983.pdf*
- HHS, HIPAA FAQ: "What is the difference between addressable and required implementation specifications in the Security Rule?" Dec. 28, 2022: *www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html*

*(continued on p. 6)*

*Benchmark of the week*

# Highest level E/M reporter depends on who, where and encounter type

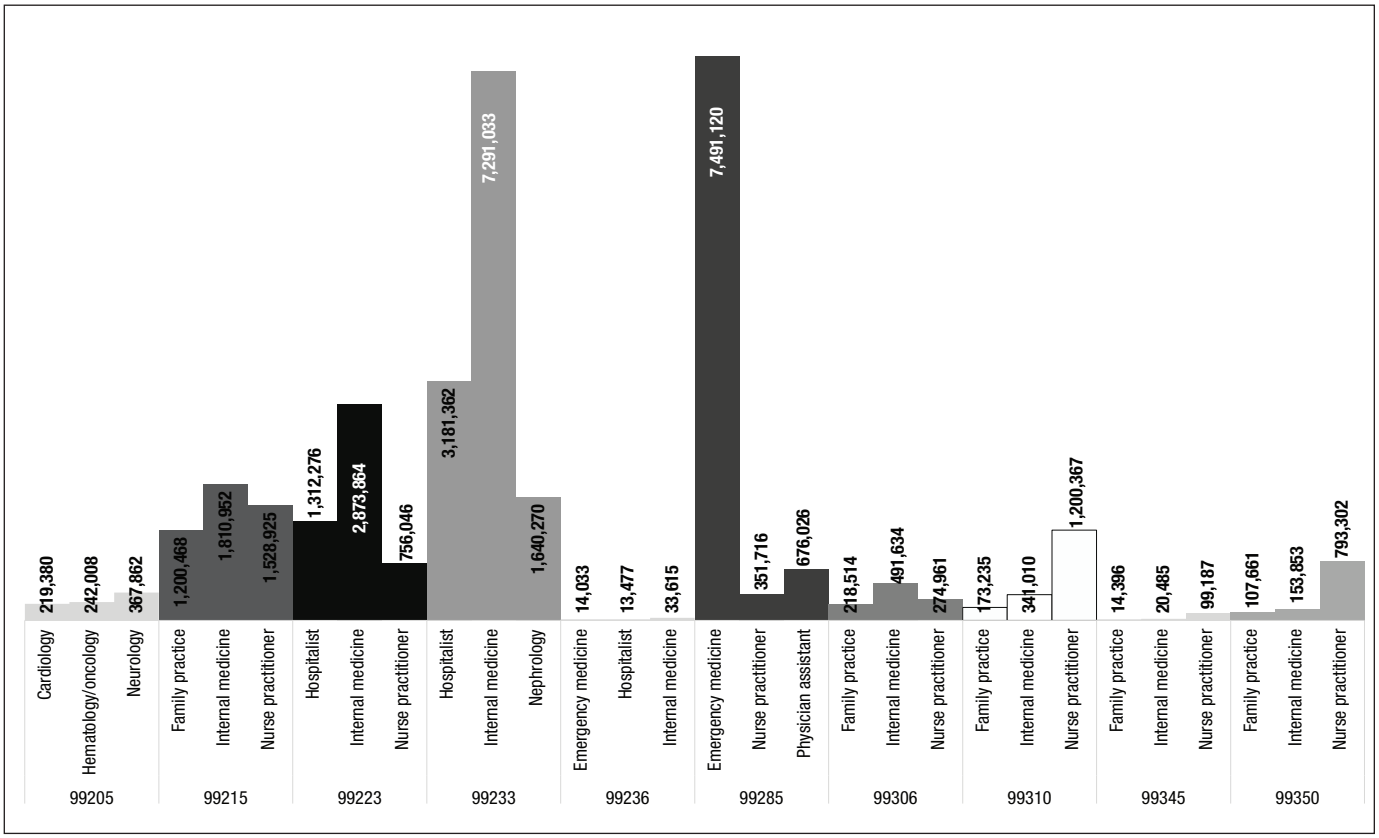
A review of the top three specialties that reported high-level E/M codes in 2023 reveals a variety of primary care providers and other specialists at the top of the list. When it comes to the highest-level office visit code for new patients, three specialties dominated claims for **99205**, the E/M visit with the highest payout.

To report a high-level encounter, the treating provider must document that they performed high-level medical decision making (MDM) or that they reached the time threshold in the code's descriptor. The only exception is the emergency department visit (**99285**), which can only be coded based on MDM.

The latest Medicare Part B claims data from calendar year 2023 shows that cardiologists, hematologist/oncologists, and neurologists were the top three reporters for the highest-level new patient office/other outpatient encounter, but the benchmark also shows that primary care specialties took the top spots for established patient visits (**99215**).

Internal medicine physicians and nurse practitioners were represented across a wide variety of top-level visits, which coincides with data on how frequently the providers report prolonged E/M visit codes (*PBN 12/12/24*). Hospitalists were represented in the initial, subsequent and same-day admission and discharge hospital services (**99223, 99233** and **99236**). — *Julia Kyles, CPC* (*julia.kyles@decisionhealth.com*)

## Highest level E/M visits by specialty, 2023




*Source:* Part B News *analysis of 2023 Medicare claims data*

*(continued from p. 4)*

- U.S. Code of Federal Regulations, "45 CFR § 164.308 - Administrative safeguards," via Cornell Law School: www.law.cornell.edu/cfr/text/45/164.308

*Correct Coding Initiative*

# CMS closes modifier 25 loophole in the 2025 NCCI manual

Teach the tighter modifier **25** guidelines in the 2025 National Correct Coding Initiative (NCCI) Manual and pass along the latest updates on mutually exclusive edits.

Coders should also note that CMS released the 2025 manual in a single document (*see resource, below*). This will spare readers the trouble of opening multiple files when they want to read more than one chapter of the manual.

## Modifier 25 when global surgery does not apply

CMS updated its guidance for submitting modifier 25 (Significant, separately identifiable evaluation and management service by the same physician or other qualified health care professional on the same day of the procedure or other service), when the E/M visit happens on the same day as a service with a global surgery indicator of XXX (Global surgery concept does not apply).

The revised guidance begins in Chapter 1, General Correct Coding Policies, section D. Evaluation & Management (E&M) Services. New language makes it clear that even when the global concept doesn't apply to the procedure, the E/M visit must be "above and beyond usual pre- and post-operative work of the procedure," to report the E/M code.

CMS also revised language that could have been interpreted as always allowing a separate E/M visit on the same day as an XXX procedure.

**Previous guidance:** "Appending modifier 25 to a significant, separately identifiable E&M service when performed on the same date of service as an 'XXX' procedure is correct coding."

**Updated guidance:** "Appending modifier 25 to a significant, separately identifiable E&M service when performed on the same date of service as an 'XXX' procedure **may be appropriate in some instances.**"

CMS added similar guidance to the NCCI manual's other chapters. You'll find the statement in the section on E/M services.

This is a reminder that practices should not automatically append modifier 25 to an E/M visit because the same-day procedure is one of the 1,458 covered codes that have an XXX global surgery indicator. The services include annual wellness visits, allergy testing, physical therapy and chemotherapy infusions. (*See bonus material, online, for a full list of XXX codes that are covered by Medicare, along with their short descriptors.*) Coders and billers should follow the same rules for determining whether the documentation for an encounter meets the requirements for modifier 25.

## More on mutually exclusive edits

You'll also find extended information on mutually exclusive edits in chapter 1. CMS added two paragraphs to section P, which confirms that it can be appropriate to override many mutually exclusive edits in the NCCI's procedure-to-procedure (PTP) table.

"For example, the 2 procedures of a code pair edit may be performed at different anatomic sites (e.g., contralateral eyes) or separate patient encounters on the same date of service," new language in the manual explains. — *Julia Kyles, CPC* (julia.kyles@decisionhealth.com)

**RESOURCES**

- Medicare Full-Complete Manual (One File) (PDF): www.cms.gov/files/document/2025nccimedicarepolicymanualcompletepdf.pdf
- 2025 physician fee schedule relative value file: www.cms.gov/medicare/payment/fee-schedules/physician/pfs-relative-value-files/rvu25a

*Coding*

# Note 63 services reportable with G2211 and 25-appended E/M visits

As of Jan. 1, practices are eligible to report visit complexity add-on code **G2211** with office visit codes **99202-99215** when appending modifier **25** to the primary E/M code (*PBN 11/18/24*). However, take note of the billing restrictions that CMS placed on the same-day services eligible for the billing opportunity.

Previously, practices were barred from reporting the add-on visit complexity code when reporting an office visit code with modifier 25.

But the final 2025 Medicare physician fee schedule cleared the way for G2211 on a 25-appended claim. With Transmittal 13015, released Dec. 23, 2024, CMS clarified the roughly five dozen services that would be appropriate for reporting on the same day as G2211.

The following list of codes, covering a range of Part B preventive services and immunization and vaccine administration services, shows the full list of allowed services. "G2211 is payable even if you report the base code with modifier 25 only when the service or other procedure requiring the reporting of modifier 25 is an allowed Part B service," according to CMS. For instance, you can report G2211 with an E/M office visit code on the same day that you perform advance care planning (**99497-99498**) or an initial or subsequent annual wellness visit (**G0438-G0439**). — *Richard Scott* (*richard.scott@decisionhealth.com*)

## Allowed service when reporting G2211 with 25-appended office visit

| Code | Short or long descriptor |
|---|---|
| **71271** | Computed tomography, thorax, low dose for lung cancer screening, without contrast material(s) |
| **76706** | Ultrasound, abdominal aorta, real time with image documentation, screening study for abdominal aortic aneurysm (AAA) |
| **76977** | Us bone density measure |
| **77063** | Breast tomosynthesis bi |
| **77067** | Scr mammo bi incl cad |
| **77078** | Ct bone density axial |
| **77080** | Dxa bone density axial |
| **77081** | Dxa bone density/peripheral |
| **77085** | Dual-energy X-ray absorptiometry (DXA), bone density study, 1 or more sites; axial skeleton (eg, hips, pelvis, spine), including vertebral fracture assessment |
| **90460** | Im admin 1st/only component |
| **90461** | Im admin each addl component |
| **90471** | Immunization admin |
| **90472** | Immunization admin each add |
| **90473** | Immune admin oral/nasal |
| **90474** | Immune admin oral/nasal addl |
| **96156** | Hlth bhv assmt/reassessment |
| **96158** | Hlth bhv ivntj indiv 1st 30 |
| **96159** | Hlth bhv ivntj indiv ea addl |
| **96164** | Hlth bhv ivntj grp 1st 30 |
| **96165** | Hlth bhv ivntj grp ea addl |
| **96167** | Hlth bhv ivntj fam 1st 30 |
| **96168** | Hlth bhv ivntj fam ea addl |
| **97802** | Medical nutrition therapy; initial assessment and intervention, individual, face-to-face with the patient, each 15 minutes |
| **97803** | Medical nutrition therapy; re-assessment and intervention, individual, face-to-face with the patient, each 15 minutes |
| **97804** | Medical nutrition therapy; group (2 or more individual(s)), each 30 minutes |
| **99406** | Smoking and tobacco use cessation counseling visit; intermediate, greater than 3 minutes up to 10 minutes |
| **99407** | Smoking and tobacco use cessation counseling visit; intensive, greater than 10 minutes |
| **99497** | Advance care planning including the explanation and discussion of advance directives such as standard forms (with completion of such forms, when performed), by the physician or other qualified health care professional; first 30 minutes, face-to-face with the patient, family member(s), and/or surrogate |
| **99498** | Advance care planning including the explanation and discussion of advance directives such as standard forms (with completion of such forms, when performed), by the physician or other qualified health care professional; each additional 30 minutes (List separately in addition to code for primary procedure) |

| Code | Short or long descriptor |
|---|---|
| **G0101** | Ca screen;pelvic/breast exam |
| **G0102** | Prostate cancer screening; digital rectal examination |
| **G0104** | Ca screen;flexi sigmoidscope |
| **G0105** | Colorectal scrn; hi risk ind |
| **G0106** | Colorectal cancer screening; alternative to g0104, screening sigmoidoscopy, barium enema |
| **G0108** | Diabetes outpatient self-management training services, individual, per 30 minutes |
| **G0109** | Diabetes outpatient self-management training services, group session (2 or more), per 30 minutes |
| **G0120** | Colorectal cancer screening; alternative to g0105, screening colonoscopy, barium enema |
| **G0121** | Colon ca scrn not hi rsk ind |
| **G0124** | Screening cytopathology, cervical or vaginal (any reporting system), collected in preservative fluid, automated thin layer preparation, requiring interpretation by physician |
| **G0130** | Single energy x-ray study |
| **G0136** | Administration of a standardized, evidence-based social determinants of health risk assessment tool, 5-15 minutes |
| **G0141** | Screening cytopathology smears, cervical or vaginal, performed by automated system, with manual rescreening, requiring interpretation by physician |
| **G0270** | Medical nutrition therapy; reassessment and subsequent intervention(s) following second referral in same year for change in diagnosis, medical condition or treatment regimen (including additional hours needed for renal disease), individual, face to face with the patient, each 15 minutes |
| **G0271** | Medical nutrition therapy, reassessment and subsequent intervention(s) following second referral in same year for change in diagnosis, medical condition, or treatment regimen (including additional hours needed for renal disease), group (2 or more individuals), each 30 minutes |
| **G0296** | Visit to determ ldct elig |
| **G0402** | Initial preventive exam |
| **G0403** | Electrocardiogram, routine ecg with 12 leads; performed as a screening for the initial preventive physical examination with interpretation and report |
| **G0404** | Electrocardiogram, routine ecg with 12 leads; tracing only, without interpretation and report, performed as a screening for the i nitial preventive physical examination |
| **G0405** | Electrocardiogram, routine ecg with 12 leads; interpretation and report only, performed as a screening for the initial preventive physical examination |
| **G0438** | Ppps, initial visit |
| **G0439** | Ppps, subseq visit |
| **G0442** | Annual alcohol misuse screening, 5 to 15 minutes |
| **G0443** | Brief face-to-face behavioral counseling for alcohol misuse, 15 minutes |
| **G0444** | Annual depression screening, 5 to 15 minutes |
| **G0445** | High intensity behavioral counseling to prevent sexually transmitted infection; face-to-face, individual, includes: education, skills training and guidance on how to change sexual behavior; performed semi-annually, 30 minutes |
| **G0446** | Annual, face-to-face intensive behavioral therapy for cardiovascular disease, individual, 15 minutes |
| **G0447** | Face-to-face behavioral counseling for obesity, 15 minutes |
| **G0473** | Face-to-face behavioral counseling for obesity, group (2- 10), 30 minutes |
| **G0513** | Prolonged preventive service(s) (beyond the typical service time of the primary procedure), in the office or other outpatient setting requiring direct patient contact beyond the usual service; first 30 minutes (list separately in addition to code for preventive service) |
| **G0514** | Prolonged preventive service(s) (beyond the typical service time of the primary procedure), in the office or other outpatient setting requiring direct patient contact beyond the usual service; each additional 30 minutes (list separately in addition to code g0513 for additional 30 minutes of preventive service) |
| **P3001** | Screening papanicolaou smear, cervical or vaginal, up to three smears, requiring interpretation by physician |
| **Q0091** | Obtaining screen pap smear |

*Source: CMS Manual System, Transmittal 13015, www.cms.gov/files/document/r13015otn.pdf*