

How it works

Medicare Common Access Card

1 Medicare beneficiaries and service providers receive a **secure ID card**.

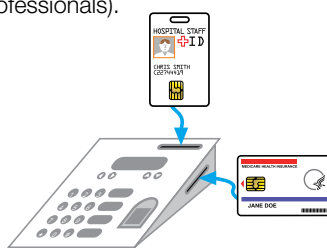
The smart card contains a computer chip that fights fraud and protects privacy.



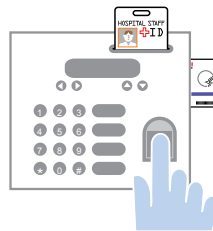
What's stored on the ID card:

- A unique Medicare identity.
- A digital picture of the healthcare professional.
- A PIN code (beneficiaries) or biometric (professionals).
- Match-on-card software: PIN or biometric stays in the card.

2 At the doctor's office, both the ID cards are inserted into the reader. The chip on the card electronically confirms the card is legitimate.



3 The doctor confirms his or her identity by touching the biometric reader, and the beneficiary by entering a PIN code, proving both were there.



4 Transaction is confirmed and a secure authenticated information packet is sent to the payment processor.



Common Access Card fights fraud, protects privacy

- Stops phantom billing. The beneficiary, the provider and their Medicare ID cards must be present to process a transaction.



- Prevents card passing. PIN code confirms patient identity.



- Protects privacy. Digital picture, PIN or biometric stays in the card.



- Because the Medicare card is a smart card, if the card is lost it can be deactivated remotely, protecting healthcare identity and information.



- Accurate identification and confirmation of eligibility of both beneficiary and service provider.



- Smart card security features prevent counterfeiting or altering ID cards and protect people's privacy and benefits.



- Privacy sensitive. Cardholders carry their PIN or biometric with them in the smart chip.

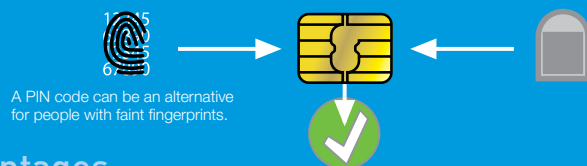


- With biometric, actual fingerprint images are not on the card, protecting privacy. Instead a mathematical value based on the person's finger is used to confirm identity.



What is match-on-card biometric technology?

- 1 During registration, the system generates a mathematical value based on the fingerprint. This value, called a template, is used for identity matching, not the actual fingerprint image.
- 2 The biometric template is encrypted and securely stored in the smart card chip.
- 3 During a transaction, the terminal scans the finger, generates a template and sends it to the card.
- 4 The match-on-card software compares the two template numerical values to see if they match. If they match, the person making the transaction is the cardholder.



Advantages

- The encrypted fingerprint biometric value never leaves the card.
- Privacy is assured because the full fingerprint image is never stored.
- Cardholder carries their biometric and PIN information with them.
- Simplifies networking, improves security and reliability, and enhances privacy. Eliminates the need for an online centralized database.

Medicare Common Access Cards stop rampant Medicare fraud.