Annex A - Client contact

Introduction

This annex provides guidance on dealing with both inbound and outbound contact with clients and third parties involved in CMS cases.

Bogus calls

Bogus callers to CMS are callers who try to get information about CMS clients under false pretences. Guidance on identifying potential bogus callers and the steps that a DM should follow if they think they have received a bogus call is available in CMS Security Check instructions.

Call recording

As the automated message on incoming calls advises callers that their call will be recorded, for quality and training purposes, it is not necessary to inform the caller of this again.

For outbound calls, whilst there is no legal obligation on CMS to advise clients that the call may be recorded, doing so provides better client service.

The DM, when they call should advise the client - "I should tell you that this call may be recorded for quality and or training purposes".

If a client expresses concern about the call being recorded, they should be reassured about the confidentiality of the CMS service. If they still do not wish to communicate with CMS by recorded call, they should be given the option to communicate with CMS in writing or offered a call back from a telephone that is not monitored.

GDPR gives individuals a legal right to see or receive a copy of personal data held about them. This includes recorded telephone calls.

Note: telephone calls not allocated to a case on the CMS system are usually deleted after three weeks.

A client can record a telephone conversation or an interview without obligation to tell CMS they intend to do so. If the client states they want or intend to record a phone interview, or if the DM suspects a phone interview is being recorded, they can ask the client if the call is being recorded. Clients will often admit they are recording the call when asked, this does not affect the client's rights to be interviewed at an office or by phone.

Complaints

The CMS has specified policies and procedures in place for handling complaints from clients and other third parties. See CMS Complaints Overview instructions.

Confidentiality statements

When first contact is made with a client, the DM must advise them of the confidentiality statement under GDPR. The confidentiality statement should be read to the client verbatim. Full details can be found in CMS Applications instructions.

Data Protection

GDPR imposes legal requirements to protect client information, and provides clients with rights to see information, records about them.

For further information, see DWP GDPR guidance.

Face to face visits

The CMS can arrange face to face visits with clients in certain limited circumstances. Further information about the situations where this may be appropriate and the guidance the DM should follow to make a referral is available in CMS Face to Face instructions.

Facilitating parental contact

This section explains the appropriate action to take if a parent with care or non-resident parent asks the CMS to help establish or re-establish contact with the other parent.

When a request to pass on contact details is received, the DM should check to ensure that this action has not been taken previously. If it has, it will not be appropriate for the details to be sent again, unless there has been a change in the relevant information.

The party making the request should complete an authorisation form confirming that they want their details to be passed on to the other parent. They should also be required to submit their contact details on an approved form.

The DM should check the approved form to ensure that only the requesting party's contact details have been included. No other communications should be forwarded and it should be made clear to the requesting party that the decision to make contact or not lies with the other parent.

Note: this guidance solely applies to requests from parents and should not be followed in relation to requests from children.

False information warnings

On first contact with a client, the criminal offence of failing to provide information statement must be given word for word. Full details can be found in CMS Applications instructions.

Freedom of information

The Freedom of Information Act 2000 provides individuals with the right to request information from any public authority. Requests for information made under the Freedom of Information Act 2000 must be responded to within twenty working days, and it is therefore important that any requests are referred to the appropriate team promptly.

For further information about the Freedom of Information Act 2000 and the process you should follow if you receive a Freedom of Information request, see DWP guidance.

Interpreters and translation services

The CMS has a range of processes in place for communicating with clients who may have difficulty using the standard methods of communication. This includes clients who are unable to speak English, or who have a hearing impairment. For further guidance about the range of services the CMS can offer in these circumstances see the CMS Interpretation Instructions.

Personal interest or sensitive cases

Sensitive cases are cases where access to the client records is restricted to a limited range of people. This can be for a number of reasons, such as

1. a CMS employee who has a connection to the case

2. the client is a transsexual

3. the client is a VIP or public figure

4. the client is an employee of the CMS, or

5. CMS consider it appropriate to do so, for example where there is an immediate threat of domestic abuse.

Any inbound contact on a case so marked should automatically route to the sensitive case team.

The DM can access additional guidance regarding sensitive cases using CMS Sensitive Case Instructions.

Representatives

Clients are entitled to arrange for a representative to deal with their case. It is important when the DM is dealing with potential representatives that they understand what authorisation is necessary from the client and what information can or cannot be disclosed.

For further guidance on working with representatives, see CMS client representative and power of attorney instructions.

Suicide Threats

If a suicide threat is received by post, this will be referred, by the DM's team leader to the Special Client Records (SCR) team. For suicide threats received by telephone, the DM must alert their TL and follow CMS Threats of suicide instructions.

Unsafe Interactions and potentially violent persons

The CMS has specified policies and procedures in place for cases where a client has acted in a way that is considered unsafe. This includes situations where a member of staff has been threatened, harassed or abused by a client in writing, in person, or verbally.

For further guidance, see Keep Customer Interactions Safe (KCIS).

Unauthorised disclosure of information

The CMS takes the unauthorised disclosure of information very seriously, whether intentionally or accidentally, this is a breach of GDPR and customer confidentiality.

If any person employed or in employment with the CMS discloses information without lawful authority, it is an offence[1].

1 CS Act 1991, s50

This can be information that was acquired by them

1. in the course of that employment with CMS, or

2. is derived from information acquired or held for the purposes of a case with CMS, and

3. relates to a particular person.

It is not an offence however to disclose information in a form that would not enable the person receiving the information to relate it to a particular parson, or which has previously been disclosed with lawful authority.

Lawful Disclosure

Disclosure is to be regarded as made with lawful authority if, and only if, it is

1. required by a civil servant executing their official duty

2. made by any other person either

    2.1 for the purposes of the function in the exercise of which he holds the information and without contravening any restriction duly imposed by the S of S, Lord Chancellor or their authorised nominees, or

    2.2 to, or in accordance with an authorisation duly given by, the S of S, Lord Chancellor or their authorised nominees

3. in response to an order from a court

4. for the purpose of initiating or actioning court proceedings

5. with the consent of the person the information relates to.

In most instances the appropriate person that information can be disclosed to will be the person that the information relates to, however the appropriate person can also be

1. a person with power of attorney

2. a Scottish mental health custodian who is entitled to act on behalf of an adult with incapacity[1]

3. the person's attorney or legal representative

4. a deputy of a person with a limited mental capacity[2].

1 AI (S) Act 2000; 2 MC Act 2005

Acceptable defence

Disclosure may be deemed acceptable if it can be proved that at the time the alleged offence was committed, the person disclosing the information believed

1. they were making the disclosure with lawful authority with no reasonable cause to believe otherwise

2. that the information in question had previously been disclosed to the public with lawful authority and had no reasonable cause to believe otherwise.

Possible outcomes of unauthorised disclosure

Any person found guilty of disclosing information without lawful authorisation may be liable to

1. imprisonment for a term not exceeding two years or a fine or both, or

2. to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both.